

РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ

В. П. Гринёв

ЦИФРОВАЯ ЭКОНОМИКА

И ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ
ЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С Л О В А Р Ь - С П Р А В О Ч Н И К

НАУЧНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Под редакцией

кандидата юридических наук, доцента **И. А. Цинделиани**

ЦИФРОВАЯ ЭКОНОМИКА: НАСТОЯЩЕЕ И БУДУЩЕЕ
ПРАВОВЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ
ПРОФЕССИОНАЛЬНЫЕ СТАНДАРТЫ
ТЕРМИНЫ, НОРМЫ И ОПРЕДЕЛЕНИЯ ОСНОВНЫХ ПОНЯТИЙ



• ПРОСПЕКТ •

РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ

В. П. Гринёв

ЦИФРОВАЯ ЭКОНОМИКА

И ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ
ЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

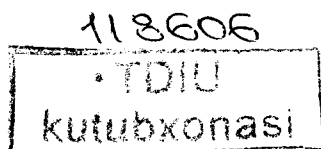
С Л О В А Р Ь - С П Р А В О Ч Н И К

НАУЧНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Под общей редакцией
кандидата юридических наук,
доцента **И. А. Цинделиани**



Электронные версии книг на сайте
www.prospekt.org



ОНТУ



• ПРОСПЕКТ •

Москва
2020

672, 15 (03)
УДК 346
ББК 67.402
Г852

672.15.7 (07)
+ 672.15.63(03) Электронные версии книг
на сайте www.prospekt.org
+ 339.13

Автор-составитель:

Гринёв В. П., окончил РГУП (с отличием) в 2005 г. Автор более 70 научных работ и публикаций общим объемом более 500 авт. л., в том числе «К вопросу о новых возможностях обеспечения государственных нужд в условиях цифровой экономики и проблемах правоприменения при переводе закупок в электронную форму», «Обеспечение закупочной деятельности в сфере обеспечения информационной безопасности: правовые аспекты» и др. Член Московского отделения Ассоциации юристов России, начальник юридического отдела Научно-исследовательского центра информатики при МИД России, эксперт научно-образовательного центра НИУ ВШЭ, кандидат военных наук, старший научный сотрудник по специальности «Иностранные государства и их потенциалы».

Рецензенты:

Егорова М. А., доктор юридических наук, профессор, член Международного комитета цифровой экономики (БРИКС);

Качалова А. В., кандидат юридических наук, доцент кафедры гражданского права Московского государственного юридического университета имени О. Е. Кутафина (МГЮА).

Под редакцией кандидата юридических наук, доцента **И. А. Цинделиани**.

Гринёв В. П.

Г85 Цифровая экономика и правовое регулирование обеспечения ее информационной безопасности : словарь-справочник : научно-методическое пособие / под ред. И. А. Цинделиани. — Москва : Проспект, 2020. — 384 с.

ISBN 978-5-392-31095-1

В настоящем издании представлены результаты комплексного анализа основных положений действующего законодательства о цифровой экономике и правовом регулировании обеспечения ее информационной безопасности.

Раскрыты основные положения национальной программы «Цифровая экономика Российской Федерации», реализуемые в ее рамках государственные программы и подпрограммы, а также федеральные проекты.

Представлены основные изменения действующего законодательства, технических заданий и национальных стандартов.

Включенный в состав данного издания словарь-справочник состоит из более 1100 терминов и определений основных понятий, используемых в нормативных правовых актах и сводах правил по вопросам цифровой экономики и правового регулирования обеспечения ее информационной безопасности.

Законодательство приведено по состоянию на 31 марта 2020 г.

Для руководителей и сотрудников органов МСУ, государственных гражданских служащих органов исполнительной власти, судебного сообщества, руководителей и специалистов организаций, предпринимателей, преподавателей, студентов, соискателей и аспирантов вузов, а также работников различных организаций, в том числе и в ходе обучения по специальным программам, предусмотренным учебными планами.

УДК 346
ББК 67.402

Справочное издание

ГРИНЁВ ВАЛЕРИЙ ПАВЛОВИЧ

**ЦИФРОВАЯ ЭКОНОМИКА И ПРАВОВОЕ РЕГУЛИРОВАНИЕ
ОБЕСПЕЧЕНИЯ ЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Словарь-справочник

Научно-методическое пособие

Подписано в печать 06.07.2020. Формат 60×90 1/16.

Печать цифровая. Печ. л. 24,0. Тираж 1000 (1-й завод 50) экз.

ООО «Проспект»

111020, г. Москва, ул. Боровая, д. 7, стр. 4.

ISBN 978-5-392-31095-1

© Гринёв В. П., 2020
© ООО «Проспект», 2020

ПРИНЯТЫЕ СОКРАЩЕНИЯ

АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
БД	–	большие данные (базы данных)
ВД	–	временный документ
ВМ	–	вычислительная машина
ГРИЗИ	–	группа реагирования на инциденты защиты информации
ГосСОПКА	–	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак
ДБС (SSA)	–	доверие к безопасности системы
DNS (Domain Name System)	–	система доменных имен
ЗАС	–	засекречивающая аппаратура связи
ЗБ (ST)	–	задание по безопасности
ЗБС (SST)	–	задание по безопасности для автоматизированной системы
ЗУ	–	запоминающее устройство
ИИ	–	искусственный интеллект
ИСПДн	–	информационные системы персональных данных
ИТ (IT)	–	информационная технология

КЖЦ	–	контракт жизненного цикла
КоАП	–	Кодекс Российской Федерации об административных правонарушениях
КСЗ	–	комплекс средств защиты
МНИ	–	машинные носители информации
МСУ	–	местное самоуправление
НКЦКИ	–	Национальный координационный центр по компьютерным инцидентам
НПА	–	нормативный правовой акт
НП ЦЭ	–	национальный проект «Национальная программа «Цифровая экономика Российской Федерации»»
НСД	–	несанкционированный доступ
НТД	–	нормативно-техническая документация
ОО (ТОЕ)	–	объект оценки
ОП	–	оперативная память
ОПКЦ	–	операционный центр, платежный клиринговый центр другой платежной системы при предоставлении операционных услуг и услуг платежного клиринга при переводе денежных средств с использованием сервиса быстрых платежей
ОС	–	операционная система
ОФБ (OSF)	–	организационные функциональные требования безопасности (функции безопасности, реализуемые организационными мерами)
ПДн	–	персональные данные
ПЗ (SP)	–	профиль защиты
ПЗС (SPP)	–	профиль защиты системы
ПО	–	программное обеспечение
ППП	–	пакет прикладных программ
ПРД	–	правила разграничения доступа

РД	–	руководящий документ
РФ	–	Российская Федерация
СВТ	–	средства вычислительной техники
СЗИ	–	система защиты информации
СЗСИ	–	система защиты секретной информации
СКЗИ	–	средства криптографической защиты информации
СМИБ (ISMS)	–	система менеджмента информационной безопасности
СНТП	–	специальное научно-техническое подразделение
СОИ	–	система обработки информации
СОО (STOE)	–	система как объект оценки
СП (SP)	–	специальная публикация
СРД	–	система разграничения доступа
ССНП	–	сервис срочного перевода и сервис несрочного перевода
СУБД	–	система управления базами данных
ТЗ	–	техническое задание
ТОО (ETR)	–	технический отчет об оценке
ТФБ (TSF)	–	технические функции безопасности
УК	–	Уголовный кодекс
ЭВМ	–	электронно-вычислительная машина
ФБС (SSF)	–	функции безопасности системы
ФЗ	–	федеральный закон
ФОИВ	–	федеральные органы исполнительной власти
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю
ЦП	–	цифровая подпись

ЭВТ	–	электронно-вычислительная техника
API	–	описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа (система) может взаимодействовать с другой программой (системой) ¹
SDMX	–	набор стандартных модулей для обмена статистической информацией с использованием технических стандартов, руководящих принципов по информационному наполнению и инструментов для создания структур данных и метаданных, а также для преобразования форматов и ввода данных ²
XML	–	формат обмена статистическими данными и метаданными, возникший при непосредственном участии крупнейших финансовых и экономических международных организаций, таких как Международный валютный фонд, Европейский центральный банк и др. ³
XML-шаблон	–	электронная версия формы статистического наблюдения ⁴

¹ Распоряжение Правительства РФ от 17 декабря 2019 г. № 3074-р «Концепция создания цифровой аналитической платформы». Пункт 1 — извлечение.

² Там же.

³ Там же.

⁴ Там же.

ВВЕДЕНИЕ

Вопрос обсуждения темы цифровой экономики во взаимосвязи с правовым регулированием обеспечения ее информационной безопасности в настоящее время имеет особую актуальность. Это связано с тем, что сегодня мир стоит перед новой реальностью, предпосылки которой обусловлены развитием информационных технологий, активизацией использования для управления в экономике, обществе и государстве искусственного интеллекта и больших данных.

Как отметил в своей статье, опубликованной в «Российской газете» еще в мае 2018 г., председатель Конституционного суда РФ В. Д. Зорькин¹, речь идет о вещах, не имеющих аналогов в прежнем мире, — интернет-вещах, цифровой экономике, криптовалюте и т. п.

По мнению В. Д. Зорькина, практически во всех отраслях народного хозяйства сейчас ведутся дискуссии об использовании роботов, в том числе и в юриспруденции, поскольку на компьютеры могут быть возложены задачи выполнения ряда типовых юридических процедур и подготовки различных документов. По его словам, сегодня зарождается в рамках информационного права «право второго модерна», регулирующее экономические, политические и социальные отношения. В этих условиях одна из основных задач государства — защищать цифровые права граждан от всевозможных нарушений, под которыми понимаются права людей на доступ, использование, создание и публикацию произведений в цифровой форме, на доступ и использование компьютеров, иных электронных устройств, а также сети Интернет.

Говоря о цифровых правах, уместно отметить, что глава 6 первой части Гражданского кодекса Российской Федерации в соответствии с Федеральным законом от 18 марта 2019 г. № 34-ФЗ была дополнена статьей 141.1 «Цифровые права», в соответствии с первой частью которой ими признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной

¹ Зорькин В. Д. Право в цифровом мире // РГ. 2018. № 115 (7578). 30 мая. С. 1, 4.

системы, отвечающей установленным законом признакам. При этом осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом, возможны только в информационной системе без обращения к третьему лицу, а в части второй этой статьи отмечается, что если иное не предусмотрено законом, обладателем цифрового права признается лицо, которое в соответствии с правилами информационной системы имеет возможность распоряжаться этим правом.

Касательно цифровых прав необходимо отметить учебник «Цифровое право» под общей редакцией В. В. Блажеева и М. А. Егоровой¹, презентация которого состоялась 27 ноября 2019 г. в рамках Кутафинских чтений на конференции «Современные проблемы развития юридических научных и образовательных программ России, Евросоюза и Азии».

В ряду знаковых событий по правовому регулированию цифровой экономики следует отметить и состоявшийся 4 декабря 2019 г. в МГУ им. М.В. Ломоносова интерактивный круглый стол «Проблемы гармонизации экономических отношений и права в цифровой экономике», в ходе которого презентовалась монография с одноименным названием².

Говоря о вкладе российских ученых-юристов в развитие цифровой экономики, следует также отметить такие работы, как «Финансовое право в условиях развития цифровой экономики»: монография / К. Т. Анисина, Б. Г. Бадмаев, И. В. Бит-Шабо и др.; под ред. И. А. Цинделиани. М.: Проспект, 2019. 320 с., «Правовое регулирование экономических отношений в современных условиях развития цифровой экономики»: монография / коллектив авторов / Московское отделение Ассоциации юристов России, МГУ имени М. В. Ломоносова, Ассоциация российских дипломатов / отв. ред. В. А. Вайпан, М. А. Егорова. М.: Юстицинформ, 2019. 376 с., и др.

В настоящее время в сфере складывающейся теории цифрового права и правового регулирования обеспечения ее информационной безопасности уже действует достаточно большое количество нормативных правовых актов (далее — НПА).

В этой связи на первый план выходят доступность и удобство использования информации о терминах и определениях основных

¹ Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. М.: Проспект, 2020. 640 с.

² Проблемы гармонизации экономических отношений и права в цифровой экономике: монография / коллектив авторов; МГУ имени М. В. Ломоносова, Университет имени О. Е. Кутафина (МГЮА), Московское отделение ассоциации юристов России, Международный союз юристов и экономистов (Франция); отв. ред. В. А. Вайпан, М. А. Егорова. М.: Юстицинформ, 2020. 280 с.

понятий законодательства о цифровой экономике и правового регулирования обеспечения ее информационной безопасности с целью объединения хозяйствующих субъектов в единое правовое пространство.

Как отметил Президент РФ В. В. Путин в своем выступлении 5 ноября 2019 г. на заседании Совета по русскому языку, «одновременно с актуализацией законодательства... **начать подготовку единого корпуса словарей, справочников, грамматик, содержащих нормы современного литературного языка при его использовании в качестве государственного языка Российской Федерации. Они должны стать обязательными для использования всеми государственными структурами**, будь то органы власти — и исполнительные, и судебные, законодательные — и школы, средства массовой информации».

В интересах достижения этой цели в рамках данной работы было проанализировано более 300 НПА, имеющих юридическую силу и регламентирующие соответствующие правоотношения в сфере цифровой экономики и правового регулирования обеспечения ее информационной безопасности, что позволило не только составить своеобразный словарь-справочник (глоссарий), включающий в себя более 1100 терминов и основных понятий, но и представить в систематизированном виде понятийный аппарат, введенный, в первую очередь, НПА федерального значения.

Для повышения практической значимости данной работы рассмотрены НПА, в соответствии с которыми в законодательство введены термины и определения основных понятий, касающиеся цифровой экономики и правового регулирования обеспечения ее информационной безопасности, приведены в Приложении 1 в виде соответствующего перечня.

С учетом того, что приведенные термины и определения основных понятий вводились различными НПА, то помимо перечня документов, регламентирующих соответствующие правоотношения по цифровой экономике и правовому регулированию обеспечения ее информационной безопасности, помещенного в Приложении 1, в Приложении 2 представлен алфавитный указатель терминов и определений основных понятий, помещенных в данное издание.

С целью создания у читателя данного учебно-методического пособия мотивирующих факторов к более углубленному изучению представленных в нем терминов и понятий, с которыми он знакомится в ходе его прочтения, структура Приложения 2 построена таким образом, что читатель сам может проставлять номера страниц, на которой находится тот или иной термин, что дает ему возможность мониторить изучаемый материал по мере его прочтения, проставляя соответствующие страницы рядом с термином или понятием по мере ознакомления с ними.

Выбранный подход изложения материала не только позволил представить в систематизированном виде термины и определения основных понятий законодательства о цифровой экономике и правовому регулированию обеспечения ее информационной безопасности, но и фактически заложил основу для подготовки энциклопедического словаря (гlossария) на эту тему.

Обсуждение вопроса о цифровой экономике и правовому регулированию обеспечения ее информационной безопасности было бы не полным, если не увязать его рассмотрение с вопросом об ответственности за соответствующие правонарушения в сфере защиты информации и информационных технологий.

С этой целью в Приложении 3 представлены материалы, касающиеся ответственности за правонарушения в обозначенной сфере деятельности, в виде соответствующих извлечений из Кодекса Российской Федерации об административных правонарушениях (Приложение 3.1) и Уголовного кодекса (Приложение 3.2).

Следует отметить, что приведенные в данной работе более 1100 законодательных дефиниций дают возможность получить определенное представление о наиболее значительных правовых категориях и исключают возможность неоднозначного толкования правовых норм в сфере цифровой экономики и правового регулирования обеспечения ее информационной безопасности.

Хотелось бы также предположить, что данная работа может быть использована в интересах исключения повторов и приведения понятийного аппарата в стройное, непротиворечивое состояние при разработке новых документов, в частности, при разработке Информационного кодекса, о необходимости которого писал в вышеупомянутой статье В. Д. Зорькин.

Следует отметить, что данное издание явилось своеобразным продолжением работы автора над систематизацией понятийного аппарата. В частности, в 2006 г. был издан словарь-справочник «Жилищное и градостроительное законодательство»¹, а в 2009 г. — словарь-справочник по пожарной безопасности и чрезвычайным ситуациям².

Что касается данной работы, непосредственно касающейся темы цифровой экономики и правового регулирования обеспечения ее информационной безопасности, то она частично раскрыта автором в ряде таких работ, как «К вопросу о новых возможностях обеспечения государственных нужд в условиях цифровой экономики и пробле-

¹ Жилищное и градостроительное законодательство: словарь-справочник / В. П. Гринев. М.: ГроссМедиа, 2006. 160 с.

² Законодательство о пожарной безопасности и чрезвычайных ситуациях: словарь-справочник / В. П. Гринев. М.: ОАО ЦПП, 2009. 60 с.

мах правоприменения при переводе закупок в электронную форму»¹, «К вопросу о переводе публичных закупок в электронную форму»², «Государственное регулирование цифровой экономики»³, «Особенности закупочной деятельности в сфере обеспечения информационной безопасности: правовые аспекты»⁴.

Касательно предложенной редакции данного издания следует отметить, что оно может быть использовано слушателями консультационных семинаров в рамках дополнительного профессионального образования по вопросам цифровой экономики и правовому регулированию обеспечения ее информационной безопасности, представителями судейского сообщества, руководителями и специалистами органов МСУ, в том числе государственными гражданскими служащими в ходе обучения в рамках программ соответствующих курсов повышения квалификации в обозначенной сфере деятельности.

Автор выражает благодарность всем коллегам, сделавшим ряд полезных замечаний и предложений по формированию содержания этой работы и ее структуре, а также надеется, что она не только вызовет у читателя определенный интерес, но и послужит мотивирующим фактором для постановки перед автором ряда вопросов, которые могли бы быть учтены в последующей работе.

¹ Публичные закупки: проблемы правоприменения: материалы VI Международной научно-практической конференции (8 июня 2018 г., МГУ имени М. В. Ломоносова). М.: Юстицинформ, 2018. С. 50–62.

² Там же. С. 32–49.

³ *Гринев В. П.* Государственное регулирование цифровой экономики // Право и цифровая экономика. 2018. № 2. С. 15–22.

⁴ Публичные закупки: проблемы правоприменения: материалы VII Международной научно-практической конференции (13–14 июня 2019 г., МГУ имени М. В. Ломоносова). М.: Юстицинформ, 2019. С. 55–68.

1. ЦИФРОВАЯ ЭКОНОМИКА: НАСТОЯЩЕЕ И БУДУЩЕЕ

Говоря о цифровой экономике, ее настоящем и будущем, важно иметь в виду, что идея электронной (цифровой) экономики зародилась сравнительно недавно, а именно в середине 20 века, в частности, в 1995 году, когда американский информатик Николас Негропonte в своей книге «Being Digital» сформулировал концепцию электронной экономики, основанной на переходе человечества в своей хозяйственной деятельности от обработки атомов к обработке электронных битов¹.

Что касается настоящего и будущего цифровой экономики в Российской Федерации, то необходимо иметь в виду, что как программа «Цифровая экономика Российской Федерации»² (далее Программа) была утверждена 28 июля 2017 г. распоряжением Правительства РФ № 1632-р.

Важно отметить, что эта Программа была принята в целях реализации Стратегии развития информационного общества в РФ на 2017–2030 годы, утвержденной Указом Президента РФ от 9 мая 2017 г. № 203, в котором приводится следующее **определение цифровой экономики**: “**Цифровая экономика** — это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг”.

¹ *Nicholas Negroponte*. Being Digital. New York: Alfred A. Knopf. 1995. 243 p.; см. также: *Вайнан В. А.* Основы правового регулирования цифровой экономики // *Право и экономика*. 2017. № 11. С. 5–18.

² В утвержденном этим распоряжением варианте Программа существовала до 12 февраля 2019 г., т. е. до издания распоряжения Правительства РФ от 12 февраля 2019 г. № 195-р, в соответствии с которым данное распоряжение как НПА утратило силу.

Основная цель Программы заключалась в создании экосистемы цифровой экономики¹ РФ, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности и в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан, а также повышение конкурентоспособности на глобальном рынке как отдельных отраслей экономики РФ, так и экономики в целом.

В настоящее время координация деятельности по вопросам цифровой экономики осуществляется Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (далее — Комиссия), Положение о которой утверждено постановлением Правительства РФ от 7 сентября 2018 г. № 1065².

Необходимо отметить, что эта Комиссия была создана в результате преобразования Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, преобразованной в свою очередь на основании постановления Правительства РФ от 26 августа 2013 г. № 735³ из Правительственной комиссии по внедрению информационных технологий в деятельность государственных органов и органов МСУ, созданной в 2010 году в соответствии с постановлением Правительства РФ от 6 февраля 2010 г. № 60⁴.

Таким образом, можно констатировать тот факт, что Правительственная комиссия по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности своими корнями уходит в далекий 2010 год.

¹ Экосистема цифровой экономики — партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан — пункт «С» части 3 «Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

² Постановление Правительства РФ от 7 сентября 2018 г. № 1065 «О Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности» (вместе с Положением о Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности).

³ Там же.

⁴ Там же.

Важно отметить, что согласно пункту 1 Положения, утвержденного постановлением Правительства РФ от 7 сентября 2018 г. № 1065, Комиссия является координационным органом, образованным в целях обеспечения взаимодействия ФОИВ и органов исполнительной власти субъектов РФ по вопросам развития экосистем цифровой экономики и повышения уровня использования информационных технологий и связи в целях формирования в РФ информационного общества и электронного правительства.

В соответствии с пунктом 4 Положения в состав Комиссии в качестве ее рабочих органов входят президиум Комиссии и подкомиссия по цифровой экономике. При этом, как отмечено в пункте 6 Положения, президиум Комиссии выполняет функции проектного комитета национальной программы «Цифровая экономика Российской Федерации».

Основная задача президиума Комиссии, как сформулировано в пункте 8 Положения, является координация деятельности органов государственной власти на федеральном и региональном уровнях по ряду вопросов, касающихся сферы цифровой экономики, в частности:

а) определения единой государственной политики развития цифровых платформ в интересах отраслей экономики, в том числе государственного управления, здравоохранения, образования, промышленности, связи, сельского хозяйства, строительства, городского хозяйства, транспортной и энергетической инфраструктуры, финансовых услуг;

б) рассмотрения предложений по совершенствованию законодательства РФ для развития цифровых платформ в интересах отраслей экономики;

в) развития и использования информационных технологий и цифровых платформ, а также формирования современной информационной и телекоммуникационной инфраструктуры;

г) повышения эффективности бюджетных расходов на внедрение информационных технологий в деятельность органов государственной власти и их использование.

В настоящее время Программа имеет статус национального проекта, который называется «Национальная программа “Цифровая экономика Российской Федерации”» (далее — Проект), условное сокращенное название НП ЦЭ.

Следует отметить, что Паспорт Проекта НП ЦЭ утвержден 4 июня 2019 г. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол № 7¹.

¹ Необходимо отметить, что Совет при Президенте Российской Федерации по стратегическому развитию и национальным проектам согласно пункту 1 Указа Президента РФ от 19 июля 2018 г. № 444 «Об упорядочении деятельности сове-

Целями данного Проекта являются:

- увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте страны) не менее чем в три раза по сравнению с 2017 годом;
- создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств;
- использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями.

По состоянию на текущую дату НП ЦЭ «Цифровая экономика Российской Федерации» как национальная Программа включает в себя 6 нижепоименованных государственных программ, а именно: «Экономическое развитие и инновационная экономика»; «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан РФ»; «Научно-технологическое развитие РФ»; «Информационное общество»; «Развитие промышленности и повышение ее конкурентоспособности» и «Содействие занятости населения», а также одну государственную подпрограмму — «Информационное государство».

Необходимо отметить, что каждая из этих государственных программ и соответствующая подпрограмма реализуются в рамках одного или нескольких федеральных проектов¹, к которым относятся шесть таких проектов как: «Нормативное регулирование цифровой среды», «Информационная инфраструктура», «Цифровое государственное управление», «Информационная безопасность», «Кадры для цифровой экономики» и «Цифровые технологии».

При этом важно иметь в виду, что ответственность за реализацию каждого из этих федеральных проектов возложена, согласно пункту 2 постановления Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации», на соответствующие ФОИВ.

шательных и консультативных органов при Президенте Российской Федерации» (вместе с Положением о Совете при Президенте Российской Федерации по стратегическому развитию и национальным проектам) был преобразован из Совета при Президенте Российской Федерации по стратегическому развитию и приоритетным проектам.

¹ Федеральный проект Программы — проект, обеспечивающий достижение целей, целевых и дополнительных показателей, выполнение задач Программы, а также достижение иных целей и показателей, выполнение иных задач по поручению и указанию Президента РФ, поручению Председателя Правительства РФ, Правительства РФ, решениям Совета, президиума Совета, Комиссии, президиума Комиссии и поручению куратора Программы. Пункт 3 Положения — извлечение.

В частности, функции ФОИВ, ответственного за реализацию федеральных проектов «Нормативное регулирование цифровой среды» и «Кадры для цифровой экономики», возложены на Минэкономразвития России; а функции ФОИВ, ответственного за реализацию федеральных проектов, таких как: «Цифровые технологии», «Цифровое государственное управление», «Информационная инфраструктура» и «Информационная безопасность» — на Минкомсвязи России.

В рамках системного подхода, используемого в ходе проведения данного исследования, на рис. 1 представлена структура этого национального проекта, наименования входящих в него элементов и их связь с федеральными проектами.

На основе анализа приведенной на рис. 1 структурной схемы национального проекта «Национальная программа “Цифровая экономика Российской Федерации”» можно сделать вывод, что в наибольшем количестве государственных программ реализуется федеральный проект «Информационная безопасность», в частности, в рамках трех государственных программ, к которым относятся: «Информационное общество», «Научно-технологическое развитие РФ», «Развитие промышленности и повышение ее конкурентоспособности», а также государственной подпрограммы «Информационное государство».

Для сравнения можно отметить, что такой федеральный проект как «Цифровые технологии» реализуется в рамках двух государственных программ, в частности, «Информационное общество» и «Развитие промышленности и повышение ее конкурентоспособности», а также государственной подпрограммы «Информационное государство».

В рамках двух государственных программ, таких как «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан РФ» и «Содействие занятости населения» реализуется федеральный проект «Цифровое государственное управление».

А три таких федеральных проекта, в частности, «Нормативное регулирование цифровой среды», «Информационная инфраструктура» и «Кадры для цифровой экономики» реализуются в рамках одной из таких государственных программ как: «Экономическое развитие и инновационная экономика», «Обеспечение доступным и комфортным жильем и коммунальными услугами» и «Кадры для цифровой экономики» соответственно (см. рис. 1).

Важно при этом иметь в виду, что паспорта¹ всех этих шести федеральных проектов утверждены 28 мая 2019 г. президиумом Прави-

¹ Паспорт федерального проекта Программы — документ, включающий в себя наименование федерального проекта Программы, его цели и показатели, в том числе с указанием значений по субъектам РФ, методики расчета показателей, задачи и результаты, вехи, контрольные точки (события) и мероприятия, обеспечивающие достижение целей и показателей, сроки реализации и объемы финансового обеспече-

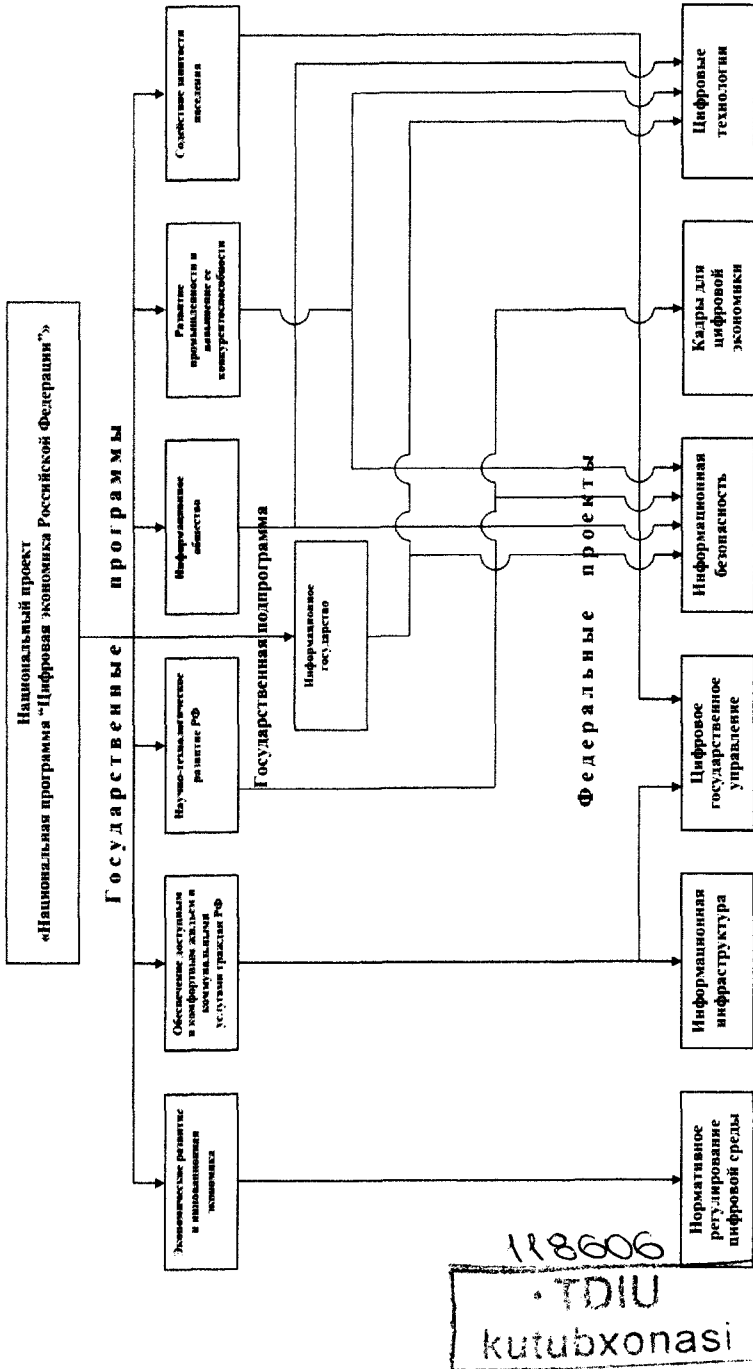


Рис. 1. Структурная схема национального проекта «Национальная программа «Цифровая экономика Российской Федерации»»

тельствственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол № 9).

В рамках проводимого исследования представляется целесообразным также отметить основные положения Паспортов каждого из шести вышеперечисленных федеральных проектов.

В частности, как указано в паспорте федерального проекта «**Информационная безопасность**» (условно именуемым в рамках настоящего исследования «первым») его реализация должна «способствовать достижению состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие РФ в условиях цифровой экономики, а также создание условий для лидирующих позиций РФ в области экспорта услуг и технологий информационной безопасности, учет национальных интересов в международных документах по вопросам информационной безопасности».

Ключевые направления, реализуемые в рамках мероприятий по данному проекту, заключаются в повышении уровня информационной безопасности и устойчивости сетей связи общего пользования; создании новых сервисов (услуг) для граждан, гарантирующих защиту их персональных данных; профилактике и выявлении правонарушений с использованием информационных технологий против общества и бизнеса; разработке новых механизмов поддержки отечественных разработчиков программного обеспечения и компьютерного оборудования в сфере информационной безопасности.

В рамках проведения работ по этим направлениям планируется проведение ряда мероприятий, в частности, таких как:

1. Введение в эксплуатацию системы обеспечения целостности, устойчивости, безопасности сети «Интернет», создание Центра мониторинга и управления сетями связи общего пользования.

2. Реализацию пилотных проектов по созданию государственных информационных систем (далее — ГИС) с использованием технологий распределенных реестров, технологий искусственного интеллекта, анализа данных.

ния федерального проекта Программы, информацию о ФОИВ, ответственном за реализацию федерального проекта Программы (далее — ответственный федеральный орган исполнительной власти), центре компетенций федерального проекта Программы (далее — центр компетенций), рабочей группе федерального проекта Программы (далее — рабочая группа) и руководителе федерального проекта Программы, а также иные сведения.

3. Создание системы мер поддержки для отечественного программного обеспечения и оборудования при госзакупках.
4. Создание киберполигона для обучения практикам обеспечения безопасности.
5. Реализацию мер поддержки экспорта информационных технологий и патентования за рубежом.
6. Создание ресурса для взаимодействия граждан и правоохранительных органов в интересах информирования о нарушениях в цифровой среде.
7. Создание защищенной среды взаимодействия двойного назначения на базе отечественных технологий для работы в стандарте LTE-450 для нужд МВД России, МЧС России, Росгвардии.
8. Оказание финансовой поддержке субъектам РФ по реализации требований федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры»¹, созданию типовых решений.
9. Разработка технологических решений по защите аппаратно-программных комплексов транспортной инфраструктуры.
10. Создание программно-аппаратные решений по повышению устойчивости и безопасности отечественной инфраструктуры теле радиовещания.
11. Реализацию комплексной поддержки разработки отечественного программного обеспечения.
12. Создание общедоступного антивирусного мультисканера.
13. Обеспечение безопасности значимых платежных систем, в том числе с использованием российских криптографических средств.

¹ Справка. В соответствии с определениями, данными в статье 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в частности, с пунктом 6 «критическая информационная инфраструктура» — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов; при этом согласно пункту 7 этой статьи «объекты критической информационной инфраструктуры» — это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры; что касается субъектов критической информационной инфраструктуры — то это, в соответствии с пунктом 8 статьи 2, государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

14. Реализацию программы повышения квалификации педагогов, осуществляющих подготовку специалистов по информационной безопасности.

15. Реализацию системы повышения грамотности и практико-ориентированной подготовки в области кибербезопасности.

Важно иметь в виду, что обеспечение информационной безопасности тесно интегрировано с другими федеральными проектами НП ЦЭ, а результаты его реализации закладывают основу для цифровой трансформации социальных и экономических процессов.

При этом необходимо иметь в виду, что началу реализации этого федерального проекта предшествовало выполнение в теперь уже почти далеком 2018 году комплекса мероприятий, предусматривающих:

– проведение комплексного анализа мировых тенденций развития информационных технологий в области информационной безопасности, определение показателей развития информационно-телекоммуникационных технологий, включая их целевые значения;

– проведение комплексного анализа и оценки потенциальных уязвимостей, угроз и рисков информационной безопасности, характерных для систем, реализованных на технологиях облачных, туманных, квантовых, виртуальных, искусственного интеллекта и дополненной реальности, технологий распределенного реестра, а также сравнительная оценка экономического эффекта от внедрения облачных, туманных, квантовых технологий, систем виртуальной и дополненной реальности, технологий распределенного реестра и технологий искусственного интеллекта;

– проведение анализа устойчивости, рисков и угроз безопасного функционирования единой сети электросвязи, а также элементов действующей инфраструктуры российского сегмента сети Интернет на территории России;

– подготовку дорожной карты разработки стандартов обеспечения информационной безопасности;

– разработку концепции, определяющей приоритетные направления разработки отечественного общесистемного и прикладного программного обеспечения, включая вопросы совместимости;

– разработку требований по использованию преимущественно отечественного компьютерного, серверного и телекоммуникационного оборудования на объектах инфраструктуры обработки данных.

Важно отметить, что на основании документа, который называется «План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации»¹ соисполнителями, участвующим в реализации этого проекта, поми-

¹ Утвержден Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18 декабря 2017 г. № 2).

мо федеральных министерств в лице Минобрнауки, Минпромторга, Минтруда, Минфина, Минэкономразвития, МВД, МИД, рассматриваются также Банк России, ФСБ, ФСО, ФСТЭК, ФНС, Росаккредитация, Роскомнадзор, Росстандарт, Академия криптографии РФ, АНО «Центр компетенций по импортозамещению в сфере ИКТ», АНО «Цифровая экономика», ГК «Внешэкономбанк», ООО «ВЭБ Инновации», ПАО «Ростелеком», ПАО «Гипросвязь», АО «Российская венчурная компания», АО «Российский экспортный центр», АО «Российское агентство по страхованию экспортных кредитов и инвестиций», Евразийская экономическая комиссия, Российский фонд развития информационных технологий, Фонд развития Интернет инициатив, Фонд развития промышленности, Фонд «Сколково», Фонд содействия инновациям, Федеральное учебно-методическое объединение в системе среднего профессионального образования по укрупненной группе профессий, специальностей «Информационная безопасность», Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей и направлений подготовки «Информационная безопасность» и др.

Что касается показателей, по которым можно будет оценивать выполнение соисполнителями работ по направлению «Информационная безопасность», следует отметить, что ими являются:

- доля внутреннего сетевого трафика Российского сегмента сети «Интернет», маршрутизируемая через иностранные серверы;
- стоимостная доля закупаемого и (или) арендуемого ФОИВ, органами исполнительной власти субъектов, государственными корпорациями, компаниями с государственным участием иностранного программного обеспечения;
- доля субъектов информационного взаимодействия (органов государственной власти и МСУ, компаний с государственным участием и (или) относящихся к информационной инфраструктуре), использующих стандарты безопасного информационного взаимодействия в киберфизических системах;
- доля субъектов информационного взаимодействия (органов государственной власти и МСУ, компаний с государственным участием и (или) относящихся к информационной инфраструктуре), использующих стандарты безопасного информационного взаимодействия в части интернета вещей;
- доля граждан, повысивших грамотность в сфере информационной безопасности, медиапотребления и использования интернет-сервисов;
- запуск в эксплуатацию информационных и технических ресурсов, предусмотренных подпрограммой, доля от общего числа;
- принятие стандартов, регламентов и типовых форм, предусмотренных подпрограммой, доля от общего числа.

Показателями и индикаторами программы, на которые оказывает влияние выполнение плана мероприятий, также является средний срок простоя государственных информационных систем в результате компьютерных атак, измеряемый в часах.

На год окончания периода реализации плана мероприятий по этому направлению ожидается достижение целевых значений информационной безопасности на сетях связи и функционирования российского сегмента сети «Интернет»; создание системы стимулов для приобретения и использования компьютерного, серверного и телекоммуникационного оборудования российского производства, национального и региональных центров реагирования на компьютерные инциденты, а также механизмов стимулирования использования отечественного программного обеспечения всеми участниками информационного взаимодействия; принятие национальных стандартов киберфизических систем, включая интернет вещей; обеспечение контроля обработки и доступа к персональным данным, большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации. Кроме того, должна быть разработана система мер поддержки российских производителей продуктов и услуг ИКТ, осуществляющих патентование продуктов за рубежом.

При этом также необходимо иметь в виду, что основной его целью является формирование комплексного законодательного регулирования отношений, возникающих в связи с развитием цифровой экономики, а также новой регуляторной среды, обеспечивающей благоприятный правовой режим для возникновения и развития современных технологий в интересах осуществления экономической деятельности, связанной с их использованием. В рамках реализации этого проекта предполагается создание постоянно действующего механизма управления изменениями и компетенциями (знаниями) в области регулирования цифровой экономики, снятие ключевых правовых ограничений и создание отдельных правовых институтов, направленных на решение первоочередных задач ее формирования. Кроме того, планируется принятие мер, направленных на стимулирование экономической деятельности, связанной с использованием современных технологий, сбором и использованием данных, а также формирование политики по развитию цифровой экономики на территории Евразийского экономического союза, гармонизации подходов к нормативному правовому регулированию, способствующих развитию цифровой экономики на пространстве Евразийского экономического союза.

Что касается паспорта второго из шести вышеперечисленных федеральных проектов, в частности, федерального проекта «Нормативное регулирование цифровой среды» то в нем указано, что он призван создать систему правового регулирования цифровой экономики,

основанную на гибком подходе в каждой сфере, а также внедрение гражданского оборота на базе цифровых технологий.

При этом отмечается, что планируемые показатели проекта должны достигаться путем функционирования сложившейся системы управления НП ЦЭ, определенной постановлением Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации».

В соответствии с данной системой управления НП ЦЭ важная роль в процессах нормативного регулирования цифровой экономики отведена бизнесу как на стадии разработки нормативных правовых актов, так и на всех последующих стадиях: согласование с ФОИВ, обсуждение в Правительстве РФ, получение заключения Государственно-правового управления Президента России и иных органов, принятие Правительством РФ, Государственной Думой РФ, Советом Федерации Российской Федерации.

Роль бизнеса заключается в посильном выявлении регуляторных барьеров, разработке управленческих и регуляторных решений, оценке предлагаемых решений.

В качестве соисполнителей в реализации этого проекта предполагается участие таких федеральных министерств как Минкомсвязь, Минюст, Минкультуры, Минобрнауки, Минпромторг, Минтранс, Минтруд, Минфин, Минздрав, а также Росаккредитация, Росархив, Роспатент, Роспотребнадзор, Росстандарт, Росстат, Россвязь, Роструд, Росфинмониторинг, ФАС, ФНС, ФСБ, ФСТЭК, Верховный Суд РФ, Евразийская экономическая комиссия, Банк России, Фонд «Сколково», АНО «Аналитический центр при Правительстве Российской Федерации», Пенсионный фонд РФ, Федеральная нотариальная палата, Фонд социального страхования РФ, Экспертный совет при Правительстве РФ, Российский союз промышленников и предпринимателей, Федеральный фонд обязательного медицинского страхования, Федерация независимых профсоюзов России, Фонд развития интернет-инициатив, ПАО «ВымпелКом», ПАО «МегаФон», ПАО «МТС», ПАО «Ростелеком», ПАО «Сбербанк», ПАО «Северсталь», ПАО «Объединенная авиастроительная корпорация», ОАО «Российские железные дороги», ОАО «Т-Платформы», ГК «Росатом», ГК «Ростех», Ассоциация «ФинТех», Российская академия народного хозяйства и государственной службы при Президенте РФ, Институт права и развития ВШЭ — Сколково, Московский государственный институт международных отношений, Московский государственный университет имени М. В. Ломоносова, Московский физико-технический институт, Высшая школа экономики, ФГБНУ «Исследовательский центр частного права имени С. С. Алексеева при Президенте РФ», ФГУП «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении», Институт иссле-

дований интернета, Институт развития информационного общества, Ассоциация участников рынка интернета вещей, Российская ассоциация электронных коммуникаций, АНО «Агентство по технологическому развитию», АНО «Центр международных и сравнительно-правовых исследований», АНО «Центр исследований в сфере экономики и права», АНО «Центр международных и сравнительно-правовых исследований», АНО «Научно-методический центр медиации и права», АНО «Робоправо», АНО «Центр компетенций по импортозамещению в сфере ИКТ», Сколковский институт науки и технологий, АО «Киви», АО «Российская венчурная компания», Адвокатское бюро «Егоров, Пугинский, Афанасьев и партнеры», Национальный совет финансового рынка, НП «Национальная организация медиаторов», ООО «Яндекс», ООО «Дентонс Юроп», ООО «Пепеляев Групп», ООО «Симплер», ООО «Таможенно-Брокерский Центр», ЦЭФК Групп; ООО «Юридическая фирма «Косенков и Суворов», «1С», АВВУУ, Компания Preferentum, Технический комитет 194 «Кибер-физические системы», Медиа-коммуникационный союз, рабочие группы по направлениям АНО «Цифровая экономика», Комитет по цифровой повестке Делового совета ЕАЭС и др.

Учитывая необходимость нормативно-правовой регламентации большинства мероприятий, которые планируется реализовать в целях достижения поставленных целей в рамках базовых и прикладных направлений развития цифровой экономики, при разработке и реализации концепций первоочередных, среднесрочных и комплексных мер по совершенствованию правового регулирования цифровой экономики в рамках направления по нормативному регулированию предполагается в полной мере учитывать предложения по нормативно-правовому регулированию иных базовых и прикладных направлений, что предполагает тесное взаимодействие создаваемых по каждому направлению центров компетенций с центром компетенций, обеспечивающим мониторинг и совершенствование правового регулирования цифровой экономики.

В результате реализации плана мероприятий по этому направлению должны быть обеспечены правовые условия для формирования единой цифровой среды доверия, в т. ч. для сбора, хранения и обработки данных, а также для внедрения и использования инновационных технологий на финансовом рынке. Кроме того, должны быть созданы правовые условия для формирования сферы электронного гражданского оборота, сформированы правовые условия для наиболее эффективного использования результатов интеллектуальной деятельности в условиях цифровой экономики, в т. ч. в сфере судопроизводства и нотариата, а также условия для внедрения новых правил сбора отчетности, в том числе статистической информации. В этот перечень мероприятий входит также определение первоочередных базовых понятий и институтов, необходимых для формирования законодатель-

ства в сфере киберфизических систем (далее — КФС) и искусственно-го интеллекта, а также принятие нормативных правовых актов в целях стимулирования развития цифровой экономики.

В этой связи необходимо отметить, что в рамках реализации этого плана предусмотрено более 20 мероприятий, включающих в себя разработку федеральных законов, технических заданий и национальных стандартов.

С учетом того, что в ходе реализации плана мероприятий по направлению «Нормативное регулирование» должен быть создан постоянно действующий механизм управления изменениями и компетенциями (знаниями) в области регулирования цифровой экономики важно иметь в виду, что для его создания планируется разработать концепцию комплексного регулирования отношений, возникающих в связи с развитием цифровой экономики на основе шести технических заданий.

В этой связи представляет определенный научный интерес более подробный анализ содержания этих технических заданий и описание ожидаемых результатов их выполнения.

Условно первым техническим заданием можно считать техническое задание на проведение исследований возможности перевода норм права в машиночитаемый вид и автоматизации их исполнения, а также проведение исследований в сфере разработки языка и инструментов для описания самоисполняемых контрактов.

В ходе проведения исследований в соответствии с этим техническим заданием планируется выявить **способы и инструменты формирования машиночитаемого языка**, предназначенного для описания самоисполняемых контрактов, а также содержащего формы и инструменты общения и конкретизации норм права.

Кроме того, должен быть проведен анализ областей права, в которых возможно машиночитаемое описание норм, и **определены ограничения применения машиночитаемых норм и элементов контрактов**.

Также должна быть проведена классификация условий сделок и административных регламентов, принципиально допускающих автоматическое исполнение, и определены пределы воздействия на юридические и физические лица, которое допускает принятие автоматических решений.

В качестве ожидаемого результата выполнения этого технического задания можно констатировать факт **проведения анализа необходимости разработки правовых оснований для создания и функционирования цифровой платформы с искусственным интеллектом для анализа содержания НПА, осуществления поиска по ним, проверки на избыточность и непротиворечивость**.

По результатам выполнения этого технического задания также должны быть определены границы применимости машиночитаемого

и алгоритмического языка в самоисполняемых контрактах и автоматизированных нормах права в целях сокращения временных издержек на поиск и анализ НПА, повышения точности выборки, в том числе при определении взаимосвязанных нормативных актов для внесения полных изменений при разработке новых проектов, создания инструментария эффективного межведомственного согласования и общественного обсуждения проектов актов, реализации возможности автоматической проверки корректности и непротиворечивости данных между документами.

Результатом выполнения технического задания является также оценка возможности применения примерных условий договоров, предусматривающих возможность самоисполнения соглашения и автоматического третейского рассмотрения возникающих споров.

Второе **техническое задание** направлено на проведение исследования по формированию единого цифрового пространства с учетом правового регулирования применения искусственного интеллекта для целей социально-экономического планирования.

К ожидаемым результатам выполнения этого технического задания относятся следующие положения:

- проведен анализ возможности формирования единого цифрового пространства на основе информации, которая учитывается уже созданными ГИС, через систему реестров с распределенным доступом различных заинтересованных субъектов;
- определен подход, при котором действующие и планируемые к внедрению ГИС удовлетворяют набору финансово-технических и архитектурных характеристик, позволяющих в дальнейшем использовать их как системные модули в парадигме цифровой экономики;
- определены правовые основания для создания, функционирования и развития цифровой комплексной платформы с искусственным интеллектом для целей социально-экономического планирования и обеспечения внутренней и внешней электронной торговли на основе цифрового доверия;
- подготовлен и рассмотрен Рабочими группами по направлениям «Нормативное регулирование» и «Информационная инфраструктура» АНО «Цифровая экономика» анализ возможных развилок по созданию комплексной цифровой платформы с искусственным интеллектом, а также анализ содержания действующих НПА на предмет внесения в них изменений, связанных с ее созданием;
- определен режим электронного (цифрового) резидентства для компаний;
- определен переход от регистрации организаций в уведомительной электронной форме через портал госуслуг к альтернативному

формату электронного (цифрового) резидентства для компаний, включая как возможность создать компанию дистанционно, так и возможность управлять компанией полностью дистанционно;

- определены случаи, при которых допускается замена «физического» адреса организации виртуальным («цифровым» офисом).

Еще одно техническое задание (условно третье) связано с разработкой направлений среднесрочного регулирования медиакоммуникационной отрасли.

Ожидаемые результаты по результатам выполнения этого (условно третьего) технического задания сводятся к тому, что в рамках разработанных направлений среднесрочного регулирования медиакоммуникационной отрасли сформулированы предложения по ее регулированию, включая деятельность операторов связи, организаторов распространения информации, масс-медиа, направленном на оборот данных (за исключением промышленных), услуг, инфраструктуры для их сбора, хранения, а также защиты прав собственности и создания условий для их оборота с целью стимулирования цифровой трансформации бизнеса, защиты интересов потребителей и государства («Инфокодекс»).

Формирование четвертого технического задания связано с проведением исследования в области развития законодательства о робототехнике и киберфизических системах (далее КФС) в части, в том числе определения понятия киберфизических систем, порядка ввода их в эксплуатацию и гражданский оборот, определения ответственности.

В качестве ожидаемых предполагаются следующие результаты:

- проведен анализ, сформулированы предложения по установлению иерархии правовых понятий в сфере создания, использования и распространения КФС, классификация КФС, основной состав прав и обязанностей лиц, участвующих в отношениях, связанных с применением КФС;
- сформированы предложения по определению ответственности в сфере использования КФС, системы страхования рисков, связанных с использованием КФС;
- сформированы предложения по определению порядка использования персональных данных различными формами КФС (чат-ботами, устройствами в интернете вещей и т. д.), деятельности по сбору, передаче, хранению, обработке и доступу к данным, генерируемым в связи с использованием информационных технологий физическими и юридическими лицами, в том числе в части сбора таких данных в зависимости от волеизъявления субъектов;
- сформированы предложения по определению условий по обработке и коммерческому использованию данных, генерируемых в связи с использованием информационных технологий физи-

ческими и юридическими лицами, механизмов сбора и использования больших массивов данных;

- сформированы предложения по определению порядка раскрытия информации, режиму открытых данных, принципам раскрытия данных по умолчанию, порядка обеспечения сохранности сведений, охраняемых законом (тайна связи, тайна личной жизни и т. п.), обрабатываемых при использовании КФС;
- сформированы предложения по определению порядка использования отдельных категорий сервисных роботов, минимальных требований к введению в эксплуатацию отдельных категорий роботов и роботизированных устройств, направленных на обеспечение безопасности и контролируемости устройств;
- сформированы предложения по определению требований к используемым датчикам, средствам измерений и измерительным системам с учетом положений законодательства об обеспечении единства измерений.

Пятое техническое задание направлено на разработку концепции комплексного правового регулирования отношений, возникающих в связи с развитием цифровой экономики.

По результатам выполнения этого технического задания ожидается получить следующие результаты:

- осуществлена гармонизация терминологии, используемой в различных НПА;
- сформулированы основные направления развития законодательства в целях его адаптации к цифровой экономике;
- сделаны предложения по комплексному регулированию различными отраслями законодательства (гражданским, административным, уголовным, образовательным, трудовым и т. п.) направлений цифровой экономики в следующих областях: оборота данных; искусственного интеллекта; технологии децентрализованного ведения реестров с учетом предложений, сформированных в рамках «дорожных карт» Национальной технологической инициативы, Стратегии научно-технологического развития и др.;
- созданы специальные правовые режимы для организаций, ведущих деятельность в приоритетных видах деятельности цифровой экономики и (или) имеющих определенный уровень информатизации процессов;
- внедрены инструменты стимулирования развития цифровой экономики;
- сформулированы принципы и подходы к трансграничному регулированию отношений в цифровой среде;
- представлен перечень мер по доведению информации о проводимых изменениях до целевых аудиторий, в том числе с помощью средств массовой информации;

- реализован перевод в электронный вид осуществления контрольно-надзорных функций, а также функций, связанных с обжалованием действий и решений органов контроля, привлечением к административной ответственности подконтрольных субъектов;
- сформулированы предложения по комплексному регулированию робототехники и КФС (в том числе определения понятия КФС, порядка ввода их в эксплуатацию и гражданский оборот, определение ответственности);
- определены подходы к правовому регулированию обработки больших объемов данных, в том числе геолокационных и личных данных граждан, включая механизмы их правовой защиты, правил и механизмов обмена данными между субъектами цифровой экономики, недискриминационного доступа к ним, ответственность за несанкционированный доступ, классификация данных с учетом требований по доступности и информационной безопасности, определен подход к созданию системы управления данными, в том числе исходя из источников и средств генерации данных (человек, машина);
- сформирован перечень стандартов по сквозным технологиям, определены возможности использования сквозных технологий в нормативном регулировании цифровой экономики;
- сформированы подходы, определены этапы и сроки по переводу в электронный вид кадрового документооборота, в том числе с учетом необходимости согласования интересов сторон социального партнерства и решения задач развития цифровой экономики;
- разработаны предложения по внедрению автоматизированных систем на рабочих местах с вредными и (или) опасными условиями труда в целях исключения вредного воздействия на работников производственных факторов, а также по актуализации тарифов страховых взносов, уплачиваемых работодателями за работников на таких рабочих местах.

И, наконец, шестое техническое задание — это задание связано с разработкой концепции организации процесса управления изменениями в области цифровой экономики.

В соответствии с разработанной концепцией организации процесса управления изменениями в области цифровой экономики должны быть осуществлены следующие мероприятия:

- определена организационная система сбора информации о качестве регулирования цифровой экономики и разработки, согласования и принятия соответствующих НПА;
- сформированы предложения по созданию специального платформенного решения (среды взаимодействия) для органов госу-

дарственной власти, а также иных заинтересованных лиц, участвующих в процессе подготовки НПА, в цифровом формате с использованием передовых технологий обмена информацией;

- внедрен механизм регулярного сбора сведений о международном опыте регулирования отношений в сфере цифровой экономики, обмена информацией и опытом с международными центрами и экспертными площадками по вопросам цифровой экономики, развития компетенций по вопросам регулирования цифровой экономики;
- разработаны методические документы для развития компетенций и условий для подготовки юристов и государственных гражданских служащих в сфере регулирования цифровой экономики.

Федеральный проект «Информационная инфраструктура» (третий по счету) направлен на решение задач по созданию и развитию конкурентоспособной информационной инфраструктуры на территории РФ.

Его основной задачей является создание глобальной инфраструктуры с целью обеспечения современными цифровыми услугами населения РФ и ключевых социально-значимых объектов инфраструктуры на основе отечественных разработок.

Реализацию поставленной задачи планируется осуществлять в рамках следующих ключевых направлений, в частности:

- создание глобальной конкурентоспособной инфраструктуры передачи данных, их обработки и хранения;
- создание глобальной конкурентоспособной инфраструктуры функционирования цифровых платформ работы с данными для обеспечения потребностей граждан, бизнеса и власти;
- создание экосистемы внедрения цифровых технологий в строительстве и управлении городским хозяйством «Умный город».

Четвертый из вышеперечисленных проектов, в частности, федеральный проект «**Кадры для цифровой экономики**» разработан для обеспечения экономики достаточным количеством человеческих ресурсов, обладающих компетенциями, необходимыми для нового века цифровых технологий и экономики знаний и данных и направлен на обеспечение подготовки высококвалифицированных кадров.

Его разработка, как и все вышеперечисленные проекты, отвечает целям и задачам майских Указов Президента РФ, в частности, Указа Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и «Стратегии развития информационного общества в Российской Федерации на 2017–2030», утвержденной Указом Президента РФ от 9 мая 2017 г. № 203.

Важно отметить, что для достижения этих целей и решения соответствующих задач в рамках этого федерального проекта должны проводиться работы по следующим направлениям:

- развитию человеческого потенциала;
- формированию информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений;
- использованию и развитию различных образовательных технологий, в том числе дистанционного, электронного обучения, при реализации образовательных программ;
- осуществлению разработки и реализации партнерских программ образовательных организаций высшего образования и российских высокотехнологических организаций, в том числе по вопросу совершенствования образовательных программ;
- развитию технологий электронного взаимодействия граждан, организаций, государственных органов, органов МСУ наряду с сохранением возможности взаимодействия граждан с указанными организациями и органами без применения информационных технологий;
- стимулирование российских организаций в целях обеспечения работникам условий для дистанционной занятости;
- создание основанных на информационных и коммуникационных технологиях систем управления и мониторинга во всех сферах общественной жизни.

При этом ключевыми направлениями данного федерального проекта являются обеспечение цифровой экономики компетентными кадрами; поддержка талантливых школьников и студентов в области математики, информатики и технологий цифровой экономики; содействие гражданам в освоении цифровой грамотности и компетенций цифровой экономики.

Пятый в этом списке — федеральный проект «**Цифровые технологии**».

Ключевая цель этого проекта — обеспечение технологической независимости государства, возможности коммерциализации отечественных исследований и разработок, а также ускорение технологического развития российских компаний и обеспечение конкурентоспособности разрабатываемых ими продуктов и решений на глобальном рынке.

Основными задачами проекта являются:

- формирование экосистемы поддержки цифровой экономики, в том числе необходимых механизмов и инструментов развития цифровых технологий в РФ;
- построение эффективного взаимодействия между государством, научными организациями, российскими компаниями-лидерами цифровой экономики, институтами развития, государственными корпорациями и т. п.

Как указано в Паспорте этого проекта данные задачи можно назвать системообразующими, в связи с тем, что скорость технологического развития государств и их перехода на цифровую экономику

становится определяющим фактором лидерства на международном рынке, как в сфере информационных технологий, так и в классических отраслях экономики.

Важно отметить, что данный федеральный проект включает в себя несколько смысловых блоков, которые в совокупности позволяют обеспечить планомерное развитие цифровых технологий.

В частности, базовым уровнем для формирования экосистемы является определение текущего состояния развития цифровых технологий и системное планирование траектории развития.

С этой целью в федеральном проекте предусмотрены следующие направления аналитической работы:

- анализ потребности секторов экономики в применении решений на основе сквозных цифровых технологий¹ (далее — СЦТ) и связанных с ними исследованиях и разработках;

- анализ уровня развития исследовательских компетенций, научных и технологических заделов отечественных компаний и организаций по СЦТ;

- разработка системы показателей Национального индекса развития цифровой экономики РФ (далее — НИРЦЭ РФ).

Результаты указанных исследований планируется размещать в открытом доступе в сети Интернет на едином информационном портале

¹ Сквозные технологии — технологии, которые примеряются во всех отраслях народного хозяйства, это цифровые, квантовые, робототехника, нейротехнологии и так далее — Послание Президента РФ Федеральному Собранию от 1 декабря 2016 г. Основными «сквозными» цифровыми технологиями, которые входят в рамки НП ЦЭ, являются большие данные; нейротехнологии и искусственный интеллект; системы распределенного реестра; квантовые технологии; новые производственные технологии; промышленный интернет; компоненты робототехники и сенсорики; технологии беспроводной связи; технологии виртуальной и дополненной реальности. При этом в ходе реализации плана мероприятий по этому направлению предполагается, что должны быть совершены следующие действия, в частности, определены сектора экономики с наиболее высоким потенциалом коммерциализации решений на базе «сквозных» технологий в области цифровой экономики; запущена цифровая трансформация секторов российской экономики и отдельных ее субъектов; сформирован спрос на продукцию российского происхождения в части «сквозных» технологий со стороны широкого круга субъектов экономики; обеспечена защита технологических решений иностранного происхождения, необходимых для развития в России приоритетных «сквозных» технологий; разработана и утверждена программа деятельности отобранных организаций-лидеров; сформированы условия для развития МНТС организаций-лидеров по приоритетным направлениям «сквозных» технологий цифровой экономики и начата реализация проектов в рамках МНТС; создана экосистема, стимулирующая развитие компаний-лидеров на рынках цифровой экономики; интенсифицирован спрос на исследования и разработки в области «сквозных» технологий цифровой экономики; создано не менее трех аспирантских и магистерских школ по каждому направлению «сквозных» технологий на базе ведущих вузов и научных организаций.

поддержки развития СЦТ, создание которого также запланировано в рамках этого федерального проекта.

На основании исследований планируется сформировать несколько дорожных карт по направлениям СЦТ, которые будут содержать в себе анализ, как существующих технологических заделов, так и сильных и слабых сторон каждой из технологий и субтехнологий, а также определять траекторию развития.

Параллельно с формированием дорожных карт, одной из главных задач федерального проекта является определение лидирующих исследовательских центров (далее — ЛИЦ), которые смогут создавать консорциумы с компаниями-лидерами по направлениям СЦТ, что позволит реализовывать актуальные для рынка и необходимые бизнесу исследования и разработки.

По итогам выполнения данной задачи к 2020 году должны быть определены не менее 18 ЛИЦ по направлениям развития СЦТ (не менее 9 ЛИЦ в 2019 году).

Еще одним блоком федерального проекта является формирование мер поддержки, в частности поддержки проектов по преобразованию приоритетных отраслей экономики на основе внедрения отечественных продуктов, сервисов и платформенных решений, созданных на баз СЦТ. Поддержка этих проектов предполагается в форме субсидий.

Обязательным условием получения государственной поддержки будет являться соответствие проектов приоритетам, установленным дорожными картами. Данная мера позволит сконцентрировать ресурсы на наиболее перспективных технологичных проектах.

Еще одним условием предоставления субсидий предполагается софинансирование реализуемых проектов за счет внебюджетных источников в объеме не менее 50%, что позволит значительно снизить риск завышения стоимости и нерезализуемости проектов.

Проектом «Цифровые технологии» также предусмотрено формирование различных мер поддержки, таких как:

- развитие льготного кредитования и государственных гарантий совместно с ВЭБ.РФ и другими кредитными организациями. Российским кредитным организациям, а также организациям ВЭБ.РФ, планируется предоставлять субсидии на возмещение недополученных ими доходов по кредитам с льготной процентной ставкой, выданным организациям на реализацию проектов в приоритетных отраслях, развития цифровой экономики;

- поддержка региональных проектов по внедрению отечественных продуктов, сервисов и платформенных решений, созданных на базе СЦТ;

- поддержка отраслевых проектов по внедрению СЦТ в приоритетных отраслях экономики совместно с профильными министерствами;

- поддержка российских компаний-лидеров, разрабатывающих продукты, сервисы и платформенные решения на базе цифровых технологий на основе отечественных разработок;

- поддержка разработки и внедрения продуктов, сервисов и платформенных решений в целях повышения доступности российского программного обеспечения и программно-аппаратных комплексов;

- поддержка проектов малых предприятий по разработке, применению и коммерциализации СЦТ;

- поддержка реализации программ деятельности ЛИЦ по направлениям развития СЦТ, в том числе в интересах российских компаний-лидеров цифровой экономики.

Необходимо отметить, что в процессе формирования данной системы мер поддержки, большое внимание должно уделяться фокусировке институтов развития в сфере цифровых технологий.

Помимо указанных мер поддержки, федеральный проект подразумевает стимулирование внутреннего спроса на цифровые технологии.

С целью запуска такого механизма предусмотрены задачи по цифровой трансформации компаний лидеров и государственных корпораций.

Для повышения эффективности трансформации и сокращения ее сроков федеральным проектом предусмотрена разработка концепции цифровой трансформации, создание типовой модели трансформации, а также формирование банка лучших международных и российских практик.

Помимо этого, планируется формирование соответствующих ключевых показателей эффективности (KPI — Key Performance Indicators), которые позволят оценить прогресс в заданном направлении.

Так, предполагается, что уже к концу 2021 года будут утверждены не менее 30 стратегий цифровой трансформации государственных корпораций и компаний с государственным участием и назначено не менее 30 заместителей высших должностных лиц в государственных корпорациях и компаниях с государственным участием, реализующих стратегии цифровой трансформации (Chief Digital Officer).

Шестой по порядку, но не по значимости — это федеральный проект «**Цифровое государственное управление**».

Необходимо отметить, что этот федеральный проект оказывает прямое влияние на обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере за счет использования цифровых технологий и платформенных решений в сферах государственного управления и оказания государственных услуг, в том числе в интересах населения и субъектов малого и среднего предпринимательства, включая индивидуальных предпринимателей, а также обеспечивает качественное улучшение ряда показателей, отражающих рост национальной экономики, и социальной сферы.

Реализация этого проекта должна позволить осуществить окончательный переход на электронное взаимодействие граждан и организаций с государством, а также сделать указанное взаимодействие более удобным.

В частности, планируется реализовать реестровую модель, экстерриториальность и механизм проактивности при предоставлении государственных и муниципальных услуг в электронной форме, сформировать механизмы обратной связи с гражданами и организациями, при этом юридически значимый документооборот должен стать по преимуществу электронным.

При этом предполагается проведение ряда обеспечивающих мероприятий, в том числе обеспечение предоставления государственных и негосударственных услуг и сервисов в цифровом виде в соответствии с прогрессирующими потребностями современного общества в условиях становления цифровой экономики; обеспечение цифровой трансформации органов государственной власти и органов МСУ, направленной на повышение качества осуществления возложенных на них функций, уменьшения издержек при их осуществлении, создание системы управления данными, в том числе сбора, хранения, обработки и распространения данных; обеспечение эксплуатации и развития инфраструктуры электронного правительства.

Также предполагается преобразование институциональных и организационных механизмов взаимодействия РФ и Евразийской экономической комиссии в рамках реализации цифровой повестки ЕАЭС.

Важно отметить, что успешная реализация этих мероприятий должна позволить сформировать устойчивую информационно-коммуникационную инфраструктуру государственных и муниципальных органов, в том числе обеспечить бесперебойное функционирование критически важных для граждан и организаций государственных сервисов, в том числе сервисов удаленной идентификации, информационного обмена, хранения юридически значимой информации, цифровой платформы предоставления государственных и муниципальных услуг.

В рамках рассмотрения вопроса о настоящем и будущем Цифровой экономики РФ представляет также определенный научный интерес анализ взаимосвязи входящих в национальный проект «Национальная программа “Цифровая экономика Российской Федерации”» государственных программ и соответствующих подпрограмм с шестью вышеперечисленными федеральными проектами на основе данных, представленных в табл. 1, к которым относится информация об ответственном исполнителе государственной программы/подпрограммы, сведения о периоде реализации соответствующих федеральных проектов, а также сам факт включения того или иного федерального проекта в государственную программу/подпрограмму.

**Связь государственных программ/подпрограмм с федеральными проектами
в рамках национального проекта «Национальная программа «Цифровая экономика Российской Федерации»
и период их реализации**

Наименование государственных программ/подпрограмм (Ответственный исполнитель)	Наименования реализуемых федеральных проектов (период реализации)					
	Нормативное регулирование цифровой среды	Информационная инфраструктура	Цифровое государственное управление	Информационная безопасность	Кадры для цифровой экономики	Цифровые технологии
Экономическое развитие и инновационная экономика ¹ (Минэкономразвития России)	+ (2018–2024)					
Обеспечение доступным и комфортным жильем и коммунальными услугами граждан РФ ² (Минстрой России)		+ (2018–2025)	+ (2018–2025)			
Научно-технологическое развитие РФ ³ (Минобрнауки России)				+ (2019–2030)	+ (2019–2030)	
Информационное общество ⁴ /Информационное государство ⁵ (Минкомсвязь России)				+ (2011–2024)		+ (2011–2024)

Развитие промышленности и повышение ее конкурентоспособности ⁶ (Минпромторг России)				+ (2013–2024)		+ (2013–2024)
Содействие занятости населения ⁷ (Минтруд России)			+ (2013–2024)			

¹ Здесь и далее указано постановление Правительства РФ об утверждении соответствующей государственной программы (подпрограммы) — Постановление Правительства РФ от 15 апреля 2014 г. № 316 (ред. от 22.05.2019) «Об утверждении государственной программы Российской Федерации «Экономическое развитие и инновационная экономика».

² Постановление Правительства РФ от 30 декабря 2017 г. № 1710 (ред. от 07.05.2019) «Об утверждении государственной программы Российской Федерации «Обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации».

³ Постановление Правительства РФ от 29 марта 2019 г. № 377 «Об утверждении государственной программы Российской Федерации «Научно-технологическое развитие Российской Федерации».

⁴ Постановление Правительства РФ от 15 апреля 2014 г. № 313 (ред. от 23.05.2019) «Об утверждении государственной программы Российской Федерации «Информационное общество».

⁵ Постановление Правительства РФ от 29 марта 2019 г. № 356-24 «О внесении изменений в постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313».

⁶ Постановление Правительства РФ от 15 апреля 2014 г. № 328 (ред. от 29.03.2019) «Об утверждении государственной программы Российской Федерации «Развитие промышленности и повышение ее конкурентоспособности».

⁷ Постановление Правительства РФ от 15 апреля 2014 г. № 298 (ред. от 28.03.2019) «Об утверждении государственной программы Российской Федерации «Содействие занятости населения».

На основе приведенных в табл. 1 данных можно сделать вывод о том, что национальный проект «**Национальная программа “Цифровая экономика Российской Федерации”**» в целях единства системы государственного стратегического планирования интегрирован с государственными программами РФ и соответствующей подпрограммой, что обеспечивается наличием у них общего структурного элемента — федерального проекта Программы¹.

Как отмечено в документе Минфина России «Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2019 год и на плановый период 2020 и 2021 годов»² федеральные проекты одного и того же национального проекта, в зависимости от его специфики, могут быть включены как в одну, так и в несколько государственных программ.

Важно отметить, что достижение целей не только НП ЦЭ, но и других национальных проектов, с учетом действующего разграничения полномочий между уровнями государственного управления, невозможно без участия регионов.

В этой связи предполагается установление в федеральных проектах целевых показателей в разрезе субъектов РФ, а также введение механизмов координации и мониторинга мероприятий, реализуемых органами исполнительной власти субъектов РФ (в том числе с заключением соглашений между руководителями федеральных и региональных проектов)³.

Важно при этом иметь в виду, что реализация вышеупомянутых федеральных проектов согласно протоколу заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7 должна быть осуществлена в период до 31 декабря 2024 г.

Что касается основных направлений реализации Программы «Цифровая экономика Российской Федерации» по отраслям народного хозяйства, то можно выделить следующие:

в здравоохранении — телемедицина, в строительной отрасли — BIM⁴ — технологии и развитие концепции «Умный дом» и вышеупомянутой концепции «Умные города», а сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд —

¹ Определение понятия «федеральный проект Программы» представлено в сноске 6 данной статьи.

² СПС «КонсультантПлюс» (дата обращения: 09.10.2019).

³ Документ Минфина России «Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2019 год и на плановый период 2020 и 2021 годов» // СПС «КонсультантПлюс» (дата обращения: 09.10.2019).

⁴ Building information modeling — информационное моделирование в строительстве.

не только переход на электронные процедуры, но и превращение контрактной системы в реально действующий механизм нормоконтроля расходования бюджетных средств¹.

В заключение данного раздела следует отметить, что в интересах достижения целей и решения задач в процессе развития цифровой экономики в РФ формируется трехуровневая система управления, включающая **стратегический, оперативный и тактический уровни**.

На стратегическом уровне системы управления утверждаются направления развития цифровой экономики, стратегические цели и планы, а также отчеты об их достижении.

На оперативном уровне управления обеспечивается выполнение функций управления реализацией Программой на консолидированном уровне, в том числе:

- формирование совместно с профессиональными сообществами форсайта и моделей будущего;
- рассмотрение и утверждение предложений по внесению изменений в Программу, возникающих в ходе ее реализации;
- анализ и внесение изменений в документы стратегического планирования с учетом целей, задач и мероприятий Программы;
- формирование методологии планирования, координации, мониторинга и отчетности при реализации Программы;
- координация деятельности ФОИВ и органов исполнительной власти субъектов РФ, органов МСУ и взаимодействие с представителями бизнеса, гражданского общества и научно-образовательного сообщества по вопросам развития цифровой экономики;
- обеспечение ресурсами выполнения Программы, координация финансирования мероприятий по развитию цифровой экономики за счет средств бюджетов всех уровней и внебюджетных источников;
- управление «портфелями» проектов и отдельными проектами по направлениям Программы;
- формирование основных направлений исследований и разработок по направлениям цифровой экономики;
- организация мониторинга развития цифровой экономики и реализации Программы, рассмотрение его результатов и контроль за ходом выполнения;
- разработка и рассмотрение предложений по непрерывному совершенствованию системы управления развитием цифровой экономики;

¹ Подробнее об этом направлении см.: *Гринев В. П.* Контрактная система как механизм нормоконтроля расходования бюджетных средств // *Право и экономика*. 2015. № 7. С. 37–44.

- установка стандартов и осуществление регулирования цифровой экономики;
- формирование требований к описаниям компетенций цифровой экономики и создание описания этих компетенций.

На тактическом уровне обеспечивается управление выполнением планов и реализацией проектов по каждому из следующих направлений:

- разработка и реализация планов цифровой трансформации органов власти, государственных учреждений, корпораций и фондов;
- исполнение проектов настоящей Программы с целью достижения результата, реализация и масштабирование пилотных проектов и лучших практик;
- организация исследований и экспертизы в области цифровой экономики;
- формирование нормативной базы компонентов образовательных программ, существенных для цифровой экономики, включая стандарты и государственные требования, а также примерные программы;
- разработка предложений по мерам законодательного регулирования развития цифровой экономики;
- обеспечение ресурсами проектов и инициатив в области цифровой экономики и их финансирование;
- участие представителей всех заинтересованных сторон (власти, бизнеса, гражданского общества и научно-образовательного сообщества) в управлении центров развития и передачи цифровых технологий, деятельности рабочих групп, экспертизе проектов и планов развития цифровой экономики.

Одной из важнейших задач системы управления является поддержка «стартапов» и субъектов малого и среднего предпринимательства в области разработки и внедрения цифровых технологий путем их информационной акселерации (популяризации, обучения новым бизнес-моделям, навигации в системе управления, координации с другими участниками и ряд других мер) и инвестиционной акселерации (финансовой поддержки, создания специальных правовых и налоговых условий, переориентации институтов развития, создания новых способов поддержки и др.).

2. ПРАВОВЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАКУПОЧНОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВОЙ ЭКОНОМИКИ

«Информационная безопасность» в условиях цифровизации общества и экономики, в частности, имеет судьбоносное значение не только для всех, кто регулярно сталкивается с применением современных информационно-коммуникационных технологий в различных сферах своей деятельности, но тех, кого эта сфера касается независимо от их волеизъявления.

Особого внимания в контексте рассматриваемого вопроса заслуживают положения 73 Сессии Первого комитета Генеральной Ассамблеи ООН, в частности пункт 96 с повесткой дня «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», которая состоялась 22 октября 2018 г., а также принятую в декабре 2019 г. по предложению Российской Федерации резолюцию по борьбе с киберпреступностью.

Что касается содержания пункта 96, то с целью подчеркивания важности этой проблемы ниже приведено извлечение из этого документа с сохранением нумерации соответствующих пунктов¹:

«3. Государства не должны использовать информационно-коммуникационные технологии и информационно-коммуникационные сети для проведения мероприятий, которые идут вразрез с задачей поддержания международного мира и безопасности.

4. Государства не должны использовать информационно-коммуникационные технологии и информационно-коммуникационные сети для вмешательства во внутренние дела других государств или с целью подрыва их политической, экономической и социальной стабильности и подтверждают право и обязанность государств бо-

¹ Интернет (дата обращения: 31.12.2019).

роться, в рамках своих конституционных прав, с распространением ложных или искаженных новостных сообщений, которые могут быть истолкованы как вмешательство во внутренние дела других государств или как нанесение вреда поощрению мира, сотрудничества и дружественных отношений между государствами и народами.

6. Государства должны прилагать усилия для обеспечения безопасности товаров и услуг, связанных с информационно-коммуникационными технологиями, на всех уровнях каналов поставки в целях недопущения того, чтобы другие государства использовали свое доминирующее положение в сфере информационно-коммуникационных технологий, в том числе доминирование в сфере ресурсов, важнейших элементов инфраструктуры, основных технологий, товаров и услуг, связанных с информационно-коммуникационными технологиями, и информационно-коммуникационных сетей, для подрыва права государств на независимый контроль товаров и услуг, связанных с информационно-коммуникационными технологиями, или создания угрозы политической, экономической и социальной безопасности государств.

9. Все государства должны играть одинаковую роль и нести равную ответственность за международное управление Интернетом, обеспечение безопасности, бесперебойности и стабильности его функционирования и его развитие таким образом, который поощряет создание многосторонних, транспарентных и демократических международных механизмов управления Интернетом, позволяющих обеспечивать справедливое распределение ресурсов, способствовать доступу для всех и гарантировать стабильное и безопасное функционирование Интернета.

15. Государства должны принимать надлежащие меры для защиты критически важных объектов своей инфраструктуры от угроз в сфере информационно-коммуникационных технологий, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи от 23 декабря 2003 г. о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции.

18. Государства должны стремиться предупреждать распространение вредоносных программных и технических средств в сфере информационно-коммуникационных технологий и использование скрытых вредоносных функций.

19. Государства должны поощрять ответственное представление информации о факторах уязвимости в сфере информационно-коммуникационных технологий и делиться соответствующей информацией о существующих способах устранения таких факторов уязвимости, чтобы ограничить, а по возможности и устранить потенциальные угрозы для информационно-коммуникационных

технологий и объектов инфраструктуры, зависящих от таких технологий».

В силу специфики рассматриваемой темы представляет определенный интерес раскрытие в рамках проводимого исследования трактовки ряда понятий, относящихся к этой сфере деятельности.

Так, в частности, **информационная безопасность** в одном из ГОСТов трактуется как свойство информации сохранять конфиденциальность, целостность и доступность. Кроме того, данное понятие может включать в себя также и свойство сохранять аутентичность, подотчетность, неотказуемость и надежность¹.

При этом термин **информационная безопасность РФ**, в соответствии с Доктриной информационной безопасности РФ — **состояние защищенности** личности, общества и государства **от внутренних и внешних информационных угроз**, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства².

Что касается используемого при раскрытии термина «информационная безопасность» понятия **«информационная угроза»**, то оно трактуется как **совокупность действий и факторов**, создающих опасность нанесения ущерба национальным интересам **в информационной сфере**³.

Уместно к теме проводимого исследования привести трактовку и термина **«информационная сфера»**, под которой подразумевается совокупность разной информации вместе с информационной инфраструктурой, а также субъектов, которые занимаются сбором, использованием и распространением информации. К предметным областям информационной сферы относятся следующие действия соответствующих субъектов: применение, передача, получение, а также реализация права на поиск информации; распространение и передача как исходной информации, так и производной; подготовка различных информационных продуктов, создание необходимых информационных ресурсов и предоставление услуг, которые связаны с информацией; производство и последующее применение информационных систем, а также иных информационно-телекоммуника-

¹ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

² Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

³ Там же.

ционных технологий; формирование механизма информационной безопасности¹.

Касаясь закупочной деятельности в сфере обеспечения информационной безопасности, важно иметь в виду возникающие при этом общественные отношения, которые связаны с правом на защиту государства и общества от воздействия недостоверной, ложной информации, а также защиту информационных систем, информационных технологий и средств их обеспечения.

В этой связи важно иметь в виду постановление Правительства РФ от 8 июня 2018 г. № 658 «О централизованных закупках офисного программного обеспечения², программного обеспечения для ведения бюджетного учета³, а также программного обеспечения в сфере информационной безопасности⁴» (далее — Постановление № 658).

При этом важно понимать, что сведения о ПО должны быть включены в единый реестр российских программ для ЭВМ и БД, а само ПО соответствовать дополнительным требованиям к программам для ЭВМ и БД, сведения о которых включены в реестр российского ПО, утвержденным постановлением Правительства РФ от 23 марта 2017 г. № 325⁵.

Что касается порядка и методики подтверждения соответствия программ для ЭВМ и БД, сведения о которых включены в реестр

¹ Интернет-портал «Информационная сфера» // URL: utmagazine.ru/posts/10431-infomagoplaa-sfera (дата обращения: 02.05.2019).

² Под **офисным программным обеспечением** (далее — ПО) понимается офисный пакет, почтовые приложения, органайзер, средства просмотра, интернет-браузер, редактор презентаций, табличный редактор, текстовый редактор, сведения о которых включены в единый реестр российских программ для ЭВМ и баз данных (далее — БД), а также соответствующие дополнительным требованиям к программам для ЭВМ и БД, сведения о которых включены в реестр российского ПО, утвержденным постановлением Правительства РФ от 23 марта 2017 г. № 325. Подпункт «а» пункта 1 Постановления — извлечение.

³ Под ПО для ведения бюджетного учета понимается ПО, обеспечивающее автоматизацию функций, необходимых для ведения бюджетного учета в соответствии с законодательством РФ, сведения о котором включены в единый реестр российских программ для ЭВМ и БД — там же.

⁴ Под ПО в сфере информационной безопасности понимается ПО, соответствующее требованиям законодательства РФ в сфере обеспечения информационной безопасности и относящееся в соответствии с классификатором программ для ЭВМ и БД к классу «средства обеспечения информационной безопасности», сведения о котором включены в единый реестр российских программ для ЭВМ и БД — там же.

⁵ Постановление Правительства РФ от 23 марта 2017 г. № 325 «Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных».

российского ПО, дополнительным требованиям, установленным к программам для ЭВМ и БД, сведения о которых включены в реестр российского ПО, утвержденным постановлением Правительства РФ от 23 марта 2017 г. № 325, то и порядок, и методика утверждены приказом Минкомсвязи России от 19 декабря 2018 г. № 722¹.

Касательно темы централизованных закупок офисного ПО и ПО в сфере обеспечения информационной безопасности, то, согласно пункту 1 Постановления № 658, **полномочия на планирование такого рода закупок**, определение поставщиков (подрядчиков, исполнителей), заключение государственных контрактов, их исполнение, в том числе на приемку поставленных товаров, выполненных работ (их результатов), оказанных услуг, обеспечение их оплаты **для федеральных органов исполнительной власти, руководство деятельностью которых осуществляет Правительство РФ, возложены на Минкомсвязи России.**

В этой связи следует отметить, что 19 декабря 2018 г. Минкомсвязи России во исполнение Постановления № 658 был издан Приказ № 725 «Об утверждении формы и порядка представления в 2019 году информации о потребности, формирования потребности в осуществлении централизованных закупок офисного ПО и ПО в сфере информационной безопасности». Можно предположить, что аналогичный по содержанию Приказ может быть издан Минкомсвязи России и на последующие годы.

Что касается формы представления информации о потребности, формирования потребности в осуществлении централизованных закупок офисного ПО и ПО в сфере информационной безопасности, то она, согласно Приложению № 2 к Приказу № 725, состоит из ряда таблиц, содержание которых заслуживает отдельного рассмотрения, как вариант — в ходе практических занятий в рамках консультационных семинаров в ходе повышения квалификации или получения дополнительного профессионального образования в стенах того или иного учебного заведения.

При этом порядок представления информации о потребности, формирования потребности в осуществлении централизованных за-

¹ Приказ Минкомсвязи России от 19 декабря 2019 г. № 722 «Об утверждении порядка и методики подтверждения соответствия программ для электронных вычислительных машин и баз данных, сведения о которых включены в реестр российского программного обеспечения, дополнительным требованиям, установленным к программам для электронных вычислительных машин и баз данных, сведения о которых включены в реестр российского программного обеспечения, утвержденным постановлением Правительства Российской Федерации от 23 марта 2017 г. № 325, и о внесении изменений в Положение об Экспертном совете по российскому программному обеспечению при Министерстве связи и массовых коммуникаций Российской Федерации, утвержденное приказом Министерства связи и массовых коммуникаций Российской Федерации от 20 июня 2016 г. № 269».

купок офисного ПО и ПО в сфере информационной безопасности изложен в Приложении № 1 к Приказу № 725.

Следует отметить, что в этом Приложении прописаны конкретные сроки, которые должны быть соблюдены при направлении тех или иных документов в Минкомсвязи России, в том числе на бумажном носителе или посредством системы межведомственного электронного документооборота (в случае наличия), в частности, в течение 10 (десяти) рабочих дней с даты вступления в силу настоящего приказа.

При этом согласно пункту 2.3 Приложения № 1 Минкомсвязи России в срок не более 20 (двадцати) рабочих дней с даты получения информации рассматривает ее на предмет соответствия требованиям Постановления № 658.

Предусматривается возможность повторного представления соответствующей информации.

В случае реорганизации или ликвидации ФОИВ, изменения функций и полномочий ФОИВ не позднее двух месяцев после реорганизации или ликвидации, изменения функций и полномочий направляет в Минкомсвязи уточненную информацию.

Что касается формирования потребности, то необходимо иметь в виду, что в соответствии с пунктом 3.1 Приложения № 1 Минкомсвязи России формирует потребность для осуществления централизованных закупок офисного ПО и ПО в сфере информационной безопасности на плановый год на основании информации, полученной от ФОИВ на этапе формирования плана закупок ГРУ для обеспечения федеральных нужд с учетом требований к срокам, определенным Минфин России, при установлении порядка формирования и представления главными распорядителями средств федерального бюджета оснований бюджетных ассигнований.

Согласно пункту 3.2 Приложения № 1 потребность в части предоставления прав пользования (лицензий) ПО для обеспечения АРМ пользователей формируется исходя из количества стоящих на балансе ФОИВ и находящихся в эксплуатации персональных компьютеров, рабочих станций, планшетов и другой вычислительной техники, выполняющих функции АРМ пользователя ФОИВ, увеличенного на количество подобной вычислительной техники, запланированной к закупке в плановом году, за минусом количества вычислительной техники, предполагаемой к списанию с баланса и прекращению эксплуатации в плановом году.

В соответствии с пунктом 3.3 Приложения № 1 потребность в части предоставления прав пользования (лицензий) ПО для обеспечения работы серверов и аппаратных средств защиты определяется ФОИВ на основе количества стоящих на балансе ФОИВ и находящихся в эксплуатации серверов и другой вычислительной техники, выполняющих

функции аппаратных средств защиты и виртуальных серверов, для которых требуются средства защиты.

При этом важно иметь в виду, что в случае если ФОИВ указана необходимость поставки на материальном носителе и (или) в электронном виде по каналам связи, а также предоставления права пользования офисным ПО и ПО в сфере информационной безопасности, Минкомсвязи России включает в потребность сведения о приобретении (продлении) прав пользования данным ПО с учетом информации об имеющихся у ФОИВ и Минкомсвязи России прав на такое ПО.

Что касается необходимости оказания услуг, связанных с сопровождением, технической поддержкой, обновлением офисного ПО и ПО в сфере информационной безопасности (далее — услуги по сопровождению), то Минкомсвязи России включает в потребность для осуществления централизованных закупок услуги, связанные с приемом, выполнением и мониторингом выполнения обращений пользователей ПО, а также с восстановлением штатного функционирования программного обеспечения, включая:

- предоставление консультаций по применению обходного решения или альтернативных настроек/сценариев работы для устранения сбоя или ошибки;

- взаимодействие с производителем ПО (вендором) в части передачи сведений о возникновении нештатных ситуаций и выявленных замечаниях в работе для поиска и устранения ошибок функционирования ПО, а также оптимизации ПО, его обновление и при необходимости — корректировку рабочей документации и доработку;

- передачу полученных от производителя ПО обновлений и скорректированной эксплуатационной документации;

- ведение и актуализацию базы знаний по типовым обращениям пользователей по результатам проведения анализа возникновения нештатных ситуаций.

Применительно к полномочиям на закупки ПО для ведения бюджетного учета для соответствующих ФОИВ и подведомственных им федеральных казенных учреждений, то они возложены на Федеральное казначейство. В целях осуществления возложенных на данное ведомство полномочий 10 октября 2018 г. им было выпущено два приказа, в частности:

№ 36н «Об утверждении графика перехода ФОИВ, руководство деятельностью которых осуществляет Правительство РФ, а также подведомственных федеральных казенных учреждений на ведение бюджетного учета с использованием программного обеспечения для ведения бюджетного учета, предоставляемого им Федеральным казначейством по результатам закупок, предусмотренных пунктом 1 постановления Правительства Российской Федерации от 8 июня 2018 г. № 658”;

№ 37н «Об утверждении формы и порядка представления информации о потребности в осуществлении централизованных закупок программного обеспечения для ведения бюджетного учета и формирования потребности для осуществления централизованных закупок программного обеспечения для ведения бюджетного учета».

В контексте юрисдикции Постановления № 658 следует иметь в виду, что ФОИВ, руководство которыми осуществляет Правительство РФ, определены Указом Президента РФ от 15 мая 2018 г. № 215. В соответствии с этим Указом к этим ФОИВ относятся все министерства (по состоянию на текущую дату их 17), за исключением пяти, в частности, МВД, МО, МИД, МЧС и Минюст России руководство которыми осуществляет Президент РФ.

При этом согласно подпункту «а» пункта 1 Постановления № 658 **под закупками офисного ПО, ПО в сфере информационной безопасности, ПО для ведения бюджетного учета понимается осуществление следующих видов закупок:**

поставку на материальном носителе и (или) в электронном виде по каналам связи ПО, а также предоставление права пользования ПО посредством использования каналов связи и внешней информационно-технологической и программно-аппаратной инфраструктуры, обеспечивающей сбор, обработку и хранение данных (услуги облачных вычислений);

выполнение работ, оказание услуг, связанных с разработкой, модификацией, модернизацией ПО, в том числе в составе существующих автоматизированных систем;

выполнение работ, оказание услуг по установке и настройке ПО;

оказание услуг, связанных с сопровождением, технической поддержкой, обновлением ПО, в том числе в составе существующих автоматизированных систем.

С учетом вышесказанного ПО можно купить как товар на носителе или в сети, вместе с техникой, на которой оно работает, или как услугу по предоставлению права пользования программой.

Однако при этом необходимо иметь в виду, что постановлением Правительства РФ от 16 ноября 2015 г. № 1236, в частности, пунктом 2, установлен запрет на допуск программ для ЭВМ и баз данных, реализуемых независимо от вида договора на материальном носителе и (или) в электронном виде по каналам связи, происходящих из иностранных государств (за исключением ПО, включенного в единый реестр программ для ЭВМ и баз данных (далее — БД) из государств — членов ЕАЭС, за исключением РФ (далее — реестр ЕАЭС), а также исключительных прав на такое ПО и прав использования такого ПО, для целей осуществления закупок для обеспечения государственных и муниципальных нужд, **за исключением следующих случаев:**

а) в едином реестре российских программ для ЭВМ и БД и реестре евразийского ПО отсутствуют сведения о ПО, соответствующем тому же классу ПО, что и ПО, планируемое к закупке;

б) ПО, сведения о котором включены в реестр российского ПО и (или) реестр евразийского ПО и которое соответствует тому же классу ПО, что и ПО, планируемое к закупке, по своим функциональным, техническим и (или) эксплуатационным характеристикам не соответствует установленным заказчиком требованиям к планируемому к закупке ПО.

Важно также отметить, что Постановлением № 1236 установлен не только соответствующий запрет, о котором шла речь выше, но и утверждены правила формирования и ведения единого реестра российских программ для ЭВМ и БД и единого реестра программ для ЭВМ и БД из государств — членов ЕАЭС, за исключением РФ¹; а также порядок подготовки обоснования невозможности соблюдения запрета на допуск ПО, происходящего из иностранных государств (за исключением ПО, включенного в единый реестр программ для ЭВМ и БД из государств — членов ЕАЭС, за исключением РФ), для целей осуществления закупок для обеспечения государственных и муниципальных нужд.

Однако надо иметь в виду, что согласно пункту 3 Постановления № 1236 вышеупомянутый запрет не распространяется на осуществление закупок ПО и (или) прав на него дипломатическими представительствами и консульскими учреждениями РФ, торговыми представительствами РФ при международных организациях для обеспечения своей деятельности на территории иностранного государства. Более подробно тема осуществления закупок заказчиками, осуществляющими деятельность на территории иностранного государства, раскрыта автором настоящей публикации в журнале «Право и экономика»².

Что касается общей юрисдикции Постановления № 1236, то, согласно пункту 4 этого Постановления, оно не распространяется на осуществление закупок ПО и (или) прав на него, сведения о котором и (или) о закупке которого составляют государственную тайну.

При этом важно иметь в виду, что в соответствии с требованиями Федерального закона от 5 апреля 2013 г. № 44-ФЗ³ (далее ФЗ № 44-ФЗ) обоснование невозможности соблюдения запрета должно раз-

¹ В соответствии с информацией СПС «КонсультантПлюс», по состоянию на текущую дату реестр российского ПО в настоящее время доступен на сайте Минкомсвязи России, реестр евразийского ПО находится в стадии разработки.

² Гринев В. П. Особенности планирования и осуществления закупок заказчиками, осуществляющими деятельность на территории иностранного государства: правовые аспекты // Право и экономика. 2018. № 6. С. 30–37.

³ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

мешаться в Единой информационной системе (далее — ЕИС) вместе с извещением о закупке.

Касательно особенностей закупочной деятельности ПО в интересах обеспечения информационной безопасности можно было бы также отметить, что основной их них является выбор способа определения поставщика (подрядчика, исполнителя).

Так согласно части 1 статьи 24 ФЗ № 44-ФЗ заказчики при осуществлении закупок используют конкурентные способы определения поставщиков (подрядчиков, исполнителей)¹ или осуществляют закупки у единственного поставщика (подрядчика, исполнителя).

При этом согласно части 2 статьи 24 ФЗ № 44-ФЗ конкурентными способами определения поставщиков (подрядчиков, исполнителей) являются конкурсы (открытый конкурс, конкурс с ограниченным участием, двухэтапный конкурс, закрытый конкурс, закрытый конкурс с ограниченным участием, закрытый двухэтапный конкурс), аукционы (электронный аукцион, закрытый аукцион), запрос котировок, запрос предложений.

Важно иметь в виду, что с учетом особенностей, установленных ФЗ № 44-ФЗ, в электронной форме проводятся открытый конкурс, конкурс с ограниченным участием, двухэтапный конкурс, электронный аукцион, запрос котировок, запрос предложений (далее также — **электронные процедуры**), а также в случаях, установленных решением Правительства Российской Федерации, предусмотренным частью 3 статьи 84.1 настоящего Федерального закона, закрытый конкурс, закрытый конкурс с ограниченным участием, закрытый двухэтапный конкурс, закрытый аукцион (далее также — **закрытые электронные процедуры**).

Среди поименованных конкурентных способов на первом месте стоит конкурс, который может быть как открытым, так и закрытым.

При этом необходимо понимать, что открытый конкурс может проводиться практически всегда, за исключением случаев, поименованных в части 2 статьи 84 ФЗ № 44-ФЗ, к которым относятся:

1) закупки товаров, работ, услуг, необходимые для обеспечения федеральных нужд, если сведения о таких нуждах составляют государственную тайну;

2) закупки товаров, работ, услуг, сведения о которых составляют государственную тайну, при условии, что такие сведения содержатся в документации о закупке или в проекте контракта;

3) заключения контрактов на оказание услуг по страхованию, транспортировке и охране ценностей Государственного фонда драгоценных металлов и драгоценных камней РФ, на оказание услуг

¹ Согласно части 2 статьи 24 ФЗ № 44-ФЗ, части 3 статьи 84.1

по страхованию, транспортировке, охране музейных предметов и музейных коллекций, редких и ценных изданий, рукописей, архивных документов (включая их копии), имеющих историческое, художественное или иное культурное значение и передаваемых заказчиками физическим лицам или юридическим лицам либо принимаемых заказчиками от физических лиц или юридических лиц во временное владение и пользование либо во временное пользование, в том числе в связи с проведением выставок на территории РФ и (или) территориях иностранных государств;

4) закупки услуг по уборке помещений, услуг водителей для обеспечения деятельности судей, судебных приставов;

5) закупки **ФОИВ**, осуществляющими функции по выработке и реализации государственной политики в области обороны, государственного управления в области обеспечения безопасности РФ, подведомственными им государственными учреждениями, государственными унитарными предприятиями, за исключением случаев, установленных частью 2 статьи 84.1 **ФЗ № 44-ФЗ**.

Важно также отметить, что согласно части 1 статьи 24.1 **ФЗ № 44-ФЗ** **проведение электронных процедур, закрытых электронных процедур**, в том числе направление участниками закупок запросов о даче разъяснений положений извещения об осуществлении закупки и (или) документации о закупке, подача участниками закупок заявок на участие в закупке, предложений о цене контракта, окончательных предложений, предоставление комиссии по осуществлению закупок доступа к указанным заявкам, сопоставление предложений о цене контракта участников закупки, формирование протоколов, заключение контракта с победителем закупки, обеспечивается на электронной площадке оператором электронной площадки, а при проведении закрытых электронных процедур на специализированной электронной площадке оператором специализированной электронной площадки.

Что касается проведения аукционов в электронной форме, то необходимо иметь в виду, что распоряжением Правительства РФ от 21 марта 2016 г. № 471-р утвержден перечень товаров, работ, услуг, в случае осуществления закупки которых заказчик обязан проводить аукцион в электронной форме (электронный аукцион).

Необходимо также иметь в виду, что закупка ПО с указанием на конкретный товарный знак или фирменное наименование по общим правилам **ФЗ № 44-ФЗ** не допускается, поскольку может повлечь ограничение количества участников. Но, как отмечается в СПС К+, из этого правила есть исключение, в частности, при описании объекта закупки можно указать на фирменное наименование необходимого ПО при соблюдении одного из условий согласно пункту 1 части 1 и части 2 статьи 33 **ФЗ № 44-ФЗ**, к которым относятся:

указание на фирменное наименование сопровождается словами «или эквивалент». При этом в документации должны быть установлены параметры эквивалентности — те характеристики, которым должно соответствовать поставляемое ПО;

ПО других производителей несовместимо с используемой техникой или другим ПО. В этом случае указывать товарный знак можно без сопровождения словами «или эквивалент». Чтобы снизить риск жалоб от участников или претензий со стороны контрольных органов, рекомендуется обосновать невозможность использования другого ПО в документации о закупке. Например, можно указать наименование, версию уже используемого ПО, модель используемой, ссылкой на пункты технической документации эксплуатируемого оборудования.

Обсуждая вопрос о конкурентных способах определения поставщика обращает на себя внимание и запрос котировок с учетом того обстоятельства, что согласно части 16 статьи 1 Федерального закона от 27 декабря 2019 г. № 449-ФЗ «О внесении изменений в Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» с 1 июля 2020 г. Заказчик вправе осуществлять закупки путем проведения запроса котировок в электронной форме при условии, что начальная (максимальная) цена контракта не превышает 3 миллионов рублей (ранее было 500 тысяч рублей).

Можно отметить, что увеличение порогового значения с 500 тысяч рублей до 3 млн рублей может благоприятно сказаться на закупке не только ПО, но и соответствующего оборудования в интересах обеспечения информационной безопасности ЦЭ.

В свете обсуждения вопроса об информационной безопасности и в этой связи допуска на российский рынок отдельных видов товаров, происходящих из иностранных государств, следует также иметь в виду постановление Правительства РФ от 21 декабря 2019 г. № 1746 «Об установлении запрета на допуск отдельных видов товаров, происходящих из иностранных государств, и внесении изменений в некоторые акты Правительства Российской Федерации», в соответствии с пунктом 1 которого установлен запрет на допуск программно-аппаратных комплексов систем хранения данных, относящихся к коду по Общероссийскому классификатору продукции по видам экономической деятельности ОК 034-2014 (КПЕС 2008) 26.20.2 «Устройства запоминающие и прочие устройства хранения данных», происходящих из иностранных государств, для целей осуществления закупок товаров (работ, услуг) для обеспечения государственных и муниципальных нужд.

Как указано в пункте 2 вышеупомянутого Постановления, данный запрет распространяется на товары, являющиеся как предметом закупки, в том числе в случае закупки работ (услуг), при выполнении

(оказании) которых предусмотрена поставка товаров, так и предметом аренды и (или) лизинга, а в пункте 3 Постановления отмечается, что подтверждением производства товаров на территории РФ является наличие сведений о товаре в Едином реестре российской радиоэлектронной продукции¹.

При этом позиция, классифицируемая кодом по ОК 034-2014 (КПЕС 2008) из 26.20.2 «Системы хранения данных», в соответствии с постановлением Правительства РФ от 10 мая 2017 г. № 550 «О внесении изменений в постановление Правительства Российской Федерации от 17 июля 2015 г. № 719» в постановлении Правительства РФ № 719 излагается в следующей редакции:

наличие у юридического лица — налогового резидента РФ, не находящегося под контролем иностранного государства, и (или) международной организации, и (или) иностранного юридического или физического лица, и (или) иностранной структуры без образования юридического лица², **прав на технологию, включая методики и ноу-хау, а также патентов, прав на конструкторскую и техническую документацию для производства и проектирования, модернизации и развития соответ-**

¹ Единый реестр российской радиоэлектронной продукции размещен по адресу <https://gisp.gov.ru/documents/10546664/#>. Примечание СПС «КонсультантПлюс» к пункту 3 постановления.

² В соответствии со сноской «б» к постановлению Правительства РФ от 17 июля 2015 г. № 719 (ред. от 21.12.2019) «О подтверждении производства промышленной продукции на территории Российской Федерации» подтверждением наличия у юридического лица — налогового резидента стран — членов Евразийского экономического союза прав на конструкторскую и техническую документацию в объеме, достаточном для производства, модернизации и развития соответствующей продукции, являются следующие документы:

в случае создания конструкторской и технической документации собственными силами юридического лица — приказ о разработке комплекта конструкторской и технической документации;

в случае приобретения готовой конструкторской и технической документации предприятием — изготовителем продукции у предприятия — разработчика конструкторской и технической документации на продукцию — договор купли-продажи или договор поставки товара, а также акт передачи конструкторской и технической документации на продукцию, являющийся неотъемлемой частью одного из указанных договоров;

в случае выполнения работ по разработке предприятием — разработчиком конструкторской и технической документации на продукцию для предприятия — изготовителя продукции — договор подряда или договор на выполнение опытно-конструкторских и технологических работ, а также акт передачи результатов работ (конструкторской и технической документации на продукцию), являющийся неотъемлемой частью одного из указанных договоров;

в случае наличия в составе конструкторской и технической документации на продукцию секрета производства (ноу-хау) — договор об отчуждении исключительного права на секрет производства или лицензионный договор о предоставлении права использования секрета производства.

ствующей продукции на территории РФ в соответствии со спецификацией на готовое изделие в следующем составе:

технические условия;
спецификация на готовое изделие с указанием сборочных единиц и деталей;

руководство (инструкция) по эксплуатации;

схема деления изделия;

схема электрическая функциональная;

технологическая инструкция;

Gerber-файлы (трассировка печатной платы и схема расположения элементов);

перечень комплектующих;

наличие прав на срок не менее 5 лет на использование, модификацию, модернизацию и изменение полного перечня программного обеспечения (встроенного микропрограммного, системного и специализированного прикладного), поставляемого в составе продукции и необходимого для полноценного функционирования продукции, в том числе комплекта программной документации в следующем составе:

комплект текстов программ (исходных кодов) и двоичных файлов-микрокодов;

руководство по компиляции и сборке полного перечня программного обеспечения (встроенного микропрограммного, системного и специализированного прикладного), необходимого для полноценного функционирования продукции и инсталляции его двоичного образа в составе продукции;

наличие на территории РФ сервисного центра, уполномоченного осуществлять ремонт, послепродажное, гарантийное и постгарантийное обслуживание продукции;

наличие научно-производственной базы, необходимой для организации разработки и производства, или договорных отношений с организациями, зарегистрированными на территории РФ, которые имеют данную базу, по ее использованию;

наличие документов, подтверждающих проведение на территории РФ следующих технологических операций:

изготовление плат печатного монтажа для электронных блоков (удельный вес операции в структуре трудоемкости производства оборудования — 0,3, а в случае применения в продукции центрального процессора, удовлетворяющего требованиям к интегральной схеме первого уровня или интегральной схеме второго уровня, предъявляемым в целях ее отнесения к продукции, произведенной на территории РФ, — 0,25);

монтаж элементов на платы печатного монтажа, электронных модулей и финишная сборка оборудования (удельный вес операции

в структуре трудоемкости производства оборудования — 0,3, а в случае применения в продукции центрального процессора, удовлетворяющего требованиям к интегральной схеме первого уровня или интегральной схеме второго уровня, предъявляемым в целях ее отнесения к продукции, произведенной на территории РФ, — 0,5);

изготовление механических деталей и корпусных элементов (удельный вес операции в структуре трудоемкости производства оборудования — 0,1, а в случае применения в продукции центрального процессора, удовлетворяющего требованиям к интегральной схеме первого уровня или интегральной схеме второго уровня, предъявляемым в целях ее отнесения к продукции, произведенной на территории РФ, — 0,05);

программирование, функциональное тестирование электронных блоков и изделия в целом (удельный вес операции в структуре трудоемкости производства оборудования — 0,3, а в случае применения в продукции центрального процессора, удовлетворяющего требованиям к интегральной схеме первого уровня или интегральной схеме второго уровня, предъявляемым в целях ее отнесения к продукции, произведенной на территории РФ, — 0,2), при этом минимально допустимый уровень локализации составляет 75% и рассчитывается по формуле:

$$Y_{\text{л}} = (0,3 \times N_1 + 0,3 \times N_2 + 0,1 \times N_3 + 0,3 \times N_4) \times 100\%,$$

а в случае применения в продукции центрального процессора, удовлетворяющего требованиям к интегральной схеме первого уровня или интегральной схеме второго уровня, предъявляемым в целях ее отнесения к продукции, произведенной на территории РФ, — по формуле:

$$Y_{\text{л}} = (0,25 \times N_1 + 0,5 \times N_2 + 0,05 \times N_3 + 0,2 \times N_4) \times 100\%,$$

где: $Y_{\text{л}}$ — уровень локализации;

N_i — доля фактически произведенной продукции по каждой технологической операции, рассчитываемая на основе регламентированных ГОСТ 3.1102-2011 документов, включающих карты технологического процесса, маршрутную карту и ведомости сборки изделия заявленного оборудования, по формуле:

$$N_i = \frac{C_{i \text{ изгот}}}{C_{i \text{ полн}}},$$

где: $C_{i \text{ изгот}}$ — материальные и трудовые затраты отдельной технологической операции, произведенной на территории РФ, источник — маршрутная карта и ведомости сборки изделия;

$C_{i \text{ полн}}$ — полные материальные и трудовые затраты отдельной технологической операции, источник — карты технологического процесса;

по 31 декабря 2019 г. соблюдение процентной доли стоимости использованных при производстве иностранных комплектующих изделий — не более 45% цены товара;

с 1 января 2020 г. соблюдение процентной доли стоимости использованных при производстве иностранных комплектующих изделий — не более 35% цены товара;

с 1 января 2021 г. соблюдение процентной доли стоимости использованных при производстве иностранных комплектующих изделий — не более 35% цены товара, включая обязательное применение в продукции центрального процессора, удовлетворяющего требованиям к интегральной схеме первого уровня или интегральной схеме второго уровня, предъявляемым в целях ее отнесения к продукции, произведенной на территории РФ;

с 1 января 2022 г. соблюдение процентной доли стоимости использованных при производстве иностранных комплектующих изделий — не более 25% цены товара, включая обязательное применение в продукции центрального процессора, удовлетворяющего требованиям к интегральной схеме первого уровня или интегральной схеме второго уровня, предъявляемым в целях ее отнесения к продукции, произведенной на территории РФ;

с 1 января 2025 г. соблюдение процентной доли стоимости использованных при производстве иностранных комплектующих изделий — не более 15% цены товара, включая обязательное применение в продукции центрального процессора, удовлетворяющего требованиям к интегральной схеме первого уровня или интегральной схеме второго уровня, предъявляемым в целях ее отнесения к продукции, произведенной на территории РФ.

Требование о соблюдении процентной доли стоимости использованных при производстве иностранных комплектующих изделий во всех годах предъявляется к изделию в базовой комплектации без учета стоимости накопителей данных — жестких магнитных дисков, твердотельных дисков, магнитных лент.

При хранении конструкторской и технической документации в электронном виде юридическое лицо обязано обеспечить ее запись, систематизацию, накопление, хранение и уточнение (обновление, изменение) с использованием баз данных, находящихся на территории РФ.

В случае использования прав на основании лицензионного соглашения срок лицензии не должен быть менее 5 лет, лицензия должна предоставлять российскому лицензиату право на самостоятельное усовершенствование, модификацию и расширение лицензионных технологий с получением прав на измененную технологию без обязательства предоставления лицензии на измененную технологию в пользу лицензиара.

Следует также отметить, что одним из изменений, которые вносятся в акты Правительства РФ в соответствии с постановлением Правительства РФ от 21 декабря 2019 г. № 1746, является изменение, состоящее в том, что в перечне радиоэлектронной продукции,

происходящей из иностранных государств, в отношении которой устанавливаются ограничения для целей осуществления закупок для обеспечения государственных и муниципальных нужд, утвержденном постановлением Правительства Российской Федерации от 10 июля 2019 г. № 878¹, позицию, классифицируемую кодом «26», изложить в следующей редакции: «26. Оборудование компьютерное, электронное и оптическое (за исключением продукции, соответствующей позиции, классифицируемой кодом 26.20.2 “Устройства запоминающие и прочие устройства хранения данных”, в отношении которой постановлением Правительства РФ от 21 декабря 2019 г. № 1746² установлен запрет на допуск сроком на 2 года)».

В контексте рассмотрения вопроса о правовом регулировании обеспечения информационной безопасности ЦЭ РФ следует отметить и Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (далее — Указ № 620).

В соответствии с пунктом 2 Указа № 620 задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ являются:

а) прогнозирование ситуации в области обеспечения информационной безопасности РФ;

б) обеспечение взаимодействия владельцев информационных ресурсов РФ, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности информационных ресурсов Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов РФ.

При этом важно иметь в виду, что постановлением Правительства РФ от 7 октября 2019 г. № 1285 утверждены Правила предоставления

¹ Постановление Правительства Российской Федерации от 10 июля 2019 г. № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, о внесении изменений в постановление Правительства Российской Федерации от 16 сентября 2016 г. № 925 и признании утратившими силу некоторых актов Правительства Российской Федерации».

² Постановление Правительства Российской Федерации от 21 декабря 2019 г. № 1746 «Об установлении запрета на допуск отдельных видов товаров, происходящих из иностранных государств, и внесении изменений в некоторые акты Правительства Российской Федерации».

субсидий из федерального бюджета на создание отраслевого центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах. Следует отметить, что утвержденные данным Постановлением Правила устанавливают цели, условия и порядок предоставления субсидий из федерального бюджета на создание отраслевого центра ГосСОПКА и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации».

В качестве заключения можно отметить, что положения данного раздела могут быть рекомендованы к использованию достаточно широкому кругу лиц, для которых как непосредственная закупка ПО и соответствующего оборудования, так и понимание особенностей ее проведения представляет профессиональный интерес в целях обеспечения информационной безопасности цифровой экономики, а также государства и личности.

3. ПРОФЕССИОНАЛЬНЫЕ СТАНДАРТЫ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВОЙ ЭКОНОМИКИ

3.1. Общие положения

Профессиональные стандарты как норма права были введены в Трудовой кодекс Российской Федерации¹ (далее ТК РФ), вступивший в силу с 1 февраля 2002 г., согласно статье 195.1² в соответствии с Федеральным законом от 3 декабря 2012 г. № 236-ФЗ, т. е. по истечении почти десятилетнего срока его действия.

Первоначальная редакция понятия «профессиональный стандарт» представляла собой характеристику квалификации, необходимой работнику для осуществления определенного вида профессиональной (трудовой) деятельности, представляющей собой, в соответствии с п. 2 приказа Минтруда России от 29 апреля 2013 г. № 170н (далее — Приказ № 170н), совокупность обобщенных трудовых функций (далее — ОТФ), имеющий близкий характер, результаты и условия труда. При этом ОТФ, согласно этому же НПА, это совокупность связанных между собой трудовых функций (далее ТФ), сложившихся в результате разделения труда в конкретном производственном или бизнес-процессе. В свою очередь ТФ трактовалась в этом приказе как система трудовых действий в рамках ОТФ, представляющая собой интегрированный и относительно автономный набор трудовых действий, определяемых бизнес-процессом и предполагающий наличие необходимых компетенций для их выполнения.

При этом под трудовыми действиями, в соответствии с Приказом № 170н, подразумевается «процесс взаимодействия работника с предметом труда, при котором достигается (решается. — прим. Авт.) определенная задача».

Важно также иметь в виду, что понятие «трудовой функции», согласно абзацу 2 части 2 статьи 57 ТК РФ, трактуется как «работа по долж-

¹ ТК РФ от 30 декабря 2001 г. № 197-ФЗ.

² Статья 195.1. Понятия квалификации работника, профессионального стандарта.

ности в соответствии со штатным расписанием, профессии, специальности с указанием квалификации; вид поручаемой работнику работы».

Что касается квалификации работника, то согласно части 1 статьи 195.1 ТК РФ, под ней в ее первоначальной редакции понимался уровень знаний, умений, профессиональных навыков и опыта работы работника.

Касательно темы профессиональных стандартов, следует отметить, что 22.01.2013 г. Правительство РФ в качестве подзаконного акта выпустило Постановление № 23 «О Правилах разработки и утверждения профессиональных стандартов» (далее — Постановление № 23).

Согласно этому Постановлению, проекты профессиональных стандартов могут разрабатываться объединениями работодателей, работодателями, профессиональными сообществами, саморегулируемыми организациями и иными некоммерческими организациями с участием образовательных организаций профессионального образования и других заинтересованных организаций. Важно при этом иметь в виду, что обязанность по координации разработки профессиональных стандартов в соответствии с этим Постановлением была возложена на Министерство труда и социальной защиты Российской Федерации (Минтруд России).

В этой связи следует учитывать, что **при разработке профессиональных стандартов** для описания трудовых функций, требований к образованию и обучению работников **должны применяться уровни квалификации**, утвержденные приказом Минтруда России от 12 апреля 2013 г. № 148н «Об утверждении уровней квалификации в целях разработки профессиональных стандартов» (далее — Приказ № 148н).

Этим приказом установлено 9 уровней квалификации, описание показателей которых представлено в табл. 2.

Таблица 2

Описание показателей уровней квалификации

Уровень	Показатели уровней	
	Полномочия	Ответственность
1	2	3
1	Деятельность под руководством	Индивидуальная
2	Деятельность под руководством с элементами самостоятельности при выполнении знакомых заданий	Индивидуальная
3	Деятельность под руководством с проявлением самостоятельности при решении типовых практических задач. Планирование собственной деятельности исходя из поставленной руководителем задачи	Индивидуальная

Окончание табл. 1

1	2	3
4	Деятельность под руководством с проявлением самостоятельности при решении практических задач, требующих анализа ситуации и ее изменений. Планирование собственной деятельности и/или деятельности группы работников исходя из поставленных задач	Ответственность за решение поставленных задач или результат деятельности группы работников
5	Самостоятельная деятельность по решению практических задач, требующих самостоятельного анализа ситуации и ее изменений. Участие в управлении решением поставленных задач в рамках подразделения	Ответственность за решение поставленных задач или результат деятельности группы работников или подразделения
6	Самостоятельная деятельность, предполагающая определение задач собственной работы и/или подчиненных по достижению цели. Обеспечение взаимодействия сотрудников и смежных подразделений	Ответственность за результат выполнения работ на уровне подразделения или организации
7	Определение стратегии, управление процессами и деятельностью, в том числе, инновационной, с принятием решения на уровне крупных организаций или подразделений	Ответственность за результаты деятельности крупных организаций или подразделений
8	Определение стратегии, управление процессами и деятельностью, в том числе, инновационной, с принятием решения на уровне крупных организаций	Ответственность за результаты деятельности крупных организаций и/или отрасли
9	Определение стратегии, управление большими техническими системами, социальными и экономическими процессами. Значительный вклад в определенную область деятельности	Ответственность за результаты деятельности на национальном или международном уровне

В свете обсуждаемого вопроса об уровне квалификации важно иметь в виду положения Федерального закона от 3 июля 2016 г. № 238-ФЗ «О независимой оценке квалификации» (далее Закон № 238-ФЗ).

В частности, следует иметь в виду, что в соответствии с этим Федеральным законом учреждено «Национальное агентство развития квалификаций», представляющее собой автономную некоммерче-

скую организацию, создаваемую в целях обеспечения деятельности по развитию квалификаций в РФ, в состав учредителей которой вошли общероссийские объединения работодателей, общероссийские объединения профессиональных союзов и РФ, от имени которой функции и полномочия учредителя осуществляют ФОИВ, уполномоченные Правительством РФ, которыми согласно распоряжению Правительства РФ от 3 ноября 2016 г. № 2348-р, вступившим в силу с 1 января 2017 г., определены Минтруд России и Минобрнауки России.

В этом же контексте следует также иметь в виду положения Указа Президента РФ от 16 апреля 2014 г. № 249 «О Национальном совете при Президенте Российской Федерации по профессиональным квалификациям», которым утверждено «Положение о Национальном совете при Президенте Российской Федерации по профессиональным квалификациям» (с изм. и доп., вступ. в силу с 1 января 2017 г.). В соответствии с этим Указом «Национальный совет при Президенте Российской Федерации по профессиональным квалификациям» является консультативным органом при Президенте РФ для рассмотрения вопросов, касающихся развития квалификаций в РФ. В настоящее время Председателем Национального совета при Президенте Российской Федерации по профессиональным квалификациям является А. Н. Шохин, который в рамках своих полномочий 3 июля 2017 г. утвердил ряд документов, в частности:

«Общие требования к проведению профессионально-общественной аккредитации основных профессиональных образовательных программ, основных программ профессионального обучения, дополнительных профессиональных программ»;

«Правила наделения работодателей, общероссийских и иных объединений работодателей, ассоциаций (союзов) и иных организаций, представляющих и (или) объединяющих профессиональные сообщества, полномочиями на проведение профессионально-общественной аккредитации»;

«Правила проведения профессионально-общественной аккредитации аккредитующими организациями»;

«Правила установления критериев оценки образовательных программ при проведении профессионально-общественной аккредитации»;

«Общие требования к квалификации экспертов, привлекаемых для проведения профессионально-общественной аккредитации»;

«Правила ведения мониторинга деятельности аккредитующих организаций».

Кроме того, необходимо также учитывать тот факт, что, согласно статье 3 Закона № 238-ФЗ, участниками системы независимой оценки квалификации, помимо вышеупомянутых органов, т. е. «Национального агентства развития квалификаций» и «Национального совета

при Президенте Российской Федерации по профессиональным квалификациям» являются также советы по профессиональным квалификациям; центры оценки квалификаций (далее ЦОК); работодатели, соискатели, а также ФОИВ в лице Минтруда России, в полномочия которого входит осуществление функций по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере труда.

Что касается независимой оценки квалификации, проводимой ЦОК, необходимо иметь в виду, что она осуществляется в порядке, определяемом Правилами проведения ЦОК в форме профессионального экзамена, утвержденными постановлением Правительства РФ от 16 ноября 2016 г. № 1204 (далее — Правила).

В соответствии с п. 2 Правил ЦОК представляют собой юридические лица, типовые требования к которым утверждены Решением Национального совета при Президенте РФ по профессиональным квалификациям (Протокол от 20 мая 2015 г. № 10).

При этом необходимо отметить, что в соответствии с п. 1 статьи 8 Закона № 238-ФЗ перечень квалификаций, по которым соответствующий ЦОК проводит экзамены, определяется советом по профессиональным квалификациям, положение о котором и порядок наделения его полномочиями утверждено приказом Минтруда России от 19 декабря 2016 г. № 758н «Об утверждении Примерного положения о совете по профессиональным квалификациям и Порядка наделения совета по профессиональным квалификациям полномочиями по организации проведения независимой оценки квалификации по определенному виду профессиональной деятельности и прекращения этих полномочий».

Что касается прохождения профессионального экзамена на предмет оценки уровня квалификации, то важно иметь в виду, что необходимые сведения указаны в «Информации» Минтруда России от 21 апреля 2017 г. «Ответы на часто задаваемые вопросы по реализации Федерального закона от 3 июля 2016 г. № 238-ФЗ “О независимой оценке квалификации”», в том числе сведения о ЦОК, в которых можно пройти оценку квалификации, размещаемые в реестре сведений о проведении независимой оценки квалификации в информационно-телекоммуникационной сети «Интернет» на сайте автономной некоммерческой организации «Национальное агентство развития квалификаций» (nok-nark.ru).

Как следует из п. 2 статьи 4 Закона № 238-ФЗ профессиональный экзамен может проводиться по инициативе соискателя за счет его собственных средств или средств иных физических и (или) юридических лиц, либо по направлению работодателя (с письменного согласия работника) за счет средств работодателя в порядке, установленном трудовым законодательством.

Для прохождения профессионального экзамена соискатель, согласно п. 7 Правил, должен представить комплект документов на бумажном или электронном носителе.

Форма заключения о прохождении профессионального экзамена утверждена приказом Минтруда России от 12 декабря 2016 г. № 725н «Об утверждении формы бланка свидетельства о квалификации и приложения к нему, технических требований к бланку свидетельства о квалификации, порядка заполнения бланка свидетельства о квалификации и выдачи его дубликата, а также формы заключения о прохождении профессионального экзамена».

С учетом того, что уровни квалификации, утвержденные Приказом № 148н, применяются для описания трудовых функций, требований к образованию и обучению работников **при разработке профессиональных стандартов**, то важно иметь в виду, что их утверждение, проводимое в соответствии с «Правилами разработки и утверждения профессиональных стандартов» (далее — Правила), утвержденными Постановлением № 23, должно осуществляется Минтруда России на основании экспертного заключения Национального совета при Президенте Российской Федерации по профессиональным квалификациям с рекомендациями о его одобрении.

В пункте 17 Правил, утвержденных Постановлением № 23, также отмечается, что в заключении Национального совета при Президенте Российской Федерации по профессиональным квалификациям указываются сведения о профессиональных стандартах, которые вносятся в реестр профессиональных стандартов (далее Реестр ПС).

При этом необходимо иметь в виду, что создание, ведение и актуализация Реестра ПС должны осуществляться ФГБУ «НИИ труда и социального страхования», который должен размещаться на специализированном сайте «Профессиональные стандарты» (<http://profstandart/gosmintud.ru>) в соответствии с приказом от 29 сентября 2014 г. № 667н (далее — Приказ № 667н).

Следует отметить, что через 2,5 года после введения в ТК РФ понятия «Профессиональный стандарт», а именно 2 мая 2015 г., в соответствии с Федеральным законом № 122-ФЗ это понятие в ТК РФ было уточнено, и в сегодняшней редакции статьи 195.1 оно представляет собой следующий вариант: «Профессиональный стандарт — характеристика квалификации, необходимой работнику для осуществления определенного вида профессиональной деятельности, в том числе выполнения определенной трудовой функции». **Акцент, как следует из новой редакции этого понятия, сделан на выполнении работником определенной трудовой функции.**

С учетом того, что профессиональные стандарты, как отмечалось выше, утверждаются соответствующими приказами Минтруда России, то в интересах настоящего издания была сформирована таблица

из 50 профессиональных стандартов, относящихся как непосредственно к сфере цифровой экономики и информационной безопасности, так и профессиональные стандарты, которым должны соответствовать сотрудники подразделений соответствующих организаций, относящиеся к административно-управленческому персоналу, бухгалтерии, отдела охраны труда и др. — табл. 3.

Таблица 3

**Приказы Министерства труда и социальной защиты
об утверждении профессиональных стандартов
в сфере цифровой экономики и информационной безопасности
(в период с 2013 по 2018 годы)**

№ п/п	Наименование профессионального стандарта	Номер приказа
1	2	3
2013 год		
13 ноября		
1	Программист	679н
Итого приказов за 2013 год — 1 приказ		
2014 год		
19 мая		
1	Инженер-радиоэлектронщик	315н
2	Инженер-проектировщик в области связи (телекоммуникаций)	316н
3	Инженер технической поддержки в области связи (телекоммуникаций)	317н
4	Специалист по радиосвязи и телекоммуникациям	318н
8 августа		
1	Специалист в области охраны труда	524н
8 сентября		
1	Технический писатель (специалист по технической документации в области информационных технологий)	612н
2	Специалист по информационным ресурсам	629н
17 сентября		
1	Руководитель разработки программного обеспечения	645н
2	Администратор баз данных	647н
13 октября		
1	Менеджер по информационным технологиям	716н
28 октября		
1	Системный аналитик	809н
31 октября		
1	Инженер связи (телекоммуникаций)	866н

Продолжение табл. 3

1	2	3
18 ноября		
1	Руководитель проектов в области информационных технологий	893н
2	Специалист по информационным системам	896н
20 ноября		
1	Менеджер продуктов в области информационных технологий	915н
22 декабря		
1	Бухгалтер	1061н
Итого приказов за 2014 год — 16 приказов		
2015 год		
23 марта		
1	Специалист по страхованию	186н
31 марта		
1	Специалист по платежным системам	204н
22 апреля		
1	Специалист по внутреннему контролю (внутренний контролер)	236н
6 мая		
1	Оператор связи	275н
2	Специалист по организационному и документационному обеспечению управления организацией	276н
24 июня		
1	Внутренний аудитор	398н
7 сентября		
1	Специалист по управлению рисками	591н
10 сентября		
1	Специалист в сфере закупок	625н
2	Эксперт в сфере закупок	626н
5 октября		
1	Системный администратор информационно-телекоммуникационных систем	684н
2	Системный программист	685н
3	Специалист по администрированию сетевых устройств информационно-коммуникационных систем	686н
4	Специалист по технической поддержке информационно-коммуникационных систем	688н
5	Специалист по дизайну графических и пользовательских интерфейсов	689н
6 октября		
1	Специалист по управлению персоналом	691н

Продолжение табл. 3

1	2	3
28 октября		
1	Специалист по организации и установлению выплат социального характера	787н
Итого приказов за 2015 год — 16 приказов		
2016 год		
15 сентября		
1	Специалист по защите информации в автоматизированных системах	522н
1 ноября		
1	Специалист по безопасности компьютерных систем и сетей	598н
2	Специалист по технической защите информации	599н
3 ноября		
1	Специалист по защите информации в телекоммуникационных системах и сетях	608н
9 ноября		
1	Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности	611н
Итого приказов за 2016 год — 5 приказов		
2017 год		
18 января		
1	Разработчик WEB и мультимедийных средств	44н
10 мая		
1	Специалист по управлению документацией организации	416н
31 мая		
1	Специалист по обслуживанию телекоммуникаций	465н
5 июня		
1	Специалист по организации и поддержке видеослуг через Интернет	472н
2	Специалист по монтажу телекоммуникационного оборудования	473н
3	Специалист по контролю качества информационно-коммуникационных систем	475н
26 июня		
1	Специалист по поддержке программно-конфигурируемых информационно-коммуникационных сетей	514н
5 сентября		
1	Специалист по интеграции прикладных решений	658н
Итого приказов за 2017 год — 8 приказов		

1	2	3
2018 год		
2 февраля		
1	Специалист административно-хозяйственной деятельности	49н
19 марта		
1	Специалист по дистанционному информационно-справочному обслуживанию	163н
17 апреля		
1	Специалист по процессному управлению	248н
19 апреля		
1	Специалист по формированию электронного архива	266н
Итого приказов за 2018 год — 4 приказа		
Всего учтено приказов за период с 2013 по 2018 годы — 50 приказов		

Важно иметь в виду, что все профессиональные стандарты, включая и 50 вышеприведенных, предполагают выполнение работником соответствующих трудовых функций, в том числе и обобщенных.

С целью выстраивания методологии использования ТФ в ходе разработки должностных инструкций (ДИ) конкретных работников, выбран подход, основанный на раскрытии содержания ОТФ и ТФ на примере рассмотрения профессионального стандарта «Программист».

Выбор этого стандарта был обусловлен двумя обстоятельствами.

С одной стороны, профессиональный стандарт «Программист» был одним из первых после введения в ТК РФ статьи 195.1, а с другой стороны тем обстоятельством, что профессия «Программист» является одной из самых востребованных на рынке услуг в сфере цифровой экономики и информационной безопасности и от трудовых действий сотрудника, в ДИ которого прописаны соответствующие ТФ согласно приказу Минтруда России от 18 ноября 2013 г. № 679н, во многом может зависеть информационная безопасность организации, в интересах которой этот работник их выполняет.

Профессиональный стандарт «Программист», утвержденный приказом Минтруда России от 18 ноября 2013 г. № 679н, по состоянию на текущую дату действует в ред. приказа Минтруда России от 12 декабря 2016 г. № 727н и включает в себя четыре обобщенные трудовые функции, каждая из которых предполагает осуществление определенного количества трудовых функций.

Наименования ОТФ и ТФ, возможные наименования должностей, а также уровень квалификации, требования к образованию и обучению, входящих в профессиональный стандарт «Программист», представлены в табл. 4.

Таблица 4

**Наименование функций, входящих в профессиональный стандарт
«Программист», уровни квалификации,
требования к образованию и обучению**

Функции		
Обобщенные трудовые функции (ОТФ)		Трудовые функции (ТФ)
Наименование ОТФ/уровень квалификации	Возможные наименования должностей/Требования к образованию и обучению	Наименование ТФ/уровень квалификации
1	2	3
1. Разработка и отладка программного кода/3	Младший программист; техник-программист/Среднее профессиональное образование; повышение квалификации	Формализация и алгоритмизация поставленных задач/3
		Написание программного кода с использованием языков программирования, определения и манипулирования данными ¹ /3
		Оформление программного кода в соответствии с установленными требованиями/3
		Работа с системой контроля версий/3
2. Проверка работоспособности и рефакторинг ² программного обеспечения/4	Программист/Среднее профессиональное образование; повышение квалификации	Разработка процедур проверки работоспособности и измерения характеристик программного обеспечения/4

¹ Содержание трудовых действий, необходимых умений и знаний, требуемых при их осуществлении этой ТФ, взятой в качестве примера, представлено в табл. 5 настоящего издания.

² Рефакторинг (англ. refactoring), или перепроектирование кода, переработка кода, равносильное преобразование алгоритмов — процесс изменения внутренней структуры программы, не затрагивающий ее внешнего поведения и имеющий целью облегчить понимание ее работы. В основе рефакторинга лежит последовательность небольших эквивалентных (т.е. сохраняющих поведение) преобразований. Поскольку каждое преобразование маленькое, программисту легче проследить за его правильностью, и в то же время вся последовательность может привести к существенной перестройке программы и улучшению ее согласованности и четкости. См.: Фаулер М., Бек К., Братт Д., Робертс Д., Андайт У. Рефакторинг: улучшение существующего кода = Refactoring: Improving the Design of Existing Code (2000). СПб: Символ-Плюс, 2009. С. 61–62; Кериевски Д. Рефакторинг с использованием шаблонов = Refactoring to Patterns. Вильямс, 2008.

1	2	3
		Разработка тестовых наборов данных/4 Проверка работоспособности программного обеспечения/4 Рефакторинг и оптимизация программного кода/4 Исправление дефектов, зафиксированных в базе данных дефектов/4
3. Интеграция программных модулей и компонент и верификация выпусков программного продукта/5	Старший программист; инженер-программист/ Высшее образование; повышение квалификации	Разработка процедур интеграции программных модулей/5 Осуществление интеграции программных модулей и компонент и верификации выпусков программного продукта/5
4. Разработка требований и проектирование программного обеспечения/6	Ведущий программист; ведущий инженер-программист/ Высшее образование; повышение квалификации	Анализ требований к программному обеспечению/6 Разработка технических спецификаций на программные компоненты и их взаимодействие/6 Проектирование программного обеспечения/6

В интересах настоящего издания в качестве примера в табл. 5 представлены содержание трудовых действий, необходимых умений и знаний, требуемых при их осуществлении, в частности, младшим программистом или техником-программистом ТФ «Написание программного кода с использованием языков программирования, определения и манипулирования данными» в рамках ОТФ «Разработка и отладка программного кода».

Таблица 5

Содержание трудовых действий, необходимых умений и знаний, требуемых при осуществлении трудовой функции «Написание программного кода с использованием языков программирования, определения и манипулирования данными» в рамках ОТФ «Разработка и отладка программного кода»

Наименование	Содержание трудовых действий, необходимых умений и знаний
1	2
Трудовые действия	Создание программного кода в соответствии с техническим заданием (готовыми спецификациями)
	Оптимизация программного кода с использованием специализированных программных средств

Окончание табл. 5

1	2
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Применять выбранные языки программирования для написания программного кода
	Использовать выбранную среду программирования и средства системы управления базами данных
	Использовать возможности имеющейся технической и/или программной архитектуры
Необходимые знания	Синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования
	Методологии разработки программного обеспечения
	Методологии и технологии проектирования и использования баз данных
	Технологии программирования
	Особенности выбранной среды программирования и системы управления базами данных
	Компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними

Полный перечень ОТФ и ТФ, содержание трудовых действий, а также требования к необходимому уровню знаний и умений применительно к профессии «Программист» в соответствии с профессиональным стандартом, утвержденным приказом Минтруда России от 18 ноября 2013 г. № 679н, приведен в табл. 6.

Таблица 6

Содержание трудовых действий, необходимых умений и знаний, требуемых при осуществлении трудовых функций применительно к профессии «Программист»

Наименование функций	
ОТФ 1 «Разработка и отладка программного кода»	
Трудовые функции в рамках ОТФ 1	
1. Формализация и алгоритмизация поставленных задач	
1	2
Трудовые действия	Составление формализованных описаний решений поставленных задач в соответствии с требованиями технического задания или других принятых в организации нормативных документов
	Разработка алгоритмов решения поставленных задач в соответствии с требованиями технического задания или других принятых в организации нормативных документов

1	2
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Использовать методы и приемы формализации задач
	Использовать методы и приемы алгоритмизации поставленных задач
	Использовать программные продукты для графического отображения алгоритмов
	Применять стандартные алгоритмы в соответствующих областях
Необходимые знания	Методы и приемы формализации задач
	Языки формализации функциональных спецификаций
	Методы и приемы алгоритмизации поставленных задач
	Нотации и программные продукты для графического отображения алгоритмов
	Алгоритмы решения типовых задач, области и способы их применения
2. Написание программного кода с использованием языков программирования, определения и манипулирования данными	
Трудовые действия	Создание программного кода в соответствии с техническим заданием (готовыми спецификациями)
	Оптимизация программного кода с использованием специализированных программных средств
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Применять выбранные языки программирования для написания программного кода
	Использовать выбранную среду программирования и средства системы управления базами данных
	Использовать возможности имеющейся технической и/или программной архитектуры
Необходимые знания	Синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования
	Методологии разработки программного обеспечения
	Методологии и технологии проектирования и использования баз данных
	Технологии программирования
	Особенности выбранной среды программирования и системы управления базами данных
	Компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними

Продолжение табл. 6

1	2
3. Оформление программного кода в соответствии с установленными требованиями	
Трудовые действия	Приведение наименований переменных, функций, классов, структур данных и файлов в соответствии с установленными в организации требованиями
	Структурирование исходного программного кода в соответствии с установленными в организации требованиями
	Комментирование и разметка программного кода в соответствии с установленными в организации требованиями
	Форматирование исходного программного кода в соответствии с установленными в организации требованиями
Необходимые умения	Применять нормативные документы, определяющие требования к оформлению программного кода
	Применять инструментарий для создания и актуализации исходных текстов программ
	Применять имеющиеся шаблоны для составления технической документации
Необходимые знания	Инструментарий для создания и актуализации исходных текстов программ
	Методы повышения читаемости программного кода
	Системы кодировки символов, форматы хранения исходных текстов программ
	Нормативные документы, определяющие требования к оформлению программного кода
4. Работа с системой контроля версий	
Трудовые действия	Регистрация изменений исходного текста программного кода в системе контроля версий
	Слияние, разделение и сравнение исходных текстов программного кода
	Сохранение сделанных изменений программного кода в соответствии с регламентом контроля версий
Необходимые умения	Использовать выбранную систему контроля версий
	Использовать вспомогательные инструментальные программные средства для обработки исходного текста программного кода
	Выполнять действия, соответствующие установленному регламенту используемой системы контроля версий
Необходимые знания	Возможности используемой системы контроля версий и вспомогательных инструментальных программных средств
	Установленный регламент использования системы контроля версий

1	2
5. Проверка и отладка программного кода	
Трудовые действия	Анализ и проверка исходного программного кода
	Отладка программного кода на уровне программных модулей
	Отладка программного кода на уровне межмодульных взаимодействий и взаимодействий с окружением
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Выявлять ошибки в программном коде
	Применять методы и приемы отладки программного кода
	Интерпретировать сообщения об ошибках, предупреждения, записи технологических журналов Применять современные компиляторы, отладчики и оптимизаторы программного кода
Необходимые знания	Методы и приемы отладки программного кода
	Типы и форматы сообщений об ошибках, предупреждений
	Способы использования технологических журналов, форматы и типы записей журналов
	Современные компиляторы, отладчики и оптимизаторы программного кода Сообщения о состоянии аппаратных средств
ОТФ 2 «Проверка работоспособности и рефакторинг кода программного обеспечения»	
Трудовые функции в рамках ОТФ 2	
1. Разработка процедур проверки работоспособности и измерения характеристик программного обеспечения	
Трудовые действия	Разработка процедуры проверки работоспособности программного обеспечения
	Разработка процедуры сбора диагностических данных
	Разработка процедуры измерения требуемых характеристик программного обеспечения
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Писать программный код процедур проверки работоспособности программного обеспечения на выбранном языке программирования
	Использовать выбранную среду программирования для разработки процедур проверки работоспособности программного обеспечения на выбранном языке программирования
Необходимые знания	Методы автоматической и автоматизированной проверки работоспособности программного обеспечения

Продолжение табл. 6

1	2
	<p>Основные виды диагностических данных и способы их представления</p> <p>Языки, утилиты и среды программирования, и средства пакетного выполнения процедур</p> <p>Типовые метрики программного обеспечения</p> <p>Основные методы измерения и оценки характеристик программного обеспечения</p>
2. Разработка тестовых наборов данных	
Трудовые действия	Подготовка тестовых наборов данных в соответствии с выбранной методикой
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Разработка и оформление контрольных примеров для проверки работоспособности программного обеспечения
	Разработка процедур генерации тестовых наборов данных с заданными характеристиками
	Подготовка наборов данных, используемых в процессе проверки работоспособности программного обеспечения
Необходимые знания	Методы создания и документирования контрольных примеров и тестовых наборов данных
	Правила, алгоритмы и технологии создания тестовых наборов данных
	Требования к структуре и форматам хранения тестовых наборов данных
3. Проверка работоспособности программного обеспечения	
Трудовые действия	Проверка работоспособности программного обеспечения на основе разработанных тестовых наборов данных
	Оценка соответствия программного обеспечения требуемым характеристикам
	Сбор и анализ полученных результатов проверки работоспособности программного обеспечения
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Применять методы и средства проверки работоспособности программного обеспечения
	Интерпретировать диагностические данные (журналы, протоколы и др.)
	Анализировать значения полученных характеристик программного обеспечения
	Документировать результаты проверки работоспособности программного обеспечения

1	2
Необходимые знания	Методы и средства проверки работоспособности программного обеспечения
	Среда проверки работоспособности и отладки программного обеспечения
	Внутренние нормативные документы, регламентирующие порядок документирования результатов проверки работоспособности программного обеспечения
4. Рефакторинг и оптимизация программного кода	
Трудовые действия	Анализ программного кода на соответствие требованиям по читаемости и производительности
	Внесение изменений в программный код и проверка его работоспособности
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Применять методы, средства для рефакторинга и оптимизации
	Применять инструментальные средства коллективной работы над программным кодом
	Публиковать результаты рефакторинга и оптимизации в коллективной базе знаний в виде лучших практик
	Использовать систему контроля версий для регистрации произведенных изменений
Необходимые знания	Методы и средства рефакторинга и оптимизации программного кода
	Языки программирования и среды разработки
	Внутренние нормативные документы, регламентирующие требования к программному коду, порядок отражения изменений в системе контроля версий
	Внутренние нормативные документы, регламентирующие порядок отражения результатов рефакторинга и оптимизации в коллективной базе знаний
5. Исправление дефектов, зафиксированных в базе данных дефектов	
Трудовые действия	Воспроизведение дефектов, зафиксированных в базе данных дефектов
	Установление причин возникновения дефектов
	Внесение изменений в программный код для устранения выявленных дефектов
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Применять методы и приемы отладки дефектного программного кода

Продолжение табл. 6

1	2
	Интерпретировать сообщения об ошибках, предупреждения, записи технологических журналов, возникающих при выполнении дефектного кода
Необходимые знания	<p>Методы и приемы отладки программного кода</p> <p>Типовые ошибки, возникающие при разработке программного обеспечения, и методы их диагностики и исправления</p>
ОТФ 3 «Интеграция программных модулей и компонент и проверка работоспособности выпусков программного продукта»	
Трудовые функции в рамках ОТФ 3	
1. Разработка процедур интеграции программных модулей	
Трудовые действия	<p>Разработка и документирование программных интерфейсов</p> <p>Разработка процедур сборки модулей и компонент программного обеспечения</p> <p>Разработка процедур развертывания и обновления программного обеспечения</p> <p>Разработка процедур миграции и преобразования (конвертации) данных</p> <p>Оценка и согласование сроков выполнения поставленных задач</p>
Необходимые умения	<p>Писать программный код процедур интеграции программных модулей</p> <p>Использовать выбранную среду программирования для разработки процедур интеграции программных модулей</p> <p>Применять методы и средства сборки модулей и компонент программного обеспечения, разработки процедур для развертывания программного обеспечения, миграции и преобразования данных, создания программных интерфейсов</p>
Необходимые знания	<p>Методы и средства сборки модулей и компонент программного обеспечения</p> <p>Интерфейсы взаимодействия с внешней средой</p> <p>Интерфейсы взаимодействия внутренних модулей системы</p> <p>Методы и средства разработки процедур для развертывания программного обеспечения</p> <p>Методы и средства миграции и преобразования данных</p> <p>Языки, утилиты и среды программирования, средства пакетного выполнения процедур</p>
2. Осуществление интеграции программных модулей и компонент и верификации выпусков программного продукта	
Трудовые действия	Процедуры сборки программных модулей и компонент в программный продукт

1	2
	<p>Подключение программного продукта к компонентам внешней среды</p> <p>Проверка работоспособности выпусков программного продукта</p> <p>Внесение изменений в процедуры сборки модулей и компонент программного обеспечения, развертывания программного обеспечения, миграции и преобразования данных</p> <p>Оценка и согласование сроков выполнения поставленных задач</p>
Необходимые умения	<p>Выполнять процедуры сборки программных модулей и компонент в программный продукт</p> <p>Производить настройки параметров программного продукта и осуществлять запуск процедур сборки</p> <p>Проводить оценку работоспособности программного продукта</p> <p>Документировать произведенные действия, выявленные проблемы и способы их устранения</p> <p>Выявлять соответствие требований заказчиков с существующими продуктами</p> <p>Создавать резервные копии программ и данных, выполнять восстановление, обеспечивать целостность программного продукта и данных</p>
Необходимые знания	<p>Методы и средства сборки и интеграции программных модулей и компонент</p> <p>Интерфейсы взаимодействия с внешней средой</p> <p>Интерфейсы взаимодействия внутренних модулей системы</p> <p>Методы и средства верификации работоспособности выпусков программных продуктов</p> <p>Языки, утилиты и среды программирования, средства пакетного выполнения процедур</p>
ОТФ 4 «Разработка требований и проектирование программного обеспечения»	
Трудовые функции в рамках ОТФ 4	
1. Анализ требований к программному обеспечению	
Трудовые действия	<p>Анализ возможностей реализации требований к программному обеспечению</p> <p>Оценка времени и трудоемкости реализации требований к программному обеспечению</p> <p>Согласование требований к программному обеспечению с заинтересованными сторонами</p> <p>Оценка и согласование сроков выполнения поставленных задач</p>

Продолжение табл. 6

1	2
Необходимые умения	Проводить анализ исполнения требований
	Вырабатывать варианты реализации требований
	Проводить оценку и обоснование рекомендуемых решений
	Осуществлять коммуникации с заинтересованными сторонами
Необходимые знания	Возможности существующей программно-технической архитектуры
	Возможности современных и перспективных средств разработки программных продуктов, технических средств
	Методологии разработки программного обеспечения и технологии программирования
	Методологии и технологии проектирования и использования баз данных
2. Разработка технических спецификаций на программные компоненты и их взаимодействие	
Трудовые действия	Разработка и согласование технических спецификаций на программные компоненты и их взаимодействие с архитектором программного обеспечения
	Распределение заданий между программистами в соответствии с техническими спецификациями
	Осуществление контроля выполнения заданий
	Осуществление обучения и наставничества
	Формирование и предоставление отчетности в соответствии с установленными регламентами
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Выбирать средства реализации требований к программному обеспечению
	Вырабатывать варианты реализации программного обеспечения
	Проводить оценку и обоснование рекомендуемых решений
	Осуществлять коммуникации с заинтересованными сторонами
Необходимые знания	Языки формализации функциональных спецификаций
	Методы и приемы формализации задач
	Методы и средства проектирования программного обеспечения
	Методы и средства проектирования программных интерфейсов
Методы и средства проектирования баз данных	

1	2
3. Проектирование программного обеспечения	
Трудовые действия	Разработка, изменение и согласование архитектуры программного обеспечения с системным аналитиком и архитектором программного обеспечения
	Проектирование структур данных
	Проектирование баз данных
	Проектирование программных интерфейсов
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Использовать существующие типовые решения и шаблоны проектирования программного обеспечения
	Применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов
	Осуществлять коммуникации с заинтересованными сторонами
Необходимые знания	Принципы построения архитектуры программного обеспечения и виды архитектуры программного обеспечения
	Типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения
	Методы и средства проектирования программного обеспечения
	Методы и средства проектирования баз данных
	Методы и средства проектирования программных интерфейсов

3.2. Порядок применения профессиональных стандартов

Порядок применения профессиональных стандартов регламентирован статьей 195.3 ТК РФ¹, введенной в него Федеральным законом от 2 мая 2015 г. № 122-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации и статьи 11 и 73 Федерального закона «Об образовании в Российской Федерации»².

В части 1 этой статьи указано, что если ТК РФ, другими федеральными законами, иными НПА РФ установлены требования к квалификации, необходимой работнику для выполнения определенной

¹ Статья 195.3. Порядок применения профессиональных стандартов.

² Вступил в силу с 1 июля 2016 г. Статья 5 Федерального закона от 2 мая 2015 г. № 122-ФЗ.

трудовой функции, **профессиональные стандарты в части указанных требований обязательны для применения работодателями.**

При этом отмечается, что характеристики квалификации, которые содержатся в профессиональных стандартах и обязательность применения которых не установлена в соответствии с частью 1 статьи 195.3 ТК РФ, применяются работодателями в качестве основы для определения требований к квалификации работников с учетом особенностей выполняемых работниками трудовых функций, обусловленных применяемыми технологиями и принятой организацией производства и труда.

С учетом положений части 3 статьи 195.3 ТК РФ следует иметь в виду, что Минтруд России как ФОИВ, осуществляющий функции по выработке государственной политики и нормативно-правовому регулированию в сфере труда, вправе давать разъяснения по вопросам применения профессиональных стандартов.

В этой связи «Информация» Минтруда России от 10 февраля 2016 г., основанная на положениях статьи 195.3 ТК РФ, в свете обсуждаемого вопроса должна учитываться работодателями в процессе внедрения профессиональных стандартов.

В частности, в этой «Информации» указывается, что статьей 4 Федерального закона от 02.05.2015 № 122-ФЗ **установлено право Правительства РФ с учетом мнения Российской трехсторонней комиссии по регулированию социально-трудовых отношений устанавливать особенности применения профессиональных стандартов в части требований, обязательных для применения государственными внебюджетными фондами Российской Федерации, государственными или муниципальными учреждениями, государственными или муниципальными унитарными предприятиями, а также государственными корпорациями, государственными компаниями и хозяйственными обществами, более пятидесяти процентов акций (долей) в уставном капитале которых находится в государственной собственности или муниципальной собственности.**

Это право Правительство РФ осуществило путем издания 27 июня 2016 г. постановления № 584 «**Об особенностях применения профессиональных стандартов в части требований, обязательных для применения государственными внебюджетными фондами Российской Федерации, государственными или муниципальными учреждениями, государственными или муниципальными унитарными предприятиями, а также государственными корпорациями, государственными компаниями и хозяйственными обществами, более пятидесяти процентов акций (долей) в уставном капитале которых находится в государственной собственности или муниципальной собственности.**».

Согласно пункту 1 этого Постановления профессиональные стандарты в части требований к квалификации, необходимой работнику для

выполнения определенной трудовой функции, **применяются** государственными внебюджетными фондами РФ, государственными или муниципальными учреждениями, **государственными или муниципальными унитарными предприятиями**, а также государственными корпорациями, государственными компаниями и хозяйственными обществами, более 50% акций (долей) в уставном капитале которых находится в государственной собственности или муниципальной собственности, **поэтапно на основе утвержденных указанными организациями с учетом мнений представительных органов работников планов** по организации применения профессиональных стандартов, содержащих в том числе: список профессиональных стандартов, подлежащих применению; этапы применения профессиональных стандартов и другие положения.

В вышеупомянутой Информации Минтруда России от 10 февраля 2016 г. также подчеркивается, что **при составлении штатного расписания**, при заполнении трудовой книжки работника, а также при изменении тарифного разряда в части наименования должности работника **следует руководствоваться действующими** по состоянию на текущую дату Единым тарифно-квалификационным справочником работ и профессий рабочих, Единым квалификационным справочником должностей руководителей, специалистов и служащих и **профессиональными стандартами**.

В заключение обсуждения темы о профессиональных стандартах представляется целесообразным отметить письмо Общероссийского Профсоюза образования от 10 марта 2017 г. № 122, опубликованное в ряде изданий, в частности: «Официальные документы в образовании», № 14, апрель, 2017 и «Солидарность», № 23, 14–21.06.2017, на страницах которых были размещены «Ответы на актуальные вопросы о профессиональных стандартах».

В приложении к этому же письму приводится и вариант формы Плана по организации применения профессиональных стандартов (далее — План), составленный в соответствии с пунктом 1 Постановления № 584, с включением в него следующих данных:

а) списка профессиональных стандартов, подлежащих применению;

б) сведений о потребности в профессиональном образовании, профессиональном обучении и (или) дополнительном профессиональном образовании работников, полученные на основе анализа квалификационных требований, содержащихся в профессиональных стандартах, с учетом кадрового состава организации, а также о проведении соответствующих мероприятий по образованию и обучению в установленном порядке;

в) этапов применения профессиональных стандартов;

г) перечня локальных нормативных актов и других документов, подлежащих изменению, в том числе по вопросам аттестации, сер-

тификации и других форм оценки квалификации работников, в связи с учетом положений профессиональных стандартов, подлежащих применению.

Что касается сроков реализации мероприятий Планов, то важно иметь в виду, что в соответствии с пунктом 2 Постановления № 584 они должны были быть завершены не позднее 1 января 2020 г., что возможно и состоялось.

Уточняйте значение слов, и Вы избавите человечество от половины заблуждений¹.

4. ТЕРМИНЫ, НОРМЫ И ОПРЕДЕЛЕНИЯ ОСНОВНЫХ ПОНЯТИЙ ЗАКОНОДАТЕЛЬСТВА О ЦИФРОВОЙ ЭКОНОМИКЕ И ОБЕСПЕЧЕНИЯ ЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ²

А

Абонент — пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации³.

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники⁴.

Автоматизированная система (Operational system) — информационная система, включая элементы, не связанные с информационной технологией, рассматриваемые с учетом условий ее эксплуатации⁵.

Автоматизированная система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций⁶.

¹ Рене Декарт — французский математик, физик, естествоиспытатель и философ (1596–1650).

² Для ряда терминов, норм и определений приведены эквиваленты на английском языке.

³ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁴ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

⁵ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

⁶ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

Автоматизированная система управления — комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления таким оборудованием и процессами¹.

Автоматизированное рабочее место — программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида. **Примечание.** Видами АРМ, например, являются АРМ оператора-технолога, АРМ инженера, АРМ проектировщика, АРМ бухгалтера и др.²

Автоматизированный производственный комплекс — автоматизированный комплекс, согласованно осуществляющий автоматизированную подготовку производства, само производство и управление им³.

Автоматизированный процесс — процесс, осуществляемый при совместном участии человека и средств автоматизации⁴.

Автоматический процесс — процесс, осуществляемый без участия человека⁵.

Авторизация — проверка, подтверждение и предоставление прав логического доступа при осуществлении субъектами доступа логического доступа⁶.

Агент (Agent) — отдельное лицо, рабочая группа или организация, ответственная за/или вовлеченная в процессы создания, ввода и/или управления документами. **Примечание.** Технологические инструменты, такие как программные приложения, могут считаться агентами, если они выполняют операции с документами⁷.

¹ Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Статья 2 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Приложение 1 — извлечение.

⁴ Там же.

⁵ Там же.

⁶ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденно приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁷ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Инфор-

Адаптивность автоматизированной системы — способность АС изменяться для сохранения своих эксплуатационных показателей в заданных пределах при изменениях внешней среды¹.

Административные данные — используемая при формировании официальной статистической информации документированная информация, получаемая федеральными органами государственной власти, иными федеральными государственными органами, органами государственной власти субъектов РФ, иными государственными органами субъектов РФ, органами МСУ, государственными организациями в связи с осуществлением ими разрешительных, регистрационных, контрольно-надзорных и других административных функций, а также иными организациями, на которые осуществление указанных функций возложено законодательством РФ².

Административный регламент — нормативный правовой акт, устанавливающий порядок предоставления государственной или муниципальной услуги и стандарт предоставления государственной или муниципальной услуги³.

Администратор — пользователь, на имя которого зарегистрировано доменное имя в Реестре⁴.

Администратор защиты (Security administrator) — субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации⁵.

Администрирование — осуществление администратором прав и обязанностей, установленных настоящими Правилами⁶.

мация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Статья 2 — извлечение.

³ Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

⁴ Правила регистрации доменных имен в доменах .RU и .RF (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

⁵ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁶ Правила регистрации доменных имен в доменах .RU и .RF (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

Адрес — описание места нахождения объекта адресации, структурированное в соответствии с принципами организации местного самоуправления в Российской Федерации и включающее в себя в том числе наименование элемента улично-дорожной сети и (или) наименование элемента планировочной структуры (при необходимости), а также цифровое и (или) буквенно-цифровое обозначение объекта адресации, позволяющее его идентифицировать¹.

Аккредитация удостоверяющего центра — признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона².

Активы (Asset) — все, что имеет ценность для организации³.

Актуализация информационного ресурса — составная часть ведения информационного ресурса, предусматривающая его гармонизацию с доверенным источником (доверенными источниками)⁴.

Акты общего регулирования — нормативные правовые акты Российской Федерации, в том числе федеральные законы, акты Президента Российской Федерации, Правительства Российской Федерации, федеральных органов исполнительной власти, государственных корпораций, а также нормативные акты Банка России⁵.

Алгоритм — конечный набор предписаний для получения решения задачи посредством конечного количества операций⁶.

Алгоритм проектирования в САПР — совокупность предписаний, необходимых для выполнения проектирования⁷.

¹ Федеральный закон от 28 декабря 2013 г. № 443-ФЗ «О федеральной информационной адресной системе и о внесении изменений в Федеральный закон «Об общих принципах организации местного самоуправления в Российской Федерации». Статья 2 — извлечение.

² Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

³ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

⁴ Проект в редакции от 4 июля 2018 г. Федерального закона «О систематизации и гармонизации информации в Российской Федерации». Статья 2 — извлечение.

⁵ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

⁶ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Приложение 1 — извлечение.

⁷ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные

Алгоритм функционирования автоматизированной системы — алгоритм, задающий условия и последовательность действий компонентов автоматизированной системы при выполнении ею своих функций¹.

Алиби — нахождение подозреваемого или обвиняемого в момент совершения преступления в другом месте².

Анализ информационного риска — систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации³.

Анализ риска (Risk analysis) — систематическое использование информации для определения источников риска и количественной оценки риска⁴.

Анализ рисков (Risk analysis) — системный подход к определению величины риска⁵.

Аннулирование регистрации — исключение информации о доменном имени из Реестра⁶.

Апелляционная инстанция — суд, рассматривающий в апелляционном порядке уголовные дела по жалобам и представлениям на не вступившие в законную силу приговоры, определения и постановления суда⁷.

системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

¹ Там же.

² Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

³ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁴ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

⁵ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

⁶ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

⁷ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

Архитектура (системы) (Architecture) — основные понятия или свойства системы в окружающей среде, воплощенной в ее элементах, отношениях и конкретных принципах ее проекта и развития¹.

Архитектура вычислительной машины — концептуальная структура вычислительной машины, определяющая проведение обработки информации и включающая методы преобразования информации в данные и принципы взаимодействия технических средств и программного обеспечения².

Архитектурное представление (Architecture view) — рабочий продукт, выражающий архитектуру некоторой системы с точки зрения определенных системных интересов³.

Аттестация объекта в защищенном исполнении — официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов и норм эффективности защиты информации⁴.

Аудит (Audit) — независимая оценка рабочего продукта или множества рабочих продуктов на их соответствие спецификациям, стандартам, контрактным соглашениям и иным критериям⁵.

Аудит информационной безопасности в организации (Аудиторская проверка информационной безопасности в организации) — периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности. **Примечание.** Аудит информационной безопасности в организации может осуществляться независимой организацией (третьей стороной) по до-

¹ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31.10.2016 № 1538-ст). Раздел 4 — извлечение.

² ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Положение о государственном лицензировании деятельности в области защиты информации (утверждено решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

⁵ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

говору с проверяемой организацией, а также подразделением или должностным лицом организации (внутренний аудит)¹.

Аудиторская проверка информационной безопасности в организации (Аудит информационной безопасности в организации) — периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности. **Примечание.** Аудит информационной безопасности в организации может осуществляться независимой организацией (третьей стороной) по договору с проверяемой организацией, а также подразделением или должностным лицом организации (внутренний аудит)².

Аутентификационные данные — данные в любой форме и на любом носителе, известные или принадлежащие легальному субъекту доступа — легальному владельцу аутентификационных данных, или данные, которыми обладает легальный субъект доступа, используемые для выполнения процедуры аутентификации при осуществлении логического доступа³.

Аутентификация (Authentication) — проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности⁴.

Аутентификация — проверка при осуществлении логического доступа принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)⁵.

¹ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

² ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁴ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁵ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

Аутентификация, идентификация лица — совокупность мероприятий по установлению идентификаторов и (или) сведений о лице, сопоставлению данных сведений с идентификатором или проверке данных сведений, а также по проверке лица на принадлежность лицу идентификатора (идентификаторов) посредством сопоставления идентификатора (идентификаторов) с имеющимися сведениями о лице, и установления обоснованности использования лицом идентификатора (идентификаторов), осуществляемых в соответствии с настоящим Федеральным законом, иными федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением сторон, в результате которых лицо считается установленным¹.

Аффилированные лица — физические и юридические лица, способные оказывать влияние на деятельность юридических и (или) физических лиц, осуществляющих предпринимательскую деятельность².

Аффилированные лица физического лица, осуществляющего предпринимательскую деятельность: лица, принадлежащие к той группе лиц, к которой принадлежит данное физическое лицо; юридическое лицо, в котором данное физическое лицо имеет право распоряжаться более чем 20 процентами общего количества голосов, принадлежащих на голосующие акции либо составляющие уставный или складочный капитал вклады, доли данного юридического лица³.

Аффилированные лица юридического лица: член его Совета директоров (наблюдательного совета) или иного коллегиального органа управления, член его коллегиального исполнительного органа, а также лицо, осуществляющее полномочия его единоличного исполнительного органа; лица, принадлежащие к той группе лиц, к которой принадлежит данное юридическое лицо; лица, которые имеют право распоряжаться более чем 20 процентами общего количества голосов, принадлежащих на голосующие акции либо составляющие уставный или складочный капитал вклады, доли данного юридического лица; юридическое лицо, в котором данное юридическое лицо имеет право распоряжаться более чем 20 процентами общего количества голосов, принадлежащих на голосующие акции либо составляющие уставный или складочный капитал вклады, доли данного юридического лица; члены Советов директоров (наблюдательных советов) или иных коллегиальных органов управления, коллегиальных исполнительных органов участников финансово-промышленной группы, а также

¹ Пункт 18.2 статьи 2 Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» в ред. проекта № 260319.

² Закон РСФСР от 22 марта 1991 г. № 948-1 «О конкуренции и ограничении монополистической деятельности на товарных рынках». Статья 4 — извлечение.

³ Там же.

лица, осуществляющие полномочия единоличных исполнительных органов участников финансово-промышленной группы¹.

Б

База данных перенесенных абонентских номеров — информационная система, содержащая сведения об абонентских номерах, которые сохраняются абонентами при заключении новых договоров об оказании услуг связи с другими операторами подвижной радиотелефонной связи, и об указанных операторах связи, заключивших такие договоры².

Базовая линия (Baseline) — формально утвержденная версия объектов конфигурации, независимо от средств и способов представления, которая была официально рассмотрена и согласована в специальное время в течение жизненного цикла объектов конфигурации³.

Базовая организация — организация, осуществляющая в соответствии с Положением о создании и функционировании советов по приоритетным направлениям научно-технологического развития Российской Федерации, утвержденным постановлением Правительства Российской Федерации от 17 января 2018 г. № 16 «Об утверждении Положения о создании и функционировании советов по приоритетным направлениям научно-технологического развития Российской Федерации», организационное, техническое и информационное обеспечение деятельности совета по приоритетному направлению научно-технологического развития Российской Федерации (далее — совет по приоритетному направлению)⁴.

Базовый образ виртуальной машины — образ виртуальной машины, используемый в качестве первоначального образа при запуске (загрузке) виртуальной машины⁵.

¹ Закон РСФСР от 22 марта 1991 г. № 948-1 «О конкуренции и ограничении монополистической деятельности на товарных рынках». Статья 4 — извлечение.

² Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

⁵ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии

Байт — единица представления данных в виде групп из 8 бит¹.

Банк — кредитная организация, которая имеет исключительное право осуществлять в совокупности следующие банковские операции: привлечение во вклады денежных средств физических и юридических лиц, размещение указанных средств от своего имени и за свой счет на условиях возвратности, платности, срочности, открытие и ведение банковских счетов физических и юридических лиц².

Банковский платежный агент — юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются кредитной организацией в целях осуществления отдельных банковских операций³.

Банковский платежный субагент — юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются банковским платежным агентом в целях осуществления отдельных банковских операций⁴.

Банкомат — автоматическое (без участия уполномоченного лица кредитной организации, или банковского платежного агента, или банковского платежного субагента) устройство для осуществления расчетов, обеспечивающее возможность выдачи и (или) приема наличных денежных средств, в том числе с использованием электронных средств платежа, и по передаче распоряжений кредитной организации об осуществлении перевода денежных средств⁵.

Безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз⁶.

Безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз или опасностей⁷.

от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

¹ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

² Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности». Статья 1 — извлечение.

³ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁴ Там же.

⁵ Там же.

⁶ Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности». Статья 1 — извлечение

⁷ ГОСТ Р 22.0.02-94 (в ред. Изменения № 1, принятого постановлением Госстандарта РФ от 31 мая 2000 г. № 148-ст) «Безопасность в чрезвычайных ситуациях. Определения основных понятий». Принят и введен в действие постановлением Госстандарта РФ от 22 декабря 1994 г. № 327 (Группа Т 00, ОКСТУ 0022). Извлечение.

Безопасность информации (Information security) — состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз¹.

Безопасность информации — состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.²

Безопасность информации (данных) — состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность³.

Безопасность критической информационной инфраструктуры — состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак⁴.

Безопасность продукции и связанных с ней процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации (далее — безопасность) — состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений⁵.

Безопасные программное обеспечение и сервис — программное обеспечение и сервис, сертифицированные на соответствие требованиям к информационной безопасности, устанавливаемым федеральным органом исполнительной власти, уполномоченным в области бес-

¹ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

² Положение о государственном лицензировании деятельности в области защиты информации (утверждено решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

³ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁴ Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Статья 2 — извлечение.

⁵ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

печения безопасности, или федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации¹.

Безотзывность перевода денежных средств — характеристика перевода денежных средств, обозначающая отсутствие или прекращение возможности отзыва распоряжения об осуществлении перевода денежных средств в определенный момент времени².

Безусловность перевода денежных средств — характеристика перевода денежных средств, обозначающая отсутствие условий или выполнение всех условий для осуществления перевода денежных средств в определенный момент времени³.

Бизнес-процесс — совокупность взаимосвязанных действий, направленных на создание определенного продукта или услуги для потребителей⁴.

Бит — двоичная единица представления данных⁵.

Близкие лица — иные, за исключением близких родственников и родственников, лица, состоящие в свойстве с потерпевшим, свидетелем, а также лица, жизнь, здоровье и благополучие которых дороги потерпевшему, свидетелю в силу сложившихся личных отношений⁶.

Бликие родственники — супруг, супруга, родители, дети, усыновители, усыновленные, родные братья и родные сестры, бабушка, бабушка, внуки⁷.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)⁸.

¹ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

² Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

³ Там же.

⁴ Пункт 8 Методических рекомендаций по подготовке корпоративных планов импортозамещения государственными корпорациями, государственными компаниями, акционерными обществами, в уставном капитале которых доля участия Российской Федерации превышает 50 процентов, организациями, реализующими инвестиционные проекты, включенные в реестр инвестиционных проектов в соответствии с решением Правительственной комиссии по импортозамещению, утвержденных распоряжением Минэкономразвития России от 11 августа 2016 г. № 219Р-АУ.

⁵ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁶ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁷ Там же.

⁸ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

Большие данные — обозначение структурированных и неструктурированных данных огромных объемов и значительного многообразия, эффективно обрабатываемых горизонтально масштабируемыми программными инструментами¹.

Бортовая ЭВМ — специализированная ЭВМ, предназначенная для установки на подвижном объекте².

Брешь (уязвимость информационной системы) — свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Примечания. 1. Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе. 2. Если уязвимость соответствует угрозе, то существует риск³.

Быстроразвивающиеся опасные природные явления и техногенные процессы — негативные явления и процессы, определенные в ходе прогнозирования угрозы возникновения чрезвычайных ситуаций, локализация и ликвидация которой требуют заблаговременной подготовки сил и средств единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций⁴.

В

Валидатор — юридическое или физическое лицо, являющееся участником реестра цифровых транзакций и осуществляющее деятельность по валидации цифровых записей в реестре цифровых транзакций в соответствии с правилами ведения реестра цифровых транзакций⁵.

Валидация, аттестация (Validation) — подтверждение (на основе представления объективных подтверждений) того, что требования, предназначенные для конкретного использования или применения, выполнены. Примечание. Валидация в контексте **жизненного цикла** представляет собой совокупность действий, гарантирующих

¹ Распоряжение Правительства РФ от 17 декабря 2019 г. № 3074-р «Концепция создания цифровой аналитической платформы». Пункт 1 — извлечение.

² ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

³ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁴ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

⁵ Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

и обеспечивающих уверенность в том, что система способна реализовать свое предназначение, текущие и перспективные цели¹.

Валидация цифровой записи — юридически значимое действие по подтверждению действительности цифровых записей в реестре цифровых транзакций, осуществляемое в порядке, установленном правилами ведения реестра цифровых транзакций².

Ввод в эксплуатацию — событие, фиксирующее готовность изделия к использованию по назначению, документально оформленное в установленном порядке. **Примечание.** Для специальных видов техники к вводу в эксплуатацию дополнительно относят подготовительные работы, контроль, приемку и закрепление изделия за эксплуатирующим подразделением³.

Ввод данных — операция чтения данных с носителя, запись этих данных в память данных⁴.

Веб-сбор — единая система сбора и обработки статистической информации информационно-вычислительной системы Федеральной службы государственной статистики в части электронного сбора данных⁵.

Ведомственная отчетность — отчетность, собираемая федеральными органами исполнительной власти в связи с осуществлением ими управленческих функций (кроме административных данных и официальной статистической отчетности)⁶.

Ведомственный проект — проект, обеспечивающий достижение целей и показателей деятельности федерального органа исполнительной власти⁷.

Вердикт — решение о виновности или невиновности подсудимого, вынесенное коллегией присяжных заседателей⁸.

¹ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

² Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

³ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ Распоряжение Правительства РФ от 17 декабря 2019 г. № 3074-р «Концепция создания цифровой аналитической платформы». Пункт 1 — извлечение.

⁶ Там же.

⁷ Пункт 3 Положения об организации проектной деятельности в Правительстве Российской Федерации, в ред. постановления Правительства РФ от 31 октября 2018 г. № 1288 (ред. от 30.07.2019) «Об организации проектной деятельности в Правительстве Российской Федерации». Извлечение.

⁸ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

Верификация (Verification) — процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие¹.

Верификация (Verification) — подтверждение (на основе предоставления объективных подтверждений) того, что заданные требования полностью выполнены. **Примечание.** Верификация в контексте **жизненного цикла** представляет собой совокупность действий по сравнению полученного результата **жизненного цикла** с требуемыми характеристиками для этого результата. Результатами **жизненного цикла** могут являться (но не ограничиваться ими) заданные требования, описание проекта и непосредственно система².

Верификация (Verification) — процессы оценки, используемые для подтверждения того, что меры обеспечения безопасности для автоматизированной системы реализованы корректно, и их применение является эффективным³.

Ветеринарно-санитарные и фитосанитарные меры — обязательные для исполнения требования и процедуры, устанавливаемые в целях защиты от рисков, возникающих в связи с проникновением, закреплением или распространением вредных организмов, заболеваний, переносчиков болезней или болезнетворных организмов, в том числе в случае переноса или распространения их животными и (или) растениями, с продукцией, грузами, материалами, транспортными средствами, с наличием добавок, загрязняющих веществ, токсинов, вредителей, сорных растений, болезнетворных организмов, в том числе с пищевыми продуктами или кормами, а также обязательные для исполнения требования и процедуры, устанавливаемые в целях предотвращения иного связанного с распространением вредных организмов ущерба⁴.

Веба — конечный итог реализации одного или нескольких мероприятий федерального проекта Программы, имеющий самостоятельное значение и ожидаемые результаты (эффекты), значимые для государства, бизнеса или общества⁵.

¹ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Госстандарта России от 30 марта 1992 г.

² ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

³ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

⁴ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

⁵ Пункт 3 Положения о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации», утвержденного постанов-

Вещатель — российское юридическое лицо, осуществляющее формирование телеканала или радиоканала и его распространение в установленном порядке на основании лицензии на телевизионное вещание, радиовещание¹.

Взаимодействие автоматизированных систем — обмен данными, командами и сигналами между функционирующими АС².

Взаимодействие информационных систем электронного документооборота — обмен электронными сообщениями (ведение служебной переписки в электронной форме) между участниками межведомственного электронного документооборота, в том числе:

- а) направление и получение в электронной форме решений и поручений Президента РФ и Правительства РФ;
- б) получение информации о ходе рассмотрения участниками межведомственного электронного документооборота электронных сообщений, в том числе поручений Президента РФ и Правительства РФ;
- в) направление в электронной форме докладов Президенту РФ и Правительству РФ;
- г) внесение в Правительство РФ ФОИВ проектов НПА, в том числе в электронной форме;
- д) осуществление участниками межведомственного электронного документооборота согласительных процедур по проектам НПА в электронной форме;
- е) направление в электронной форме НПА ФОИВ на государственную регистрацию в Министерство юстиции Российской Федерации³.

Вид профессиональной деятельности — совокупность обобщенных трудовых функций, имеющих близкий характер, результаты и условия труда⁴.

лением Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации». Извлечение.

¹ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Постановление Правительства РФ от 22 сентября 2009 г. № 754 «Об утверждении Положения о системе межведомственного электронного документооборота». Пункт 4 Положения — извлечение.

⁴ Приказ Минтруда России от 29 апреля 2013 г. № 170н «Об утверждении методических рекомендаций по разработке профессионального стандарта». Пункт 2 — извлечение.

Виртуальный — определение, характеризующее процесс или устройство в системе обработки информации кажущихся реально существующими, поскольку все их функции реализуются какими-либо другими средствами¹.

Владелец сайта в сети «Интернет» — лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте².

Владелец сертификата ключа проверки электронной подписи — лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи³.

Внедрение инновационного решения — процесс создания и/или приобретения инновационного решения и его применение для решения задач Заказчика⁴.

Внедряемый компонент — шлюз системы межведомственного электронного документооборота (далее — шлюз), который является программно-техническим комплексом, выполняющим функции по обеспечению обмена электронными сообщениями с системой электронного документооборота и обеспечивающим хранение, просмотр, поиск и выгрузку (загрузку) электронных сообщений. Шлюз состоит из объединенных в локальную информационно-телекоммуникационную сеть сервера базы данных шлюза и автоматизированного рабочего места шлюза. В составе шлюза развертывается клиентское программное обеспечение комплекса программ «Почтовая служба»⁵.

Внемашинная информационная база автоматизированной системы — часть информационной базы АС, представляющая собой сово-

¹ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

² Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

³ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

⁴ Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/Д01и «О направлении методических материалов» (вместе с Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

⁵ Распоряжение Правительства РФ от 2 октября 2009 г. № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти». Извлечение.

купность документов, предназначенных для непосредственного восприятия человеком без применения средств вычислительной техники¹.

Внешняя автоматизированная система (External operational system) — отдельная автоматизированная система, которая имеет связи с автоматизированной системой, являющейся объектом оценки².

Внешняя память — память, данные в которой доступны центральному процессору посредством операции ввода-вывода³.

Военная техника — технические средства, предназначенные для боевого, технического и тылового обеспечения деятельности войск, а также оборудование и аппаратура для контроля и испытаний этих средств, составные части этих средств и комплектующие изделия⁴.

Военные объекты — боевые позиции войск, воинские части, стационарные пункты управления, военные научно-исследовательские организации, полигоны, узлы связи, базы, склады, комплексы или отдельные здания и другие сооружения военного назначения⁵.

Войска — Вооруженные Силы Российской Федерации, другие войска, воинские формирования, органы и создаваемые на военное время специальные формирования, предусмотренные Федеральным законом от 31 мая 1996 г. № 61-ФЗ «Об обороне», а также подразделения связи специального назначения⁶.

Вооружение — средства, предназначенные для поражения живой силы, техники, сооружений и других объектов противника, составные части этих средств и комплектующие изделия⁷.

Впервые выпускаемая в обращение продукция — продукция, которая ранее не находилась в обращении на территории Российской Фе-

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

³ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁴ Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне». Примечания, пункт 3 — извлечение.

⁵ Там же.

⁶ Там же.

⁷ Там же.

дерации либо которая ранее выпускалась в обращение и свойства или характеристики которой были впоследствии изменены¹.

Вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы².

Вредоносная программа — программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы³.

Вспомогательная функция автоматизированной системы управления технологическим процессом — функция АСУ технологическим процессом, включающая сбор и обработку данных о состоянии АСУТП и либо представление этой информации персоналу системы или осуществление управляющих воздействий на соответствующие технические и/или программные средства АСУТП⁴.

Вспомогательный информационный ресурс — информационный ресурс, содержащий информацию, используемую исключительно для формирования и ведения не более одного регламентного информационного ресурса⁵.

Входная информация автоматизированной системы — информация, поступающая в АС в виде документов, сообщений, данных, сигналов, необходимая для выполнения функций АС⁶.

Вывод данных — операция чтения данных в памяти данных и последующая их запись на носитель данных или отображение на экране⁷.

¹ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

² ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

³ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁵ Проект в редакции от 4 июля 2018 г. Федерального закона «О систематизации и гармонизации информации в Российской Федерации». Статья 2 — извлечение.

⁶ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁷ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

Выделение полосы радиочастот — разрешение в письменной форме на использование конкретной полосы радиочастот, в том числе для разработки, модернизации, производства в Российской Федерации и (или) ввоза в Российскую Федерацию радиоэлектронных средств или высокочастотных устройств с определенными техническими характеристиками¹.

Высокопроизводительные рабочие места — замещенные рабочие места российской организации, производительность труда которых равна или превышает среднеотраслевое значение².

Высокотехнологичная промышленная продукция — продукция, включенная в перечень высокотехнологичной продукции, утверждаемый Министерством промышленности и торговли Российской Федерации³.

Высокочастотные устройства — оборудование или приборы, предназначенные для генерирования и использования радиочастотной энергии в промышленных, научных, медицинских, бытовых или других целях, за исключением применения в области электросвязи⁴.

Выходная информация автоматизированной системы — информация, получаемая в результате выполнения функций АС и выдаваемая на объект ее деятельности, пользователю или в другие системы⁵.

Выход, выходной результат процесса (Process outcome) — наблюдаемый результат успешного достижения цели процесса.

Вычислительная машина — совокупность технических средств, создающая возможность проведения обработки информации и получение результата в необходимой форме. **Примечание.** Как правило, в состав ВМ входит и системное программное обеспечение⁶.

¹ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

² Пункт 2 Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции, утвержденных постановлением Правительства РФ от 30 апреля 2019 г. № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции». Извлечение.

³ Там же.

⁴ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

Г

Гарантия качества (Quality assurance) — часть менеджмента качества, сосредоточенная на предоставлении уверенности в том, что требования к качеству будут выполнены¹.

Гармонизация информации — приведение информации в соответствие с доверенным источником путем применения установленных настоящим Федеральным законом методов гармонизации информации².

Главный редактор — лицо, возглавляющее редакцию (независимо от наименования должности) и принимающее окончательные решения в отношении производства и выпуска средства массовой информации³.

Головная организация интегрированной структуры оборонно-промышленного комплекса — юридическое лицо, которое входит в интегрированную структуру оборонно-промышленного комплекса и имеет возможность определять решения, принимаемые остальными юридическими лицами⁴.

Государственная информационная система промышленности — федеральная государственная информационная система, содержащая информацию о состоянии отраслей промышленности и прогнозе их развития⁵.

Государственная пошлина — единственный и достаточный платеж за совершение государственным органом юридически значимых действий, к каковым приравнена выдача документов, включая водительские удостоверения⁶ (Определение Конституционного Суда РФ от 1 марта 2007 г. № 326-О-П)⁷.

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разве-

¹ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

² Проект в редакции от 4 июля 2018 г. Федерального закона «О систематизации и гармонизации информации в Российской Федерации». Статья 2 — извлечение.

³ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

⁴ Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

⁵ Там же.

⁶ Определение дано на основании положения статей 8 и 333.16 и подпункта 36 пункта 1 статьи 333.33 Налогового кодекса Российской Федерации в соответствии с примечанием СПС «КонсультантПлюс» к статье 8 Налогового кодекса Российской Федерации (часть первая) от 31 июля 1998 г. № 146-ФЗ.

⁷ Налоговый кодекс Российской Федерации (часть первая) от 31 июля 1998 г. № 146-ФЗ. Статья 8 — извлечение.

дывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации¹.

Государственная услуга, предоставляемая федеральным органом исполнительной власти, органом государственного внебюджетного фонда, исполнительным органом государственной власти субъекта Российской Федерации, а также органом местного самоуправления при осуществлении отдельных государственных полномочий, переданных федеральными законами и законами субъектов Российской Федерации — деятельность по реализации функций соответственно федерального органа исполнительной власти, государственного внебюджетного фонда, исполнительного органа государственной власти субъекта Российской Федерации, а также органа местного самоуправления при осуществлении отдельных государственных полномочий, переданных федеральными законами и законами субъектов Российской Федерации (далее — органы, предоставляющие государственные услуги), которая осуществляется по запросам заявителей в пределах установленных нормативными правовыми актами Российской Федерации и нормативными правовыми актами субъектов Российской Федерации полномочий органов, предоставляющих государственные услуги².

Государственно-частное партнерство, муниципально-частное партнерство — юридически оформленное на определенный срок и основанное на объединении ресурсов, распределении рисков сотрудничество публичного партнера, с одной стороны, и частного партнера, с другой стороны, которое осуществляется на основании соглашения о государственно-частном партнерстве, соглашения о муниципально-частном партнерстве, заключенных в соответствии с настоящим Федеральным законом в целях привлечения в экономику частных инвестиций, обеспечения органами государственной власти и органами местного самоуправления доступности товаров, работ, услуг и повышения их качества³.

Государственные органы — органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и иные государственные органы, образуемые в соот-

¹ Закон Российской Федерации о государственной тайне от 21 июля 1993 года № 5485-1. Статья 2 — извлечение.

² Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

³ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

ветствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации¹.

Государственный адресный реестр — государственный информационный ресурс, содержащий сведения об адресах².

Государственный заказчик — государственный орган (в том числе орган государственной власти), Государственная корпорация по атомной энергии «Росатом», Государственная корпорация по космической деятельности «Роскосмос», орган управления государственным внебюджетным фондом либо государственное казенное учреждение, действующие от имени Российской Федерации или субъекта Российской Федерации, уполномоченные принимать бюджетные обязательства в соответствии с бюджетным законодательством Российской Федерации от имени Российской Федерации или субъекта Российской Федерации и осуществляющие закупки³.

Государственный контракт, муниципальный контракт — гражданско-правовой договор, предметом которого являются поставка товара, выполнение работы, оказание услуги (в том числе приобретение недвижимого имущества или аренда имущества) и который заключен от имени Российской Федерации, субъекта Российской Федерации (государственный контракт), муниципального образования (муниципальный контракт) государственным или муниципальным заказчиком для обеспечения соответственно государственных нужд, муниципальных нужд⁴.

Государственный обвинитель — поддерживающее от имени государства обвинение в суде по уголовному делу должностное лицо органа прокуратуры⁵.

Гриф секретности — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляе-

¹ Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Статья 1 — извлечение.

² Федеральный закон от 28 декабря 2013 г. № 443-ФЗ «О федеральной информационной адресной системе и о внесении изменений в Федеральный закон «Об общих принципах организации местного самоуправления в Российской Федерации». Статья 2 — извлечение.

³ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Пункт 5 статьи 3 — извлечение.

⁴ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Пункт 8 статьи 3 — извлечение.

⁵ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

мые на самом носителе и (или) в сопроводительной документации на него¹.

Группа реагирования на инциденты защиты информации — действующая на постоянной основе группа работников финансовой организации и (или) иных лиц, привлекаемых ею, которая выполняет регламентированные в финансовой организации процедуры реагирования на инциденты защиты информации².

Д

Данные — информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека³.

Действие процессуальное — следственное, судебное или иное действие, предусмотренное УПК РФ⁴.

Декларация о соответствии — документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов⁵.

Декларирование соответствия — форма подтверждения соответствия продукции требованиям технических регламентов; декларация о соответствии — документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов⁶.

Делегирование домена — размещение и хранение информации о доменном имени и соответствующих ему серверах DNS на серверах DNS домена верхнего уровня, что является необходимым условием для функционирования доменной адресации в сети Интернет⁷.

¹ Закон Российской Федерации о государственной тайне от 21 июля 1993 г. № 5485-1. Статья 2 — извлечение.

² ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

³ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁵ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

⁶ Там же.

⁷ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

Деятельность, действие (Activity) — множество связанных задач процесса¹.

Деятельность (Activity) — основная задача, выполняемая деловой структурой в рамках ее функций².

Диалоговый режим — режим взаимодействия человека с системой обработки информации, при котором человек и система обмениваются информацией в темпе, который соизмерим с темпом обработки информации человеком³.

Диалоговый режим выполнения функции автоматизированной системы — режим выполнения функции АС, при котором человек управляет решением задачи, изменяя ее условия и (или) порядок функционирования АС на основе оценки информации, представляемой ему техническими средствами АС⁴.

Динамический анализ исходных текстов программ — совокупность методов контроля (не) соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на идентификации фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе проведения статического анализа⁵.

Дискретно выполняемая функция автоматизированной системы управления технологическим процессом — функция АСУ технологическим процессом, выполняемая по запросу или временному регламенту⁶.

¹ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

² ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

³ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁵ Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114). Пункт 2 — извлечение.

⁶ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

Дискреционное управление доступом (Discretionary access control) — ограничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту¹.

Дислокация объекта — совокупность сведений о местоположении на земной поверхности или в ее недрах объекта, в том числе географические, геоцентрические или прямоугольные координаты, линейные и угловые величины, привязка к ориентирам на местности².

Диспетчер доступа (ядро защиты) (Security kernel) — технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа³.

Доверенная третья сторона — юридическое лицо, осуществляющее деятельность по проверке электронной подписи в электронных документах в конкретный момент времени в отношении лица, подписавшего электронный документ, для обеспечения доверия при обмене данными и электронными документами и иные функции, предусмотренные настоящим Федеральным законом⁴.

Доверенный источник — информационный ресурс, определенный в качестве основы для гармонизации⁵.

Дознаватель — должностное лицо органа дознания, правомочное либо уполномоченное начальником органа дознания осуществлять предварительное расследование в форме дознания, а также иные полномочия, предусмотренные УПК РФ⁶.

Дознание — форма предварительного расследования, осуществляемого дознавателем (следователем), по уголовному делу, по которому производство предварительного следствия необязательно⁷.

Доказательство (Evidence) — документация о транзакции (деловой операции). **Примечание.** Документальное подтверждение совершения

¹ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

² Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне». Примечания, пункт 3 — извлечение

³ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁴ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2, пункт 17 — извлечение.

⁵ Проект в редакции от 4 июля 2018 г. Федерального закона «О систематизации и гармонизации информации в Российской Федерации». Статья 2 — извлечение.

⁶ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁷ Там же.

транзакции (деловой операции), созданное при обычных условиях ведения деятельности и являющееся целостным (неповрежденным) и полным. Этот термин применяется не только в юридическом смысле¹.

Документация на автоматизированную систему — комплект взаимоувязанных документов, полностью определяющих технические требования к АС, проектные и организационные решения по созданию и функционированию АС².

Документация на автоматизированную систему — комплекс взаимоувязанных документов, в котором полностью описаны все решения по созданию и функционированию системы, а также документов, подтверждающих соответствие системы требованиям технического задания и готовность ее к эксплуатации (функционированию)³.

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель⁴.

Документная система (Records system) — информационная система, обеспечивающая управление документами и доступ к ним в течение определенного времени. **Примечание.** Документная система может состоять из технических элементов, таких как программное обеспечение, которое может быть специально разработано для управления документами либо для какой-либо другой коммерческой цели, а также нетехнических элементов, включая политику, процедуры, людей и других агентов, а также распределение обязанностей⁵.

¹ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ ГОСТ 34.201-89 «Государственный стандарт Союза ССР. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (утв. постановлением Госстандарта СССР от 24 марта 1989 г. № 664). Приложение 1 — извлечение.

⁴ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁵ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

Документы (Records) — документированная информация, созданная, полученная и сохраняемая организацией или частным лицом в качестве доказательства и актива для подтверждения правовых обязательств или деловой транзакции¹.

Должностное лицо — лицо, постоянно, временно или по специальному полномочию осуществляющее функции представителя власти либо выполняющее организационно-распорядительные, административно-хозяйственные функции в государственном органе или органе местного самоуправления².

Домен — область (ветвь) иерархического пространства доменных имен, обозначаемая уникальным доменным именем и обслуживаемая набором серверов DNS (DNS — domain name system — система доменных имен)³.

Домен .РФ — домен верхнего уровня с уникальным обозначением «рф»⁴.

Домен .RU — домен верхнего уровня с уникальным обозначением «ru»⁵.

Домен безопасности (Security domain) — часть автоматизированной системы, которая реализует одни и те же политики безопасности⁶.

Доменное имя — обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет»⁷.

Доменное имя — символьное обозначение, предназначенное для сетевой адресации, в которой используется система доменных имен (DNS)⁸.

Допуск к государственной тайне — процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну,

¹ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

² Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращения граждан Российской Федерации». Статья 4 — извлечение.

³ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

⁴ Там же.

⁵ Там же.

⁶ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие Приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

⁷ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁸ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

а предприятий, учреждений и организаций — на проведение работ с использованием таких сведений¹.

Доступ (Access) — право, возможность, средства, обеспечивающие поиск, использование или извлечение информации².

Доступ к информации (Access to information) — ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации³.

Доступ к информации — возможность получения информации и ее использования⁴.

Доступ к информации, составляющей коммерческую тайну — ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации⁵.

Доступ к сведениям, составляющим государственную тайну — санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну⁶.

Доступность (Availability) — свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта⁷.

Досудебное производство — уголовное судопроизводство с момента получения сообщения о преступлении до направления прокурором уголовного дела в суд для рассмотрения его по существу⁸.

¹ Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне». Статья 2 — извлечение.

² ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

³ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁴ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁵ Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Статья 3 — извлечение.

⁶ Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне». Статья 2 — извлечение.

⁷ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

⁸ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

Досудебное соглашение о сотрудничестве — соглашение между сторонами обвинения и защиты, в котором указанные стороны согласовывают условия ответственности подозреваемого или обвиняемого в зависимости от его действий после возбуждения уголовного дела или предъявления обвинения¹.

Е

Единая информационная система в сфере закупок (единая информационная система) — совокупность информации, указанной в части 3 статьи 4 настоящего Федерального закона и содержащейся в базах данных, информационных технологий и технических средств, обеспечивающих формирование, обработку, хранение такой информации, а также ее предоставление с использованием официального сайта единой информационной системы в информационно-телекоммуникационной сети «Интернет» (официальный сайт)².

Единая система идентификации и аутентификации — федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах³.

Ж

Жалоба — просьба гражданина о восстановлении или защите его нарушенных прав, свобод или законных интересов либо прав, свобод или законных интересов других лиц⁴.

Жалоба на нарушение порядка предоставления государственной или муниципальной услуги — требование заявителя или его законного представителя о восстановлении или защите нарушенных прав или законных интересов заявителя органом, предоставляющим государственную услугу, органом, предоставляющим муниципальную услугу, многофункциональным центром, должностным лицом органа, предоставляющего государственную услугу, органа, предоставляющего муниципальную услугу, работником многофункционального центра, государственным или муниципальным

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

³ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁴ Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации». Статья 4 — извлечение.

служащим либо организациями, предусмотренными частью 1.1 статьи 16 настоящего Федерального закона, или их работниками при получении данным заявителем государственной или муниципальной услуги¹.

Живучесть автоматизированной системы — свойство АС, характеризующее способность выполнять установленный объем функций в условиях воздействий внешней среды и отказов компонентов системы в заданных пределах².

Жизненно важные интересы — совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства³.

Жизненный цикл (Life cycle) — развитие системы, продукции, услуги, проекта или другой создаваемой человеком сущности от замысла до списания⁴.

Жизненный цикл автоматизированной системы — совокупность взаимосвязанных процессов создания и последовательного изменения состояния АС от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации АС⁵.

Жизненный цикл изделия — совокупность разработки, изготовления, обращения, эксплуатации и утилизации изделия от начала исследования возможности его создания до окончания применения. Отличительной особенностью эксплуатации является использование или ожидание использования изделия по назначению⁶.

Жизненный цикл информационной системы — совокупность взаимосвязанных процессов последовательного изменения состояния инфор-

¹ Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности». Статья 1 — извлечение.

⁴ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

мационной системы от принятия решения о ее создании, формирования исходных требований к ней и до окончания ее эксплуатации (вывода из эксплуатации), включая хранение содержащейся в ее базах данных информации¹.

Жилище — индивидуальный жилой дом с входящими в него жилыми и нежилыми помещениями, жилое помещение независимо от формы собственности, входящее в жилищный фонд и используемое для постоянного или временного проживания, а равно иное помещение или строение, не входящее в жилищный фонд, но используемое для временного проживания².

Журналист — лицо, занимающееся редактированием, созданием, сбором или подготовкой сообщений и материалов для редакции зарегистрированного средства массовой информации, связанное с ней трудовыми или иными договорными отношениями либо занимающееся такой деятельностью по ее уполномочию³.

3

Загрузка в память — пересылка данных между различными уровнями памяти данных с целью непосредственного их использования в операциях центрального процессора⁴.

Задание на проектирование в САПР — первичное описание объекта проектирования в заданной форме⁵.

Задача (Task) — требование, рекомендация или разрешенное действие, предназначенные для содействия достижению одного или более выходов процесса⁶.

¹ Постановление Правительства РФ от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» (вместе с Положением о координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов, Правилами подготовки планов информатизации государственных органов и отчетов об их выполнении). Пункт 2 Положения — извлечение.

² Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

³ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен

Задача автоматизированной системы — функция или часть функции АС, представляющая собой формализованную совокупность автоматических действий, выполнение которых приводит к результату заданного вида¹.

Задача, требующая инновационного (высокотехнологичного) решения (Задача) — отраженное во внутренних документах Заказчика представление о текущих и перспективных потребностях Заказчика в инновационных (высокотехнологичных) решениях².

Задержание подозреваемого — мера процессуального принуждения, применяемая органом дознания, дознавателем, следователем на срок не более 48 часов с момента фактического задержания лица по подозрению в совершении преступления³.

Заинтересованная сторона, правообладатель (Stakeholder) — индивидуум или организация, имеющие право, долю, требование или интерес в системе или в обладании ее характеристиками, удовлетворяющими их потребности и ожидания. **Пример.** Конечные пользователи, организации конечного пользователя, поддерживающие стороны, разработчики, производители, обучающие стороны, сопровождающие и утилизирующие организации, приобретающие стороны, организации поставщика, органы регуляторов. **Примечание.** Некоторые заинтересованные стороны могут иметь противоположные интересы в системе⁴.

Заказчик — заказчик комплексной программы, комплексного проекта, являющийся организацией реального сектора экономики, заинтересованной в использовании научных, научно-технических результатов комплексной программы, комплексного проекта и уча-

в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/Д01и «О направлении методических материалов» (вместе с Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁴ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

ствующей в выполнении и реализации их мероприятий с целью производства продукции и оказания услуг¹.

Заказчик — государственный или муниципальный заказчик либо в соответствии с частями 1 и 2.1 статьи 15 настоящего Федерального закона бюджетное учреждение, государственное, муниципальное унитарные предприятия, осуществляющие закупки².

Заказчик (Customer) — организация или лицо, получающие продукт или услугу. Примечания. 1 Заказчик может быть внутренним или внешним по отношению к организации. 2. Другие термины, используемые для термина «заказчик»: приобретающая сторона, розничный покупатель, оптовый покупатель³.

Заказчик — организация, закупочная деятельность которой осуществляется в соответствии с законодательством о закупках⁴.

Закладочное средство (устройство) — техническое средство (устройство) приема, передачи и обработки информации, преднамеренно устанавливаемое на объекте информатизации или в контролируемой зоне в целях перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы автоматизированной информационной системы. Примечание. Местами установки закладочных средств (устройств) на охраняемой территории могут быть любые элементы контролируемой зоны, например: ограждение, конструкции, оборудование, предметы интерьера, транспортные средства⁵.

¹ Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

² Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/ДО1и «О направлении методических материалов» (вместе с Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

⁵ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

Заключение суда — вывод о наличии или об отсутствии в действиях лица, в отношении которого применяется особый порядок производства по уголовному делу, признаков преступления¹.

Законные представители — родители, усыновители, опекуны или попечители несовершеннолетнего подозреваемого, обвиняемого либо потерпевшего, представители учреждений или организаций, на попечении которых находится несовершеннолетний подозреваемый, обвиняемый либо потерпевший, органы опеки и попечительства².

Закупка товара, работы, услуги для обеспечения государственных или муниципальных нужд (далее — закупка) — совокупность действий, осуществляемых в установленном настоящим Федеральным законом порядке заказчиком и направленных на обеспечение государственных или муниципальных нужд. Закупка начинается с определения поставщика (подрядчика, исполнителя) и завершается исполнением обязательств сторонами контракта. В случае, если в соответствии с настоящим Федеральным законом не предусмотрено размещение извещения об осуществлении закупки или направление приглашения принять участие в определении поставщика (подрядчика, исполнителя), закупка начинается с заключения контракта и завершается исполнением обязательств сторонами контракта³.

Закупки офисного программного обеспечения, программного обеспечения в сфере информационной безопасности, программного обеспечения для ведения бюджетного учета (далее при совместном упоминании — программное обеспечение) — осуществление следующих видов закупок: поставка на материальном носителе и (или) в электронном виде по каналам связи программного обеспечения, а также предоставление права пользования программным обеспечением посредством использования каналов связи и внешней информационно-технологической и программно-аппаратной инфраструктуры, обеспечивающей сбор, обработку и хранение данных (услуги облачных вычислений);

выполнение работ, оказание услуг, связанных с разработкой, модификацией, модернизацией программного обеспечения, в том числе в составе существующих автоматизированных систем;

выполнение работ, оказание услуг по установке и настройке программного обеспечения;

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Там же.

³ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

оказание услуг, связанных с сопровождением, технической поддержкой, обновлением программного обеспечения, в том числе в составе существующих автоматизированных систем¹.

Замысел защиты информации — основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации².

Запоминающее устройство — устройство, реализующее функцию памяти данных³.

Запрос — обращение пользователя информацией в устной или письменной форме, в том числе в виде электронного документа, в государственный орган или орган местного самоуправления либо к его должностному лицу о предоставлении информации о деятельности этого органа⁴.

Защита информации — комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т. п.⁵

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию⁶.

¹ Постановление Правительства РФ от 8 июня 2018 г. № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности». Пункт 3, подпункт «а» — извлечение.

² ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

³ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁴ Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Статья 1 — извлечение.

⁵ Положение о государственном лицензировании деятельности в области защиты информации (утверждено решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

⁶ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

Защита информации от иностранной разведки — защита информации, направленная на предотвращение получения защищаемой информации иностранной разведкой¹.

Защита информации от непреднамеренного воздействия — защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации².

Защита информации от несанкционированного воздействия — защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации³.

Защита информации от несанкционированного доступа — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации. **Примечание.** Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо⁴.

Защита информации от преднамеренного воздействия — защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях⁵.

Защита информации от разглашения — защита информации, направленная на предотвращение несанкционированного доведения за-

¹ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

² Там же.

³ Там же.

⁴ Там же.

⁵ Там же.

щищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации¹.

Защита информации от утечки — защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами. **Примечание.** Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо².

Защита от вредоносного кода на уровне гипервизора — способ реализации защиты от вредоносного кода виртуальных машин с использованием программных средств защиты от вредоносного кода, функционирующих как отдельные виртуальные машины на уровне гипервизора, без непосредственной установки агентов на защищаемые виртуальные машины³.

Защита от несанкционированного доступа (Protection from unauthorized access) — предотвращение или существенное затруднение несанкционированного доступа⁴.

Защитные контрмеры — методы, разработанные для обеспечения безопасного использования кода, такие как предотвращение использования данных, перемешивание адресов адресного пространства (технология ASLR) или «игра в песочнице» (механизм обеспечения безопасности подкачаных из сети или полученных по электронной почте программ, предусматривающий изоляцию на время выполнения загружаемого кода в ограниченную среду — «песочницу»)⁵.

¹ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

² Там же.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁴ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁵ В соответствии с Указом Президента РФ от 21 июля 2014 г. № 519 «О внесении изменений в Список товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль, утвержденный Указом Президента Российской Федерации от 17 декабря 2011 г. № 1661». Извлечение (пункт 87.1).

Защищаемая информационная система — информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности¹.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. **Примечание.** Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо².

Защищаемый объект информатизации — объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности³.

Защищенное средство вычислительной техники (защищенная автоматизированная система) (Trusted computer system) — средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты⁴.

Защищенность (Security) — защита против намеренной подрывной деятельности или вызванного отказа. Соединение четырех атрибутов — конфиденциальности, целостности, доступности и подотчетности и аспектов пятого атрибута — практичности, у всех из которых имеется соответствующий источник их обеспечения⁵.

Заявитель — физическое или юридическое лицо, которое для подтверждения соответствия принимает декларацию о соответствии или обращается за получением сертификата соответствия, получает сертификат соответствия⁶.

Заявитель — физическое или юридическое лицо (за исключением государственных органов и их территориальных органов, органов государственных внебюджетных фондов и их территориальных органов, органов местного самоуправления) либо их уполномоченные представители, обратившиеся в орган, предоставляющий государственные услуги, или в орган, предоставляющий муниципальные услуги,

¹ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

² Там же.

³ Там же.

⁴ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁵ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁶ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

либо в организации, указанные в частях 2 и 3 статьи 1 настоящего Федерального закона, или в организации, указанные в пункте 5 настоящей статьи, с запросом о предоставлении государственной или муниципальной услуги, в том числе в порядке, установленном статьей 15.1 настоящего Федерального закона, выраженным в устной, письменной или электронной форме¹.

Заявитель — коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности РФ или государственные должности субъектов РФ, должностные лица государственных органов, органов МСУ, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица (далее — нотариусы), обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата².

Заявка — пакет документов, формируемый в соответствии с Положением, направленный в соответствии с формой, установленной Положением³.

Заявление — просьба гражданина о содействии в реализации его конституционных прав и свобод или конституционных прав и свобод других лиц, либо сообщение о нарушении законов и иных нормативных правовых актов, недостатках в работе государственных органов, органов местного самоуправления и должностных лиц, либо критика деятельности указанных органов и должностных лиц⁴.

¹ Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

² Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2, пункт 16 — извлечение.

³ Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/Д01и «О направлении методических материалов» (вместе с Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

⁴ Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации». Статья 4 — извлечение.

- Знак обращения на рынке** — обозначение, служащее для информирования приобретателей, в том числе потребителей, о соответствии выпускаемой в обращение продукции требованиям технических регламентов¹.
- Знак соответствия** — обозначение, служащее для информирования приобретателей, в том числе потребителей, о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту².
- Значимая платежная система** — платежная система, отвечающая критериям, установленным настоящим Федеральным законом (системно значимая платежная система, социально значимая платежная система, национально значимая платежная система)³.
- Значимый объект критической информационной инфраструктуры** — объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры⁴.
- Зона чрезвычайной ситуации** — территория, на которой сложилась чрезвычайная ситуация⁵.
- Зона экстренного оповещения населения** — территория, подверженная риску возникновения быстроразвивающихся опасных природных явлений и техногенных процессов, представляющих непосредственную угрозу жизни и здоровью находящихся на ней людей⁶.

И

- Идентификатор** — уникальное обозначение сведений о лице, необходимое для определения такого лица путем применения технических и (или) технологических способов⁷.
- Идентификатор доступа (Access identifier)** — уникальный признак субъекта или объекта доступа⁸.

¹ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

² Там же.

³ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁴ Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Статья 2 — извлечение.

⁵ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

⁶ Там же.

⁷ Пункт 18.1 статьи 2 Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» в ред. проекта № 260319.

⁸ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

Идентификация (Identification) — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов¹.

Идентификация — присвоение для осуществления логического доступа субъекту (объекту) доступа уникального признака (идентификатора); сравнение при осуществлении логического доступа предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов².

Идентификация, аутентификация лица — совокупность мероприятий по установлению идентификаторов и (или) сведений о лице, сопоставлению данных сведений с идентификатором или проверке данных сведений, а также по проверке лица на принадлежность лицу идентификатора (идентификаторов) посредством сопоставления идентификатора (идентификаторов) с имеющимися сведениями о лице, и установления обоснованности использования лицом идентификатора (идентификаторов), осуществляемых в соответствии с настоящим Федеральным законом, иными федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением сторон, в результате которых лицо считается установленным³.

Идентификация продукции — установление тождественности характеристик продукции ее существенным признакам; контроль (надзор) за соблюдением требований технических регламентов — проверка выполнения юридическим лицом или индивидуальным предпринимателем требований технических регламентов к продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации и принятие мер по результатам проверки⁴.

¹ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

² ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

³ Пункт 18.2 статьи 2 Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» в ред. проекта № 260319.

⁴ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

Избрание меры пресечения — принятие дознавателем, следователем, а также судом решения о мере пресечения в отношении подозреваемого, обвиняемого¹.

Издатель — издательство, иное учреждение, предприятие (предприниматель), осуществляющее материально-техническое обеспечение производства продукции средства массовой информации, а также приравненное к издателю юридическое лицо или гражданин, для которого эта деятельность не является основной либо не служит главным источником дохода².

Импортозамещение (см. Мероприятия по импортозамещению).

Индустриальный интернет — концепция построения информационных и коммуникационных инфраструктур на основе подключения к информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет») промышленных устройств, оборудования, датчиков, сенсоров, систем управления технологическими процессами, а также интеграции данных программно-аппаратных средств между собой без участия человека³.

Индустриальный (промышленный) парк — совокупность объектов промышленной инфраструктуры, предназначенных для создания промышленного производства или модернизации промышленного производства и управляемых управляющей компанией — коммерческой или некоммерческой организацией, созданной в соответствии с законодательством Российской Федерации⁴.

Инжиниринговый центр — юридическое лицо, оказывающее инженерно-консультационные услуги по подготовке процесса производства и реализации продукции (работ, услуг), подготовке строительства и эксплуатации промышленных, инфраструктурных и других объектов, предпроектные и проектные услуги⁵.

Инициативное предложение — предложение об установлении экспериментального правового режима, включающее в том числе описание предлагаемого специального регулирования, описание мер, направленных на снижение рисков причинения вреда жизни и

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

³ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁴ Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

⁵ Там же.

здоровью человека, обороне страны и безопасности государства, иным охраняемым федеральным законом ценностям¹.

Инициатор — лицо, вносящее инициативное предложение в порядке, установленном настоящим Федеральным законом².

Инициатор комплексной программы — заинтересованные органы государственной власти, члены советов по приоритетным направлениям научно-технологического развития Российской Федерации, организации реального сектора экономики, общественные объединения, институты развития, иные организации³.

Инициатор комплексного проекта — заинтересованные органы государственной власти, члены советов по приоритетным направлениям научно-технологического развития Российской Федерации, организации реального сектора экономики, общественные объединения, институты развития, иные организации⁴.

Инновационная продукция — продукция, применение которой Заказчиком обеспечивает существенное повышение эффективности решения производственных и иных задач Заказчика за счет: новых или существенно измененных свойств продукции; применения при производстве продукции новых или измененных материалов, оборудования, технологий, производственных и организационных процессов, существенно снижающих стоимость такой продукции⁵.

Инновационное решение (решение) — совокупность товаров, работ и услуг, совместное применение которых обеспечивает существенное повышение эффективности решения производственных и иных задач Заказчика за счет: использования в решении инновационной продукции; использования в решении новых способов применения продукции⁶.

¹ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

² Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922896-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

³ Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

⁴ Там же.

⁵ Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/Д01и «О направлении методических материалов» (вместе с Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

⁶ Там же.

Инновационный цикл — комплекс работ, включающий основные этапы и результаты инновационного процесса, а также выполнение прикладных научных исследований и опытно-конструкторских работ с целью коммерциализации научного знания в новых продуктах, производство продукции¹.

Иностранная платежная система — совокупность организаций, присоединившихся к правилам платежной системы, организованной в соответствии с иностранным законодательством, и взаимодействующих по правилам платежной системы (участники иностранной платежной системы), в соответствии с которыми иностранный банк (иностранная кредитная организация) может выступать в качестве плательщика и получателя средств по переводам денежных средств участников иностранной платежной системы (иностранный центральный платежный клиринговый контрагент)².

Иностранная продукция — продукция, не являющаяся отечественной³.

Интеграционные подсистемы — информационные системы, реализующие функции управления базами данных системы координации и формирования единого хранилища данных, обеспечения защиты информации, информационно-технологического взаимодействия подсистем системы координации между собой и с иными информационными системами, а также функции общесистемных технологических сервисов⁴.

Интегрированная автоматизированная система — совокупность двух или более взаимоувязанных АС, в которой функционирование одной из них зависит от результатов функционирования другой

¹ Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

² Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

³ Пункт 8 Методических рекомендаций по подготовке корпоративных планов импортозамещения государственными корпорациями, государственными компаниями, акционерными обществами, в уставном капитале которых доля участия Российской Федерации превышает 50 процентов, организациями, реализующими инвестиционные проекты, включенные в реестр инвестиционных проектов в соответствии с решением Правительственной комиссии по импортозамещению, утвержденных распоряжением Минэкономразвития России от 11 августа 2016 г. № 219Р-АУ.

⁴ Постановление Правительства РФ от 14 ноября 2015 г. № 1235 «О федеральной государственной информационной системе координации информатизации» (вместе с Положением о федеральной государственной информационной системе координации информатизации). Пункт 14 части III Положения — извлечение.

(других) так, что эту совокупность можно рассматривать как единую АС¹.

Интегрированная структура оборонно-промышленного комплекса — объединение ведущих совместную деятельность юридических лиц, которое не является юридическим лицом, создается в соответствии с решениями Президента Российской Федерации или Правительства Российской Федерации и в котором одно юридическое лицо имеет возможность определять решения, принимаемые остальными юридическими лицами².

Интерактивный режим — режим взаимодействия процесса обработки информации системы обработки информации с человеком, выражающийся в разном рода воздействиях на этот процесс, предусмотренных механизмом управления конкретной системы и вызывающих ответную реакцию процесса³.

Интерес (системы) (Concern) — польза или проблемы в системе, относящиеся к одной или нескольким заинтересованным сторонам.
Примечание. Интерес относится к любому воздействию на систему в ее окружающей среде, включая воздействия разработки, технологические, деловые, эксплуатационные, организационные, политические, экономические, юридические, регулирующие, экологические и социальные воздействия⁴.

Интернет вещей — концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека⁵.

Интерфейс — совокупность средств и правил, обеспечивающих взаимодействие устройств вычислительной машины или системы обработки информации и (или) программ⁶.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

³ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁴ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁵ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁶ ГОСТ 15971-90 «Системы обработки информации. Термины и определения»

Информатизация (англ. **Informatization**) — политика и процессы, направленные на построение и развитие телекоммуникационной инфраструктуры, объединяющей территориально распределенные информационные ресурсы¹.

Информатика (фр. **Informatique**; англ. **Computer science**) — наука о методах и процессах сбора, хранения, обработки, передачи, анализа и оценки информации с применением компьютерных технологий...²

Информационная база автоматизированной системы — совокупность упорядоченной информации, используемой при функционировании АС³.

Информационная безопасность (Information security) — свойство информации сохранять конфиденциальность, целостность и доступность.

Примечание. Кроме того, данное понятие может включать в себя также и свойство сохранять аутентичность, подотчетность, неотказуемость и надежность⁴.

Информационная безопасность Российской Федерации (далее — информационная безопасность) — состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства⁵.

Информационная инфраструктура Российской Федерации (далее — информационная инфраструктура) — совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Феде-

(утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

¹ Википедия — ru.wikipedia.org.

² Информатика — Википедия, ru.wikipedia.org. Информатика. Понятие «информатика» возникло в 60-х годах во Франции. Так решили назвать область знаний, изучающую применение ЭВМ для автоматизации обработки данных. Слово «информатика» образовано из двух слов: «информация» и «автоматика».

³ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁴ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

⁵ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

рации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации¹.

Информационная модель — модель объекта, представленная в виде информации, описывающей существенные для данного рассмотрения параметры и переменные величины объекта, связи между ними, входы и выходы объекта и позволяющая путем подачи на модель информации об изменениях входных величин моделировать возможные состояния объекта².

Информационная модель объекта капитального строительства — совокупность взаимосвязанных сведений, документов и материалов об объекте капитального строительства, формируемых в электронном виде на этапах выполнения инженерных изысканий, осуществления архитектурно-строительного проектирования, строительства, реконструкции, капитального ремонта, эксплуатации и (или) сноса объекта капитального строительства³.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств^{4,5}.

Информационная система общего пользования — информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано⁶.

Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств⁷.

¹ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Приложение 1 — извлечение.

³ Пункт 10.3 статьи 1 Градостроительного кодекса Российской Федерации от 29 декабря 2004 г. № 190-ФЗ (ред. от 02.08.2019).

⁴ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁵ ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение.

⁶ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

⁷ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

Информационная совместимость автоматизированных систем — частная совместимость АС, характеризующаяся возможностью использования в них одних и тех же данных и обмена данными между ними¹.

Информационная технология (технология обработки (передачи) информации в информационной системе) — процесс, метод поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов².

Информационная технология — приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных³.

Информационная угроза (угроза информационной безопасности Российской Федерации) — совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере⁴.

Информационная функция автоматизированной системы управления технологическим процессом — функция АСУ технологическим процессом, включающая получение информации, обработку и передачу информации персоналу АСУТП или вовне системы о состоянии технологического объекта управления или внешней среды⁵.

Информационно-коммуникационные технологии — совокупность информационных технологий, информационных систем и информационно-телекоммуникационных сетей, необходимых для реализации полномочий государственного органа и обеспечения его деятельности⁶.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение.

³ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Приложение 1 — извлечение.

⁴ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ Постановление Правительства РФ от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» (вместе с Положением о координации

Информационное изделие в автоматизированной системе — информационное средство, изготовленное, прошедшее испытания установленного вида и поставляемое как продукция производственно-технического назначения для применения в АС¹.

Информационное обеспечение автоматизированной системы — совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании².

Информационное общество — общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан³.

Информационное пространство — совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры⁴.

Информационное средство — комплекс упорядоченной относительно постоянной информации на носителе данных, описывающей параметры и характеристики заданной области применения, и соответствующей документации, предназначенный для поставки пользователю. Примечание. Документация информационного средства может поставляться на носителе данных⁵.

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники⁶.

мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов, Правилами подготовки планов информатизации государственных органов и отчетов об их выполнении). Пункт 2 Положения — извлечение.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Там же.

³ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁴ Там же.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов¹.

Информационный обмен между виртуальными машинами — межпроцессорное взаимодействие, а также сетевые информационные потоки между виртуальными машинами, в том числе реализуемые средствами гипервизора и виртуальными вычислительными сетями².

Информационный объект — элемент программы, содержащий фрагменты информации, циркулирующей в программе. В зависимости от языка программирования в качестве информационных объектов могут выступать переменные, массивы, записи, таблицы, файлы, фрагменты оперативной памяти и т. п.³

Информационный ресурс — совокупность систематизированной информации с определенной структурой информационного ресурса, порядком его формирования, ведения, изменения, а также применения содержащейся в нем информации⁴.

Информация — сведения (сообщения, данные) независимо от формы их представления⁵.

Информация конфиденциального характера — информация, для которой в соответствии с законодательством Российской Федерации, в том числе нормативными актами Банка России, и (или) внутренними документами финансовой организации обеспечивается сохранение свойства конфиденциальности⁶.

¹ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

² ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

³ Руководящий документ. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114). Пункт 2 — извлечение.

⁴ Проект в редакции от 4 июля 2018 г. Федерального закона «О систематизации и гармонизации информации в Российской Федерации». Статья 2 — извлечение.

⁵ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁶ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

Информация о деятельности государственных органов и органов местного самоуправления — информация (в том числе документированная), созданная в пределах своих полномочий государственными органами, их территориальными органами, органами местного самоуправления или организациями, подведомственными государственным органам, органам местного самоуправления (далее — подведомственные организации), либо поступившая в указанные органы и организации. К информации о деятельности государственных органов и органов местного самоуправления относятся также законы и иные нормативные правовые акты, а к информации о деятельности органов местного самоуправления — муниципальные правовые акты, устанавливающие структуру, полномочия, порядок формирования и деятельности указанных органов и организаций, иная информация, касающаяся их деятельности¹.

Информация, составляющая коммерческую тайну (секрет производства) — сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны².

Информирование населения о чрезвычайных ситуациях — доведение до населения через средства массовой информации и по иным каналам информации о прогнозируемых и возникших чрезвычайных ситуациях, принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты, а также проведение пропаганды знаний в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, в том числе обеспечения безопасности людей на водных объектах, и обеспечения пожарной безопасности³.

Инфраструктура взаимодействия — защищенные каналы связи, обеспечивающие безопасное подключение информационных систем

¹ Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Статья 1 — извлечение.

² Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Статья 3 — извлечение.

³ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

органов власти к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, являющиеся неотъемлемой частью инфраструктуры электронного правительства¹.

Инфраструктура поддержки деятельности в сфере промышленности — коммерческие организации и некоммерческие организации, осуществляющие меры стимулирования деятельности в сфере промышленности².

Инфраструктура цифрового профиля — совокупность информационных систем в единой системе идентификации и аутентификации, обеспечивающих доступ к цифровому профилю³.

Инфраструктура экономики Российской Федерации — отрасли экономики Российской Федерации, функционирующие в интересах обеспечения обороноспособности и безопасности государства⁴.

Инфраструктура электронного правительства — совокупность размещенных на территории Российской Федерации государственных информационных систем, программно-аппаратных средств и сетей связи, обеспечивающих при оказании услуг и осуществлении функций в электронной форме взаимодействие органов государственной власти Российской Федерации, органов местного самоуправления, граждан и юридических лиц; неотъемлемой частью инфраструктуры электронного правительства являются защищенные каналы связи, обеспечивающие безопасное подключение информационных систем органов власти к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме (см. также — **инфраструктура взаимодействия**).

Инцидент (Incident) — отклонение или неожиданное событие, множество событий, условия или ситуация в любое время во время жизненного цикла проекта, продукции, услуги или системы⁵.

¹ Письмо Минкомсвязи от 24 декабря 2018 г. № МП-П13-070-30187. Извлечение.

² Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

³ Пункт 1 статьи 14.2 Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» в ред. проекта № 260319.

⁴ Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне». Примечания, пункт 3 — извлечение.

⁵ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен

Инцидент информационной безопасности (Information security incident) — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. **Примечание.** Инцидентами информационной безопасности являются: утрата услуг, оборудования или устройств; системные сбои или перегрузки; ошибки пользователей; несоблюдение политики или рекомендаций по ИБ; нарушение физических мер защиты; неконтролируемые изменения систем; сбои программного обеспечения и отказы технических средств; нарушение правил доступа¹.

Искусственный интеллект — способность вычислительной машины моделировать процесс мышления за счет выполнения функций, которые обычно связывают с человеческим интеллектом. **Примечание.** Такими функциями являются, например, обучение и логический вывод².

Использование по назначению — см. «Использование»³.

Использование радиочастотного спектра — обладание разрешением на пользование и (или) фактическое пользование полосой радиочастот, радиочастотным каналом или радиочастотой для оказания услуг электросвязи и других, не запрещенных федеральными законами или иными нормативными правовыми актами Российской Федерации целей⁴.

Источник угрозы безопасности информации — субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации⁵.

в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

¹ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

² ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

³ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁴ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁵ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

Итоговое судебное решение — приговор, иное решение суда, вынесенное в ходе судебного разбирательства, которым уголовное дело разрешается по существу¹.

К

Канал ввода-вывода — устройство, обеспечивающее пересылку данных между основной памятью ЭВМ и периферийными устройствами².

Кассационная инстанция — суд, рассматривающий в кассационном порядке уголовные дела по жалобам и представлениям на вступившие в законную силу приговоры, определения и постановления судов³.

Качество эксплуатации продукции — По ГОСТ 15467-79⁴.

Квалификация (Qualification) — процесс демонстрации, определяющий, способен ли какой-либо объект полностью удовлетворять заданным требованиям⁵.

Квалификация работника — уровень знаний, умений, профессиональных навыков и опыта работы работника⁶.

Квалифицированный сертификат ключа проверки электронной подписи (далее — квалифицированный сертификат) — сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее — уполномоченный федеральный орган)⁷.

Класс защищенности средств вычислительной техники (автоматизированной системы) (Protection class of computer systems) — определен-

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁴ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁵ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁶ Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ. Статья 195.1, часть первая — извлечение.

⁷ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

ная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации¹.

Классификация (Classification) — систематическая идентификация и/или упорядочение деловой деятельности и/или документов по категориям в соответствии с логически структурированными условиями, методами и процедурными правилами².

Ключ электронной подписи — уникальная последовательность символов, предназначенная для создания электронной подписи³.

Ключ проверки электронной подписи — уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее — проверка электронной подписи)⁴.

Код «AuthInfo-код» — код, выдаваемый администратору регистратором-донором для передачи поддержки сведений о доменном имени⁵.

Коммерческая тайна — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду⁶.

Комплекс программ «Почтовая служба» — специальное программное обеспечение, используемое в системе межведомственного электронного документооборота и предназначенное для организации почтового обмена электронными сообщениями по защищенным каналам связи⁷.

¹ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

² ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

³ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

⁴ Там же.

⁵ Правила регистрации доменных имен в доменах .RU и .RF (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

⁶ Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Статья 3 — извлечение.

⁷ Распоряжение Правительства РФ от 2 октября 2009 г. № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти». Извлечение.

Комплекс средств автоматизации автоматизированной системы — совокупность всех компонентов АС, за исключением людей¹.

Комплекс средств защиты (Trusted computing base) — совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации².

Комплексная программа — комплексная научно-техническая программа полного инновационного цикла, представляющая собой совокупность скоординированных по задачам, срокам и ресурсам мероприятий, включающих в себя научные исследования и этапы инновационного цикла до создания технологий, продукции и оказания услуг³.

Комплексная система экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций — элемент системы оповещения населения о чрезвычайных ситуациях, представляющий собой комплекс программно-технических средств систем оповещения и мониторинга опасных природных явлений и техногенных процессов, обеспечивающий доведение сигналов оповещения и экстренной информации до органов управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций и до населения в автоматическом и (или) автоматизированном режимах⁴.

Комплексный план научных исследований — план взаимоувязанных научных исследований и разработок научных и образовательных организаций, организаций реального сектора экономики для создания новых или выявления имеющихся перспективных (прорывных) и востребованных в экономике результатов, формируемый в порядке, установленном Министерством науки и высшего обра-

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

³ Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

⁴ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

зования Российской Федерации, в целях реализации комплексных программ¹.

Комплексный проект — комплексный научно-технический проект полного инновационного цикла, представляющий собой комплекс работ, скоординированных по задачам, срокам и ресурсам, включающий в себя научные исследования и этапы инновационного цикла до создания технологий, продукции и оказания услуг².

Комплексный проект — комплекс взаимосвязанных мероприятий и процессов по разработке цифровых платформ и (или) программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции, ограниченный по времени и ресурсам, включающий: выполнение научно-исследовательских, опытно-конструкторских и (или) технологических работ; организацию апробации результатов комплексного проекта в отраслях экономики; последующую коммерциализацию результатов комплексного проекта в организациях, выпускающих высокотехнологичную промышленную продукцию либо осуществляющих деятельность в области прикладных научных исследований и разработок, направленных на создание высокотехнологичной промышленной продукции; создание высокопроизводительных рабочих мест в организациях, выпускающих высокотехнологичную промышленную продукцию и внедривших разработанные в рамках реализации комплексного проекта цифровые платформы и (или) программные продукты в целях создания и (или) развития производства высокотехнологичной промышленной продукции³.

¹ Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

² Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

³ Пункт 2 Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции, утвержденных постановлением Правительства РФ от 30 апреля 2019 г. № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции». Извлечение.

Комплектуемое изделие в автоматизированной системе — изделие или единица научно-технической продукции, применяемое как составная часть АС в соответствии с техническими условиями или техническим заданием на него¹.

Компонент (Component) — поддающаяся идентификации отдельная часть (элемент) автоматизированной системы, которая реализует часть функциональных возможностей системы².

Компонент автоматизированной системы — часть АС, выделенная по определенному признаку или совокупности признаков и рассматриваемая как единое целое³.

Компонент информационной системы — часть информационной системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств⁴.

Компоненты информационно-телекоммуникационной инфраструктуры — совместно используемые информационными системами программно-технические комплексы и средства, выполняющие общие технологические функции и обеспечивающие основу функционирования указанных информационных систем, в том числе обеспечивающие их информационно-технологическое взаимодействие⁵.

Компрометация аутентификационных данных — событие, связанное с возникновением возможности использования аутентификаци-

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие Приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

³ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁴ ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение.

⁵ Постановление Правительства РФ от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» (вместе с Положением о координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов, Правилами подготовки планов информатизации государственных органов и отчетов об их выполнении). Пункт 2 Положения — извлечение.

онных данных субъектом, не являющимся легальным владельцем указанных аутентификационных данных¹.

Компромисс (Trade-off) — действия по принятию решений, в ходе которых на основе конечной выгоды правообладателей производится выбор из различных требований и альтернативных решений².

Компьютеризация — автоматизация каких-либо процессов в любой области деятельности человека за счет применения вычислительных машин³.

Компьютерная атака — целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации⁴.

Компьютерная атака — целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств⁵.

Компьютерная информация — сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи⁶.

¹ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

² ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

³ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁴ Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Статья 2 — извлечение.

⁵ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

⁶ Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ. Примечание к статье 272 — извлечение.

Компьютерный вирус — вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы¹.

Компьютерный инцидент — факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки².

Конверсия радиочастотного спектра — экономические, организационные и технические мероприятия, направленные на расширение использования радиочастотного спектра радиоэлектронными средствами гражданского назначения³.

Конвертирование (Conversion) — процесс перевода документов из одного формата в другой⁴.

Конец эксплуатации — момент снятия с эксплуатации⁵.

Контентные услуги — вид услуг связи, которые технологически неразрывно связаны с услугами подвижной радиотелефонной связи и направлены на повышение их потребительской ценности (в том числе услуги по предоставлению абонентам возможности получать на пользовательское (оконечное) оборудование в сетях связи справочную, развлекательную и (или) иную дополнительно оплачиваемую информацию, участвовать в голосовании, играх, конкурсах и аналогичных мероприятиях) и стоимость оказания которых оплачивается абонентом оператору связи, с которым у абонента заключен договор об оказании услуг связи⁶.

¹ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

² Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Статья 2 — извлечение.

³ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁴ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

⁵ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁶ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

Контрагент — сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию¹.

Контракт — государственный или муниципальный контракт либо гражданско-правовой договор, предметом которого являются поставка товара, выполнение работы, оказание услуги (в том числе приобретение недвижимого имущества или аренда имущества) и который заключен бюджетным учреждением, государственным или муниципальным унитарным предприятием либо иным юридическим лицом в соответствии с частями 1, 2.1, 4 и 5 статьи 15 настоящего Федерального закона².

Контракт жизненного цикла — контракт, предусматривающий поставку товара или выполнение работы (в том числе при необходимости проектирование объекта капитального строительства, конструирование товара, который должен быть создан в результате выполнения работы), последующие обслуживание, при необходимости эксплуатацию в течение срока службы, ремонт и (или) утилизацию поставленного товара или созданного в результате выполнения работы объекта капитального строительства или товара³.

Контрактная система в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд (контрактная система в сфере закупок) — совокупность участников контрактной системы в сфере закупок (федеральный орган исполнительной власти по регулированию контрактной системы в сфере закупок, органы исполнительной власти субъектов Российской Федерации по регулированию контрактной системы в сфере закупок, иные федеральные органы исполнительной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, уполномоченные на осуществление нормативно-правового регулирования и контроля в сфере закупок, Государственная корпорация по атомной энергии «Росатом», Государственная корпорация по космической деятельности «Роскосмос», заказчики, участники закупок, в том числе признанные поставщиками (подрядчиками, исполнителями), уполномоченные органы, уполномоченные учреждения, специализированные организации,

¹ Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Статья 3 — извлечение.

² Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Пункт 8.1 статьи 3 — извлечение.

³ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Пункт 8.2 статьи 3 — извлечение.

операторы электронных площадок) и осуществляемых ими, в том числе с использованием единой информационной системы в сфере закупок (за исключением случаев, если использование такой единой информационной системы не предусмотрено настоящим Федеральным законом), в соответствии с законодательством Российской Федерации и иными нормативными правовыми актами о контрактной системе в сфере закупок действий, направленных на обеспечение государственных и муниципальных нужд¹.

Контроль телефонных и иных переговоров — прослушивание и запись переговоров путем использования любых средств коммуникации, осмотр и прослушивание фонограмм².

Контрольный орган в сфере закупок — федеральный орган исполнительной власти, орган исполнительной власти субъекта Российской Федерации, орган местного самоуправления муниципального района, орган местного самоуправления городского округа, уполномоченные на осуществление контроля в сфере закупок, а также федеральный орган исполнительной власти, уполномоченный на осуществление функций по контролю (надзору) в сфере государственного оборонного заказа и в сфере закупок товаров, работ, услуг для обеспечения федеральных нужд, которые не относятся к государственному оборонному заказу и сведения о которых составляют государственную тайну (далее — контрольный орган в сфере государственного оборонного заказа)³.

Контур безопасности — совокупность объектов информатизации, определяемая областью применения настоящего стандарта, используемых для реализации бизнес-процессов и (или) технологических процессов финансовой организации единой степени критичности (важности), для которой финансовой организацией применяется единая политика (режим) защиты информации (единый набор требований к обеспечению защиты информации)⁴.

¹ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

² Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

³ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

⁴ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

Конфигурация информационной системы — взаимосвязанные структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между компонентами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, а также с полномочиями субъектов доступа к объектам доступа информационной системы¹.

Конфигурация системы обработки информации — совокупность функциональных частей системы обработки информации и связей между ними, обусловленная основными техническими характеристиками этих функциональных частей, а также требованиями решаемых задач².

Конфиденциальная информация (Sensitive information) — информация, требующая защиты³.

Конфиденциальность (Confidentiality) — свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса⁴.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя⁵.

Концепция диспетчера доступа (Reference monitor concept) — концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам⁶.

¹ ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение.

² ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

³ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁴ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

⁵ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁶ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

Концепция функционирования, эксплуатации (Concept of operations) — описательные и/или графические положения в границах предположений или намерений организации в отношении функционирования, эксплуатации. **Примечания.** 1. Концепция функционирования, эксплуатации часто воплощается в стратегических и ежегодных эксплуатационных планах. В последнем случае концепция функционирования, эксплуатации охватывает в плане ряд связанных операций, которые будут выполнены одновременно или по очереди. Понятие разработано для того, чтобы дать полную картину функционирования, эксплуатации организации (см. также «операционная концепция»). 2. Это обеспечивает основу для ограничения операционного пространства, возможностей системы, взаимодействий и эксплуатационной среды¹.

Координатор — уполномоченное юридическое лицо, осуществляющее управление доменами .RU и .РФ в интересах российского и мирового интернет-сообщества и организующее функционирование Реестра².

Координационный орган — орган, определяемый Правительством Российской Федерации для разрешения разногласий между государственными органами и организациями по результатам рассмотрения инициативных предложений и иных вопросов, относящихся к предмету настоящего Федерального закона³.

Корпоративная информационная система — информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц⁴.

Кредитная организация — юридическое лицо, которое для извлечения прибыли как основной цели своей деятельности на основании специального разрешения (лицензии) Центрального банка Российской Федерации (Банка России) имеет право осуществлять банковские операции, предусмотренные настоящим Федеральным законом⁵.

¹ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

² Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

³ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

⁴ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

⁵ Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности».

Кредитная организация образуется на основе любой формы собственности как хозяйственное общество¹.

Криптовалюта — вид цифрового финансового актива, создаваемый и учитываемый в распределенном реестре цифровых транзакций участниками этого реестра в соответствии с правилами ведения реестра цифровых транзакций².

Криптографическая защита информации — защита информации с помощью ее криптографического преобразования³.

Критическая информационная инфраструктура — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов⁴.

Криптографическое средство защиты информации — средство защиты информации, реализующее алгоритмы криптографического преобразования информации⁵.

Критерий эффективности деятельности — соотношение, характеризующее степень достижения цели деятельности и принимающее различные числовые значения в зависимости от используемых воздействий на объект деятельности или конкретных результатов деятельности⁶.

Критическая информационная инфраструктура Российской Федерации (далее — критическая информационная инфраструктура) — совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой⁷.

¹ Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности». Статья 1 — извлечение.

² Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

³ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁴ Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Статья 2 — извлечение.

⁵ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁶ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Приложение 1 — извлечение.

⁷ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

Критически важный объект — это объект, нарушение или прекращение функционирования которого приведет к потере управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы субъекта Российской Федерации, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения¹.

Критический маршрут выполнения функциональных объектов — такой маршрут, при выполнении которого существует возможность неконтролируемого нарушения установленных правил обработки информационных объектов².

Кросс-отраслевые процессы — межотраслевые процессы, интегрирующие деятельность субъектов из различных отраслей экономики³.

Крупный ущерб — ущерб, сумма которого превышает один миллион рублей⁴.

Л

Легальный субъект доступа — субъект доступа, наделенный финансовой организацией полномочиями на осуществление физического и (или) логического доступа⁵.

Лидерная эксплуатация — нормальная эксплуатация заданного количества изделий, выделенных для более интенсивного расходования ресурса по сравнению с остальным парком изделий⁶.

¹ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

² Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114). Пункт 2 — извлечение.

³ Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». Раздел 1. Определения — извлечение.

⁴ Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ. Примечание к статье 272 — извлечение.

⁵ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁶ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

Лидирующий исследовательский центр — структурное подразделение российской организации, отобранной в соответствии с Положением о проведении конкурсного отбора на предоставление государственной поддержки программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий, утвержденным постановлением Правительства Российской Федерации от 3 мая 2019 г. № 551 «О государственной поддержке программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий» (далее — Положение об отборе)¹.

Ликвидация чрезвычайных ситуаций — аварийно-спасательные и другие неотложные работы, проводимые при возникновении чрезвычайных ситуаций и направленные на спасение жизни и сохранение здоровья людей, снижение размеров ущерба окружающей среде и материальных потерь, а также на локализацию зон чрезвычайных ситуаций, прекращение действия характерных для них опасных факторов².

Лимит бюджетных обязательств — объем прав в денежном выражении на принятие казенным учреждением бюджетных обязательств и (или) их исполнение в текущем финансовом году (текущем финансовом году и плановом периоде)³.

Лингвистическая совместимость автоматизированных систем — частная совместимость АС, характеризующаяся возможностью использования одних и тех же языковых средств общения персонала с комплексом средств автоматизации этих АС⁴.

¹ Пункт 2 Правил предоставления субсидий из федерального бюджета на государственную поддержку программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий, утвержденных постановлением Правительства РФ от 3 мая 2019 г. № 551. Извлечение.

² Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

³ Приказ Минкомсвязи России от 30 декабря 2016 г. № 745 «Об утверждении рекомендаций по согласованию с Министерством связи и массовых коммуникаций Российской Федерации предлагаемых главными распорядителями средств федерального бюджета изменений в сводную бюджетную роспись федерального бюджета и лимиты бюджетных обязательств по бюджетным ассигнованиям, предусмотренным на закупку товаров, работ, услуг в сфере информационно-коммуникационных технологий». Пункт 2 Рекомендаций — извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные

Лингвистическое обеспечение автоматизированной системы — совокупность средств и правил для формализации естественного языка, используемых при общении пользователей и эксплуатационного персонала АС с комплексом средств автоматизации при функционировании АС¹.

Линейно-кабельные сооружения связи — объекты инженерной инфраструктуры, созданные или приспособленные для размещения кабелей связи².

Линии связи — линии передачи, физические цепи и линейно-кабельные сооружения связи³.

Лицензиат — юридическое лицо или индивидуальный предприниматель, имеющие лицензию⁴.

Лицензиат в области защиты информации — сторона, получившая право на проведение работ в области защиты информации⁵.

Лицензионные требования — совокупность требований, которые установлены положениями о лицензировании конкретных видов деятельности, основаны на соответствующих требованиях законодательства Российской Федерации и направлены на обеспечение достижения целей лицензирования⁶.

Лицензирование — деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования⁷.

системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

¹ Там же.

² Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

³ Там же.

⁴ Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». Статья 3 — извлечение.

⁵ Положение о государственном лицензировании деятельности в области защиты информации (утверждено решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

⁶ Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». Статья 3 — извлечение.

⁷ Там же.

Лицензирование в области защиты информации — деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ¹.

Лицензирование в области защиты информации — деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации².

Лицензируемый вид деятельности — вид деятельности, на осуществление которого на территории Российской Федерации и на иных территориях, над которыми Российская Федерация осуществляет юрисдикцию в соответствии с законодательством Российской Федерации и нормами международного права, требуется получение лицензии в соответствии с настоящим Федеральным законом, в соответствии с федеральными законами, указанными в части 3 статьи 1 настоящего Федерального закона и регулируемыми отношения в соответствующих сферах деятельности³.

Лицензирующие органы — уполномоченные федеральные органы исполнительной власти и (или) их территориальные органы, а в случае передачи осуществления полномочий Российской Федерации в области лицензирования органам государственной власти субъектов Российской Федерации органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование⁴.

Лицензия — специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа⁵.

¹ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

² Положение о государственном лицензировании деятельности в области защиты информации (утверждено решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

³ Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». Статья 3 — извлечение.

⁴ Там же.

⁵ Там же.

Лицензия в области защиты информации — оформленное соответствующим образом разрешение на право проведения тех или иных работ в области защиты информации¹.

Логический доступ к ресурсу доступа (логический доступ) — доступ к ресурсу доступа, в том числе удаленный, реализуемый с использованием вычислительных сетей, позволяющий, в том числе без физического доступа, осуществить доступ к защищаемой информации или выполнить операции по обработке защищаемой информации².

М

Майнинг — деятельность, направленная на создание криптовалюты и/или валидацию с целью получения вознаграждения в виде криптовалюты. Майнинг признается предпринимательской деятельностью в случае, когда лицо, которое его осуществляет, в течение трех месяцев подряд превышает лимиты энергопотребления, установленные Правительством Российской Федерации³.

Мандатное управление доступом (Mandatory access control) — разграничение доступа субъектов к объектам, основанное на характеризующей метке конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности⁴.

Массовая информация — печатные, аудио-, аудиовизуальные и иные сообщения и материалы, предназначенные для неограниченного круга лиц⁵.

Массовые беспорядки — нарушения общественного порядка на определенной территории, носящие массовый характер, представля-

¹ Положение о государственном лицензировании деятельности в области защиты информации (утверждено решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

² ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

³ Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

⁴ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁵ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

ющие угрозу жизни и здоровью людей, дезорганизирующие работу предприятий, учреждений и организаций либо направленные на разрушение или уничтожение государственного и личного имущества граждан¹.

Массовый трансфер — единовременная передача поддержки сведений о значительном количестве доменных имен по инициативе регистратора-донора².

Математическое обеспечение автоматизированной системы — совокупность математических методов, моделей и алгоритмов, примененных в АС³.

Матрица доступа (Access matrix) — таблица, отображающая правила разграничения доступа⁴.

Машинная информационная база автоматизированной системы — часть информационной базы АС, представляющая собой совокупность используемой в АС информации на носителях данных⁵.

Машинное моделирование — реализуемый на вычислительной машине метод исследования, предполагающий замену реального процесса его математической моделью⁶.

Межведомственное информационное взаимодействие — осуществляемое в целях предоставления государственных и муниципальных услуг взаимодействие по вопросам обмена документами и информацией, в том числе в электронной форме, между органами, предоставляющими государственные услуги, органами, предоставляющими муниципальные услуги, подведомственными государственным

¹ ГОСТ Р 22.0.02-94 (в ред. Изменения № 1, принятого постановлением Госстандарта РФ от 31 мая 2000 г. № 148-ст) «Безопасность в чрезвычайных ситуациях. Определения основных понятий». Принят и введен в действие постановлением Госстандарта РФ от 22 декабря 1994 г. № 327 (Группа Т 00, ОКСТУ 0022). Извлечение.

² Правила регистрации доменных имен в доменах .RU и .RF (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

³ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁴ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

органам или органам местного самоуправления организациями, участвующими в предоставлении предусмотренных частью 1 статьи 1 настоящего Федерального закона государственных или муниципальных услуг, иными государственными органами, органами местного самоуправления, органами государственных внебюджетных фондов, многофункциональными центрами¹.

Межведомственный запрос — документ на бумажном носителе или в форме электронного документа о представлении документов и информации, необходимых для предоставления государственной или муниципальной услуги, направленный органом, предоставляющим государственную услугу, органом, предоставляющим муниципальную услугу, либо многофункциональным центром в государственный орган, орган местного самоуправления, подведомственную государственному органу или органу местного самоуправления организацию, участвующую в предоставлении предусмотренных частью 1 статьи 1 настоящего Федерального закона государственных или муниципальных услуг, на основании запроса о предоставлении государственной или муниципальной услуги или запроса, указанного в статье 15.1 настоящего Федерального закона, и соответствующий требованиям, установленным статьей 7.2 настоящего Федерального закона².

Межведомственный электронный документооборот — взаимодействие информационных систем электронного документооборота ФОИВ, органов исполнительной власти субъектов РФ и иных государственных органов, а также государственных внебюджетных фондов единого института развития в жилищной сфере и государственных корпораций (далее соответственно — информационные системы электронного документооборота, участники межведомственного электронного документооборота)³.

Международно-правовая защита присвоения (назначения) радиочастот или радиочастотных каналов — правовые, технические, организационные и научно-исследовательские мероприятия, осуществляемые в целях обеспечения международного признания присвоения (назначения) радиочастот или радиочастотных каналов для радиоэлектронных средств различных радиослужб Российской Федерации⁴.

¹ Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

² Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

³ Постановление Правительства РФ от 22 сентября 2009 г. № 754 «Об утверждении Положения о системе межведомственного электронного документооборота». Пункт 1 Положения — извлечение.

⁴ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

Международный стандарт — стандарт, принятый международной организацией; национальный стандарт — стандарт, утвержденный национальным органом Российской Федерации по стандартизации; орган по сертификации — юридическое лицо или индивидуальный предприниматель, аккредитованные в соответствии с законодательством Российской Федерации об аккредитации в национальной системе аккредитации для выполнения работ по сертификации¹.

Менеджмент качества (Quality management) — скоординированная деятельность по руководству и управлению организацией применительно к качеству².

Менеджмент риска (Risk management) — скоординированные действия по руководству и управлению организацией в отношении риска.

Примечание. Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникацию риска³.

Менеджмент рисков (Risk management) — весь процесс идентификации, контроля и управления или минимизации подозрительных (неопределенных) событий, которые могут оказать негативное воздействие на ресурсы системы. **Примечание.** Адаптированный термин из ИСО/МЭК 13335-1. Менеджмент рисков обычно включает в себя анализ рисков, обработку рисков, принятие рисков, распространение информации о рисках (обмен или предоставление в совместное пользование информации о рисках между лицом, принимающим решение, и другими заинтересованными лицами)⁴.

Мероприятия по импортозамещению — комплекс мер (перечень мероприятий), направленных на плановое и поэтапное замещение закупки иностранной продукции (работ, услуг) закупкой, эквивалентной по техническим характеристикам и потребительским свойствам отечественной продукции (работ, услуг), исходя

¹ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

² ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

³ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

⁴ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

из принципов экономической целесообразности и технологической обоснованности¹.

Мероприятия по информатизации — мероприятия государственных органов, направленные на создание, развитие, эксплуатацию или использование информационно-коммуникационных технологий, а также вывод из эксплуатации информационных систем и компонентов информационно-телекоммуникационной инфраструктуры².

Мероприятия по информатизации — мероприятия по использованию информационно-коммуникационных технологий в деятельности государственных органов³.

Меры безопасности — меры защиты и контрмеры⁴.

Меры обеспечения безопасности (Security controls) — управленческие, организационные и технические меры обеспечения безопасности, применяемые в информационной системе для защиты и доступности системы и ее информации. **Примечания.** 1. Данное определение распространяется также на меры обеспечения безопасности, связанные с обеспечением подотчетности, аутентичности, неотказуемости, приватности и надежности, которые иногда рассматриваются отдельно от конфиденциальности, целостности и доступности⁵.

¹ Пункт 4 Методических рекомендаций по подготовке корпоративных планов импортозамещения государственными корпорациями, государственными компаниями, акционерными обществами, в уставном капитале которых доля участия Российской Федерации превышает 50 процентов, организациями, реализующими инвестиционные проекты, включенные в реестр инвестиционных проектов в соответствии с решением Правительственной комиссии по импортозамещению, утвержденных распоряжением Минэкономразвития России от 11 августа 2016 г. № 219Р-АУ.

² Постановление Правительства РФ от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» (вместе с Положением о координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов, Правилами подготовки планов информатизации государственных органов и отчетов об их выполнении). Пункт 2 Положения — извлечение.

³ Приказ Минкомсвязи России от 30 декабря 2016 г. № 745 «Об утверждении рекомендаций по согласованию с Министерством связи и массовых коммуникаций Российской Федерации предлагаемых главными распорядителями средств федерального бюджета изменений в сводную бюджетную роспись федерального бюджета и лимиты бюджетных обязательств по бюджетным ассигнованиям, предусмотренным на закупку товаров, работ, услуг в сфере информационно-коммуникационных технологий». Пункт 2 Рекомендаций — извлечение.

⁴ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

⁵ Там же.

Меры стимулирования деятельности в сфере промышленности — действия правового, экономического и организационного характера, которые осуществляются органами государственной власти, органами местного самоуправления, организациями, входящими в состав инфраструктуры поддержки деятельности в сфере промышленности, и направлены на достижение целей промышленной политики¹.

Метаданные документов (Metadata for records) — структурированная или полуструктурированная информация, которая позволяет создавать, управлять и использовать документы в разное время и в различных областях деятельности².

Место осуществления лицензируемого вида деятельности — объект (помещение, здание, сооружение, иной объект), который предназначен для осуществления лицензируемого вида деятельности и (или) используется при его осуществлении, соответствует лицензионным требованиям, принадлежит соискателю лицензии или лицензиату на праве собственности либо иным законным основанием, имеет почтовый адрес или другие позволяющие идентифицировать объект данные. Место осуществления лицензируемого вида деятельности может совпадать с местом нахождения соискателя лицензии или лицензиата³.

Место осуществления отдельного вида деятельности, подлежащего лицензированию — объект (помещение, здание, сооружение, иной объект), который предназначен для осуществления лицензируемого вида деятельности и (или) используется при его осуществлении, соответствует лицензионным требованиям, принадлежит соискателю лицензии или лицензиату на праве собственности либо иным законным основанием, имеет почтовый адрес или другие позволяющие идентифицировать объект данные. Место осуществления лицензируемого вида деятельности может совпадать с местом нахождения соискателя лицензии или лицензиата⁴.

Метка доверенного времени — достоверная информация в электронной форме о дате и времени подписания электронного документа электронной подписью, создаваемая и проверяемая доверенной

¹ Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

² ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

³ Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». Статья 3 — извлечение.

⁴ Там же.

третьей стороной, удостоверяющим центром или оператором информационной системы и полученная в момент подписания электронного документа электронной подписью в установленном уполномоченным федеральным органом порядке с использованием программных и (или) аппаратных средств, прошедших процедуру подтверждения соответствия требованиям, установленным в соответствии с настоящим Федеральным законом¹.

Метка конфиденциальности (Sensitivity label) — элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте².

Методическое обеспечение автоматизированной системы — совокупность документов, списывающих технологию функционирования АС, методы выбора и применения пользователями технологических приемов для получения конкретных результатов при функционировании АС³.

Метрологическая совместимость автоматизированных систем — частная совместимость АС, характеризующаяся тем, что точность результатов измерений, полученных в одной АС, позволяет использовать их в другой⁴.

Миграция (Migration) — процесс перемещения документов из одной аппаратной или программной конфигурации в другую без изменения формата⁵.

Микроданные — первичные данные после их первоначальной проверки на корректность, преобразованные к виду, удобному для автоматической обработки⁶.

Микро-ЭВМ — ЭВМ, относящаяся к классу вычислительных машин, центральная часть которых построена на одном или нескольких

¹ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2, пункт 19 — извлечение.

² Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

³ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁴ Там же.

⁵ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

⁶ Распоряжение Правительства РФ от 17 декабря 2019 г. № 3074-р «Концепция создания цифровой аналитической платформы». Пункт 1 — извлечение.

микропроцессорах и разработанных, исходя из требования минимизации физического объема¹.

Мини-ЭВМ — ЭВМ, относящаяся к классу вычислительных машин, разрабатываемых из требования минимизации стоимости и предназначенных для решения достаточно простых задач. Примечание. Как правило, мини-ЭВМ устанавливаются в обычных рабочих помещениях².

Многоуровневая защита (Multilevel secure) — защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности³.

Многофакторная аутентификация — аутентификация, для осуществления которой используются два и более различных факторов аутентификации⁴.

Многофункциональный центр предоставления государственных и муниципальных услуг (далее — многофункциональный центр) — организация, созданная в организационно-правовой форме государственного или муниципального учреждения (в том числе являющаяся автономным учреждением), отвечающая требованиям, установленным настоящим Федеральным законом, и уполномоченная на организацию предоставления государственных и муниципальных услуг, в том числе в электронной форме, по принципу «одного окна»⁵.

Модель жизненного цикла (Life cycle model) — структурная основа процессов и действий, относящихся к жизненному циклу, которая также служит в качестве общего эталона для установления связей и понимания⁶.

¹ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

² Там же.

³ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁴ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁵ Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

⁶ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

Модель защиты (Protection model) — абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа¹.

Модель нарушителя правил разграничения доступа (Security policy violator's model) — абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа².

Модель угроз безопасности информации — физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации. **Примечание.** Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ³.

Модернизация высокопроизводительных рабочих мест — комплекс организационно-технических мероприятий (дооборудование, реконструкция, приобретение соответствующего оборудования), которые приводят к повышению первоначальных характеристик и улучшению условий труда⁴.

Момент фактического задержания — момент производимого в порядке, установленном настоящим Кодексом (УПК РФ), фактического лишения свободы передвижения лица, подозреваемого в совершении преступления⁵.

Мониторинг безопасности информации — постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации⁶.

¹ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Госстехкомиссии России от 30 марта 1992 г.

² Там же.

³ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁴ Пункт 2 Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции, утвержденных постановлением Правительства РФ от 30 апреля 2019 г. № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции». Извлечение.

⁵ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁶ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

Мониторинг экспериментального правового режима — система наблюдений, осуществляемых на постоянной основе посредством сбора, обобщения, систематизации и оценки информации о выполнении программы экспериментального правового режима¹.

Монтированная емкость — величина, характеризующая технологические возможности оператора связи по оказанию на определенной территории Российской Федерации услуг электросвязи, услуг присоединения и услуг по пропуску трафика и измеряемая техническими возможностями оборудования, введенного в сеть оператора связи².

Мультипрограммирование — режим обработки информации, при котором ресурсы вычислительной машины или системы обработки информации используются более чем одним процессом обработки информации³.

Муниципальная отчетность — отчетность, собираемая органами местного самоуправления, за исключением административных данных⁴.

Муниципальная услуга, предоставляемая органом местного самоуправления (далее — **муниципальная услуга**) — деятельность по реализации функций органа местного самоуправления (далее — орган, предоставляющий муниципальные услуги), которая осуществляется по запросам заявителей в пределах полномочий органа, предоставляющего муниципальные услуги, по решению вопросов местного значения, установленных в соответствии с Федеральным законом от 6 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» и уставами муниципальных образований, а также в пределах предусмотренных указанным Федеральным законом прав органов местного самоуправления на решение вопросов, не отнесенных к вопросам местного значения, прав органов местного самоуправления на участие в осуществлении иных государственных полномочий (не переданных им в соответствии со статьей 19 указанного Федерального закона), если это участие предусмотрено федеральными законами, прав органов местного самоуправления на решение иных вопросов, не отнесенных к компетенции органов местного самоуправления

¹ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

² Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

³ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁴ Распоряжение Правительства РФ от 17 декабря 2019 г. № 3074-р «Концепция создания цифровой аналитической платформы». Пункт 1 — извлечение.

других муниципальных образований, органов государственной власти и не исключенных из их компетенции федеральными законами и законами субъектов Российской Федерации, в случае принятия муниципальных правовых актов о реализации таких прав¹.

Муниципальный заказчик — муниципальный орган или муниципальное казенное учреждение, действующие от имени муниципального образования, уполномоченные принимать бюджетные обязательства в соответствии с бюджетным законодательством Российской Федерации от имени муниципального образования и осуществляющие закупки².

Муниципальный контракт — гражданско-правовой договор, предметом которого являются поставка товара, выполнение работы, оказание услуги (в том числе приобретение недвижимого имущества или аренда имущества) и который заключен от имени муниципального образования муниципальным заказчиком для обеспечения муниципальных нужд³.

Н

Наведенный в токопроводящих линейных элементах технических средств сигнал; наводка — ток и напряжение в токопроводящих элементах, вызванные электромагнитным излучением, емкостными и индуктивными связями⁴.

Надежность автоматизированной системы — комплексное свойство АС сохранять во времени в установленных пределах значения всех параметров, характеризующих способность АС выполнять свои функции в заданных режимах и условиях эксплуатации. **Примечание.** Надежность АС включает свойства безотказности и ремонтпригодности АС, а в некоторых случаях и долговечности технических средств АС⁵.

¹ Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

² Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Пункт 6 статьи 3 — извлечение.

³ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Пункт 8 статьи 3 — извлечение.

⁴ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

Надзорная инстанция — Президиум Верховного Суда Российской Федерации, рассматривающий в порядке надзора уголовные дела по надзорным жалобам и представлениям на вступившие в законную силу приговоры, определения и постановления судов¹.

Налог — обязательный, индивидуально безвозмездный платеж, взимаемый с организаций и физических лиц в форме отчуждения принадлежащих им на праве собственности, хозяйственного ведения или оперативного управления денежных средств в целях финансового обеспечения деятельности государства и (или) муниципальных образований².

Нарушитель правил разграничения доступа (Security policy violator) — субъект доступа, осуществляющий несанкционированный доступ к информации³.

Научно-технический уровень автоматизированной системы — показатель или совокупность показателей, характеризующая степень соответствия техническим и экономическим характеристикам АС современным достижениям науки и техники⁴.

Национальная безопасность — состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства⁵.

Национальная безопасность Российской Федерации (далее — национальная безопасность) — состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее — граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопас-

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Налоговый кодекс Российской Федерации (часть первая) от 31 июля 1998 г. № 146-ФЗ. Статья 8 — извлечение.

³ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁵ Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». Пункт 6.

ность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности¹.

Национальная платежная система — совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, операторов платежных систем, операторов услуг платежной инфраструктуры (субъекты национальной платежной системы)².

Национальная электронная библиотека — федеральная государственная информационная система, представляющая собой совокупность документов и сведений в электронной форме (объекты исторического, научного и культурного достояния народов Российской Федерации), доступ к которым предоставляется с использованием сети «Интернет»³.

Национальные интересы Российской Федерации — совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства⁴.

Национальные интересы Российской Федерации — объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития⁵.

Национальные интересы Российской Федерации в информационной сфере (далее — национальные интересы в информационной сфере) — объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы⁶.

¹ Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». Раздел I, пункт 6 — извлечение.

² Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

³ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁴ Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». Пункт 6.

⁵ Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». Раздел I, пункт 6 — извлечение.

⁶ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

Национальные счета — совокупность балансовых таблиц и методов их составления, обеспечивающая формирование официальной статистической информации о валовом внутреннем продукте и других макроэкономических показателях¹.

Национальный проект — проект (программа), обеспечивающий достижение целей и целевых показателей, выполнение задач, определенных Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» (далее — Указ), а также при необходимости достижение дополнительных показателей и выполнение дополнительных задач по поручению и (или) указанию Президента Российской Федерации, поручению Председателя Правительства Российской Федерации, Правительству Российской Федерации, решению Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (далее — Совет), президиума Совета и подлежащий разработке в соответствии с Указом².

Начало эксплуатации — момент ввода изделия в эксплуатацию. Для изделий бытового назначения началом эксплуатации является момент их продажи через розничную торговую сеть или получения их покупателем при внерыночном потреблении. Начало эксплуатации комплектующих изделий и составных частей совпадает с началом эксплуатации основного изделия³.

Начальник органа дознания — должностное лицо органа дознания, в том числе заместитель начальника органа дознания, уполномоченное давать поручения о производстве дознания и неотложных следственных действий, осуществлять иные полномочия, предусмотренные УПК РФ⁴.

Начальник подразделения дознания — должностное лицо органа дознания, возглавляющее соответствующее специализированное под-

¹ Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Статья 2 — извлечение.

² Пункт 3 Положения об организации проектной деятельности в Правительстве Российской Федерации, в ред. постановления Правительства РФ от 31 октября 2018 г. № 1288 (ред. от 30.07.2019) «Об организации проектной деятельности в Правительстве Российской Федерации». Извлечение.

³ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

разделение, которое осуществляет предварительное расследование в форме дознания, а также его заместитель¹.

Неавтоматизированный режим выполнения функции автоматизированной системы — режим выполнения функции АС, при котором она выполняется человеком².

Недекларированные возможности — функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. Реализацией недекларированных возможностей, в частности, являются **программные закладки**³.

Недекларированные возможности программного обеспечения — функциональные возможности программного обеспечения, не описанные в документации⁴.

Некапитальные строения, сооружения — строения, сооружения, которые не имеют прочной связи с землей и конструктивные характеристики которых позволяют осуществить их перемещение и (или) демонтаж и последующую сборку без несоразмерного ущерба назначению и без изменения основных характеристик строений, сооружений (в том числе киосков, навесов и других подобных строений, сооружений)⁵.

Неопределенность — состояние хотя бы частичной неполноценности информации, необходимой для понимания или познания события, его последствий и вероятности наступления этого события⁶.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Руководящий документ. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114). Пункт 2 — извлечение.

⁴ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

⁵ Пункт 10.2 статьи 1 Градостроительного кодекса Российской Федерации от 29 декабря 2004 г. № 190-ФЗ (ред. от 02.08.2019).

⁶ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

Неотложные следственные действия — действия, осуществляемые органом дознания после возбуждения уголовного дела, по которому производство предварительного следствия обязательно, в целях обнаружения и фиксации следов преступления, а также доказательств, требующих незамедлительного закрепления, изъятия и исследования¹.

Непрерывно выполняемая функция автоматизированной системы управления технологическим процессом — функция АСУ технологическим процессом, у которой в любой момент времени функционирования есть результат ее выполнения².

Непричастность — неустановленная причастность либо установленная непричастность лица к совершению преступления³.

Несанкционированное воздействие на информацию — воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации⁴.

Несанкционированный доступ к информации (Unauthorized access to information) — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем⁵.

Норма эффективности защиты информации — значение показателя эффективности защиты информации, установленное нормативными и правовыми документами⁶.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁴ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁵ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Госстехкомиссии России от 30 марта 1992 г.

⁶ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

Нормальная эксплуатация — эксплуатация изделий в соответствии с действующей эксплуатационной документацией. Для специальных видов техники вместо термина «Нормальная эксплуатация» допускается использовать термин «Штатная эксплуатация»¹.

Нормативно-справочная информация автоматизированной системы — информация, заимствованная из нормативных документов и справочников и используемая при функционировании АС².

Нормативный правовой акт — это письменный официальный документ, принятый (изданный) в определенной форме правотворческим органом в пределах его компетенции и направленный на установление, изменение или отмену правовых норм. В свою очередь, под правовой нормой принято понимать общеобязательное государственное предписание постоянного или временного характера, рассчитанное на многократное применение³.

Носители сведений, составляющих государственную тайну — материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов⁴.

Носитель данных — материальный объект, предназначенный для записи и хранения данных⁵.

Носитель защищаемой информации — физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин⁶.

¹ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Постановление ГД ФС РФ от 11 ноября 1996 г. № 781-11 ГД «Об обращении в Конституционный Суд Российской Федерации». Извлечение.

⁴ Закон Российской Федерации о государственной тайне от 21 июля 1993 г. № 5485-1. Статья 2 — извлечение.

⁵ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁶ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

Ночное время — промежуток времени с 22 до 6 часов по местному времени¹.

Нумерация — цифровое, буквенное, символьное обозначение или комбинации таких обозначений, в том числе коды, предназначенные для однозначного определения (идентификации) сети связи и (или) ее узловых или оконечных элементов².

О

Обвинение — утверждение о совершении определенным лицом деяния, запрещенного уголовным законом, выдвинутое в порядке, установленном УПК РФ³.

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных⁴.

Обеспечение информационной безопасности — осуществление взаимосвязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления⁵.

Обеспечение информационной безопасности — деятельность органов федеральной службы безопасности, осуществляемая ими в пределах своих полномочий: при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств; при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу зашифрованной информации, в Россий-

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ, статья 5. Извлечение.

² Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁴ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

⁵ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

ской Федерации и ее учреждениях, находящихся за пределами Российской Федерации¹.

Обеспечение национальной безопасности — реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов².

Обеспечивающая система (Enabling system) — система, которая служит дополнением к рассматриваемой системе на протяжении стадий ее жизненного цикла, но необязательно вносит непосредственный вклад в ее функционирование. **Примечания.** 1. Например, когда рассматриваемая система вступает в стадию производства, требуется обеспечивающая производственная система. 2. Каждая обеспечивающая система имеет свой собственный жизненный цикл. Настоящий стандарт может применяться для любой обеспечивающей системы, если она представляется в качестве рассматриваемой системы³.

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам⁴.

Обладатель информации, составляющей коммерческую тайну — лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны⁵.

Облачные вычисления — информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети «Интернет» к общему набору конфигурируемых вычислительных ресурсов («облаку»), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены

¹ Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности». Статья 11.2. — извлечение.

² Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». Раздел I, пункт 6 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Федеральный закон от 2 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁵ Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Статья 3 — извлечение.

и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера¹.

Обмен электронными сообщениями — получение операционным центром электронных сообщений, содержащих распоряжения участников платежной системы, передача указанных сообщений в платежный клиринговый центр, расчетный центр, а также передача извещений (подтверждений) о приеме и об исполнении распоряжений участников платежной системы².

Обобщенная трудовая функция — совокупность связанных между собой трудовых функций, сложившаяся в результате разделения труда в конкретном производственном или (бизнес) процессе³.

Обоснование бюджетных ассигнований — документ, характеризующий бюджетные ассигнования в очередном финансовом году (очередном финансовом году и плановом периоде)⁴.

Обработка больших объемов данных — совокупность подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных, источников информации, в объемах, которые невозможно обработать вручную за разумное время⁵.

Обработка информации — систематическое выполнение операций над данными, представляющими предназначенную для обработки информацию⁶.

¹ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

² Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

³ Приказ Минтруда России от 29 апреля 2013 г. № 170н «Об утверждении методических рекомендаций по разработке профессионального стандарта». Пункт 2 — извлечение.

⁴ Приказ Минкомсвязи России от 30 декабря 2016 г. № 745 «Об утверждении рекомендаций по согласованию с Министерством связи и массовых коммуникаций Российской Федерации предлагаемых главными распорядителями средств федерального бюджета изменений в сводную бюджетную роспись федерального бюджета и лимиты бюджетных обязательств по бюджетным ассигнованиям, предусмотренным на закупку товаров, работ, услуг в сфере информационно-коммуникационных технологий». Пункт 2 Рекомендаций — извлечение.

⁵ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁶ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных¹.

Обработка риска (Risk treatment) — процесс выбора и осуществления мер по модификации риска. **Примечания:** 1. Меры по обработке риска могут включать в себя избежание, оптимизацию, перенос или сохранение риска. 2. В настоящем стандарте термин «мера управления» (control) использован как синоним термина «мера» (measure)².

Обработка рисков (Risk treatment) — процесс выбора и реализации мер обеспечения безопасности (security controls) для изменения рисков. **Примечание.** Адаптированный термин из ИСО/МЭК 13335-1³.

Обработка текстов — использование вычислительной машины для ввода, редактирования, форматирования и печати текстов и документов⁴.

Обращение гражданина — направленные в государственный орган, орган местного самоуправления или должностному лицу в письменной форме или в форме электронного документа предложение, заявление или жалоба, а также устное обращение гражданина в государственный орган, орган местного самоуправления⁵.

Общее программное обеспечение автоматизированной системы — часть программного обеспечения АС, представляющая собой совокупность программных средств, разработанных вне связи с созданием данной АС. **Примечание.** Обычно ОПО АС представляет собой со-

¹ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

² ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

³ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации». Статья 4 — извлечение.

вокупность программ общего назначения, предназначенных для организации вычислительного процесса и решения часто встречающихся задач обработки информации¹.

Общее регулирование — нормативное правовое регулирование, содержащее общеобязательные государственные предписания постоянного или временного характера, рассчитанные на многократное применение, и действующее в Российской Федерации по состоянию на дату начала срока действия экспериментального правового режима, установленного Правительством Российской Федерации, а по направлению, предусмотренному пунктом 4 части 2 статьи 1 настоящего Федерального закона, — Банком России².

Общество знаний — общество, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов Российской Федерации³.

Объект адресации — объект капитального строительства, земельный участок или другой объект, предусмотренный установленным Правительством Российской Федерации перечнем объектов адресации⁴.

Объект деятельности — объект (процесс), состояние которого определяется поступающими на него воздействиями человека (коллектива) и, возможно, внешней среды⁵.

Объект доступа (Access object) — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа⁶.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

³ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁴ Федеральный закон от 28 декабря 2013 г. № 443-ФЗ «О федеральной информационной адресной системе и о внесении изменений в Федеральный закон «Об общих принципах организации местного самоуправления в Российской Федерации». Статья 2 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Приложение 1 — извлечение.

⁶ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Госкомиссии России от 30 марта 1992 г.

Объект доступа — объект информатизации, представляющий собой аппаратное средство, средство вычислительной техники и (или) сетевое оборудование, в том числе входящие в состав АС финансовой организации. Примечание — В составе основных типов объектов доступа рекомендуется как минимум рассматривать: АРМ пользователей и эксплуатационного персонала; серверное и сетевое оборудование; системы хранения данных; аппаратные модули безопасности (HSM); устройства печати и копирования информации; объекты доступа, расположенные в публичных (общедоступных) местах (в том числе банкоматы, платежные терминалы)¹.

Объект защиты информации — информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации².

Объект информатизации — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров³.

Объект капитального строительства — здание, строение, сооружение, объекты, строительство которых не завершено (далее — объекты незавершенного строительства), за исключением некапитальных строений, сооружений и неотделимых улучшений земельного участка (замощение, покрытие и другие)⁴.

Объект народного хозяйства — предприятие, объединение, учреждение или организация сферы материального производства или непродовольственной сферы хозяйства, расположенное на единой площадке⁵.

¹ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

² ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

³ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

⁴ Пункт 10 статьи 1 Градостроительного кодекса Российской Федерации от 29 декабря 2004 г. № 190-ФЗ (ред. от 02.08.2019).

⁵ ГОСТ Р 22.0.02-94 (в ред. Изменения № 1, принятого постановлением Госстандарта РФ от 31 мая 2000 г. № 148-ст) «Безопасность в чрезвычайных ситуациях.

Объекты административного управления — создаваемые заблаговременно по решению руководителей федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций объекты мобилизационного назначения, предназначенные для размещения и обеспечения деятельности соответствующего органа управления в период мобилизации и в военное время¹.

Объекты инженерной инфраструктуры — элементы систем водо-, тепло-, энерго-, газоснабжения, водоотведения, телефонизации, связи или иных систем, обеспечивающих функционирование режимных объектов².

Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры³.

Объекты критической информационной инфраструктуры — информационные системы и информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, в сфере здравоохранения, транспорта, связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности⁴.

Объекты режимные — объекты, на которых ведутся работы с использованием сведений, составляющих государственную тайну, и для функционирования которых установлены специальные меры безопасности⁵.

Объекты систематизации — информация об объектах и субъектах правоотношений и связанных с ними юридических фактах,

Определения основных понятий». Принят и введен в действие постановлением Госстандарта РФ от 22 декабря 1994 г. № 327 (Группа Т 00, ОКСТУ 0022). Извлечение.

¹ Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне». Примечания, пункт 3 — извлечение.

² Там же.

³ Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Статья 2 — извлечение.

⁴ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁵ Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне». Примечания, пункт 3 — извлечение.

а также технико-экономическая, социальная и информация, описывающая (характеризующая) предметы и явления окружающего мира¹.

Объекты ядерного комплекса — сооружения с ядерными реакторами, в том числе атомные станции, суда и другие плавсредства, космические и летательные аппараты, другие транспортные и транспортные средства или сооружения с промышленными, экспериментальными и исследовательскими ядерными реакторами, критическими и подкритическими ядерными стендами; сооружения, полигоны, установки и устройства с ядерными зарядами; другие содержащие ядерные материалы сооружения, установки для производства, использования, переработки, транспортирования ядерного топлива и ядерных материалов².

Однофакторная аутентификация — аутентификация, для осуществления которой используется один фактор аутентификации³.

Ожидание использования по назначению — нахождение изделия в состоянии готовности к использованию по назначению, предусмотренное в нормативно-технической документации⁴.

Оконечное оборудование — технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей⁵.

Окончателность перевода денежных средств — характеристика перевода денежных средств, обозначающая предоставление денежных средств получателю средств в определенный момент времени⁶.

¹ Проект в редакции от 4 июля 2018 г. Федерального закона «О систематизации и гармонизации информации в Российской Федерации». Статья 2 — извлечение.

² Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне». Примечания, пункт 3 — извлечение.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта» М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁴ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁵ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁶ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

Оперативная информация автоматизированной системы — информация, отражающая, на данный момент времени состояние объекта, на который направлена деятельность АС¹.

Оперативная память — память, в которой размещаются данные, над которыми непосредственно производятся операции процессора.

Примечание. Оперативная память может иметь несколько иерархических уровней².

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными³.

Оператор — организация, наделенная функциями организационно-технического, информационного и аналитического сопровождения организации и проведения конкурсного отбора получателей государственной поддержки, доведения до получателей государственной поддержки средств в виде субсидий, а также мониторинга программ деятельности лидирующих исследовательских центров⁴.

Оператор (Operator) — лицо или организация, которые выполняют операции системы (обеспечивают функционирование системы).

Примечания. 1. Роль оператора и роль пользователя могут выполняться одновременно или последовательно одним и тем же человеком или организацией. 2. Некоторые операторы в сочетании с их знаниями, умением и выполняемыми процедурами могут рассматриваться как системный элемент⁵.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

³ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

⁴ Пункт 2 Правил предоставления субсидий из федерального бюджета на государственную поддержку программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий, утвержденных постановлением правительства РФ от 3 мая 2019 г. № 551. Извлечение.

⁵ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

Оператор, занимающий существенное положение в сети связи общего пользования — оператор, который вместе с аффилированными лицами обладает в географически определенной зоне нумерации или на всей территории Российской Федерации не менее чем двадцатью пятью процентами монтированной емкости либо имеет возможность осуществлять пропуск не менее чем двадцати пяти процентов трафика¹.

Оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных².

Оператор обмена цифровых финансовых активов — юридическое лицо, совершающее сделки по обмену токенов на рубли или иностранную валюту. Операторами обмена цифровых финансовых активов могут быть только юридические лица, которые созданы в соответствии с законодательством Российской Федерации и осуществляют виды деятельности, указанные в статьях 3, 4, 5 Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг» (далее — Федеральный закон «О рынке ценных бумаг»), или юридические лица, являющиеся организаторами торговли в соответствии с Федеральным законом от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах» (далее — Федеральный закон «Об организованных торгах»)³.

Оператор обязательных общедоступных телеканалов и (или) радиоканалов — оператор связи, который на основании договора с абонентом оказывает услуги связи для целей телевизионного вещания и (или) радиовещания (за исключением услуг связи для целей проводного радиовещания) и в соответствии с настоящим Федеральным законом обязан осуществлять трансляцию обязательных общедоступных телеканалов и (или) радиоканалов, перечень которых определяется законодательством Российской Федерации о средствах массовой информации⁴.

Оператор платежной системы — организация, определяющая правила платежной системы, а также выполняющая иные обязанности, предусмотренные настоящим Федеральным законом

¹ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

² Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

³ Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

⁴ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

(от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»)¹.

Оператор по переводу денежных средств — организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств².

Оператор связи — юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии³.

Оператор специализированной электронной площадки — российское юридическое лицо, которое владеет специализированной электронной площадкой, в том числе необходимыми для ее функционирования программно-аппаратными средствами, обеспечивает ее функционирование, а также соответствует установленным в соответствии с пунктами 1 и 3 части 2 статьи 24.1 настоящего Федерального закона требованиям и включено в утвержденный Правительством Российской Федерации перечень операторов специализированных электронных площадок⁴.

Оператор универсального обслуживания — оператор связи, который оказывает услуги связи в сети связи общего пользования и на которого в порядке, предусмотренном настоящим Федеральным законом, возложена обязанность по оказанию универсальных услуг связи⁵.

Оператор услуг платежной инфраструктуры — операционный центр, платежный клиринговый центр и расчетный центр⁶.

Оператор электронной площадки — непубличное хозяйственное общество, в уставном капитале которого иностранным гражданам, лицам без гражданства, иностранным юридическим лицам принадлежит не более чем двадцать пять процентов долей (акций) такого общества и которое владеет электронной площадкой, в том числе необходимыми для ее функционирования программно-аппаратными средствами, обеспечивает ее функционирование, а также соответствует установленным в соответствии с пунктами 1 и 2 ча-

¹ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

² Там же.

³ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁴ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

⁵ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁶ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

сти 2 статьи 24.1 настоящего Федерального закона требованиям и включено в утвержденный Правительством Российской Федерации перечень операторов электронных площадок¹.

Оператор электронных денежных средств — оператор по переводу денежных средств, осуществляющий перевод электронных денежных средств без открытия банковского счета (перевод электронных денежных средств)².

Операционная концепция (Operational concept) — описательные и/или графические положения в границах предположений или намерений организации в отношении операций (функционирования, эксплуатации) или соответствующего множества систем. Примечание — Операционная концепция проектируется для того, чтобы дать общую картину операций (функционирования, эксплуатации) с использованием одной или более специальных систем или соответствующего множества систем в эксплуатационной среде организации на перспективу с точки зрения пользователя или оператора (см. также «концепция функционирования, эксплуатации»)³.

Операционная система — совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг⁴.

Операционные услуги — обеспечение в рамках платежной системы для участников платежной системы и их клиентов доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями⁵.

Операционный центр — организация, обеспечивающая в рамках платежной системы для участников платежной системы и их клиен-

¹ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

² Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

тов доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями¹.

Операция записи данных — операция занесения порции данных в память данных².

Операция устройства вычислительной машины — однозначно определенное действие, выполняемое устройством вычислительной машины и составляющее выполнение команды или реакцию на определенные условия³.

Операция чтения данных — операция получения порции данных из памяти данных⁴.

Оповещение населения о чрезвычайных ситуациях — доведение до населения сигналов оповещения и экстренной информации об опасностях, возникающих при угрозе возникновения или возникновении чрезвычайных ситуаций природного и техногенного характера, а также при ведении военных действий или вследствие этих действий, о правилах поведения населения и необходимости проведения мероприятий по защите⁵.

Определение поставщика (подрядчика, исполнителя) — совокупность действий, которые осуществляются заказчиками в порядке, установленном настоящим Федеральным законом, начиная с размещения извещения об осуществлении закупки товара, работы, услуги для обеспечения государственных нужд (федеральных нужд, нужд субъекта Российской Федерации) или муниципальных нужд либо в установленных настоящим Федеральным законом случаях с направления приглашения принять участие в определении поставщика (подрядчика, исполнителя) и завершаются заключением контракта⁶.

Орган исполнительной власти субъекта Российской Федерации по регулированию контрактной системы в сфере закупок — орган исполнительной власти субъекта Российской Федерации, уполномоченный

¹ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

² ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

³ Там же.

⁴ Там же.

⁵ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

⁶ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

на осуществление функций по обеспечению (во взаимодействии с федеральным органом исполнительной власти по регулированию контрактной системы в сфере закупок) реализации государственной политики в сфере закупок для обеспечения нужд субъекта Российской Федерации, организации мониторинга закупок для обеспечения нужд субъекта Российской Федерации, а также по методологическому сопровождению деятельности заказчиков, осуществляющих закупки для обеспечения нужд субъекта Российской Федерации¹.

Орган по сертификации — юридическое лицо или индивидуальный предприниматель, аккредитованные в соответствии с законодательством Российской Федерации об аккредитации в национальной системе аккредитации для выполнения работ по сертификации².

Организационная мера защиты информации — мера, не являющаяся технической мерой защиты информации, предусматривающая установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации и (или) иных связанных с ним объектов³.

Организационная совместимость автоматизированных систем — частная совместимость АС, характеризуемая согласованностью правил действия их персонала, регламентирующих взаимодействие этих АС⁴.

Организационное обеспечение автоматизированной системы — совокупность документов, устанавливающих организационную структуру, права и обязанности пользователей и эксплуатационного персонала АС в условиях функционирования, проверки и обеспечения работоспособности АС⁵.

¹ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

² Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁵ Там же.

Организационные меры безопасности (Operational controls) — меры безопасности информационной системы, которые, главным образом, реализуются и выполняются операторами, а не системами¹.

Организация (Organization) — лицо или группа лиц и необходимых средств с распределением ответственностей, полномочий и взаимоотношений. **Пример.** Компания, корпорация, фирма, предприятие, институт, благотворительная организация, единоличный торговец, ассоциация, части или комбинация перечисленного. **Примечание.** Определенная часть организации (даже такая небольшая, как единственное лицо) или определенная группа организаций могут рассматриваться как организация, если она имеет ответственность, полномочия и определенные отношения. Объединение лиц, организованных для некоторой конкретной цели, такое, как клуб, союз, корпорация или общество являются организацией².

Организация предпринимательского сообщества — определенная Правительством Российской Федерации некоммерческая организация (или некоммерческие организации), объединяющая на основе членства субъектов предпринимательской деятельности и представляющая предпринимательское сообщество по вопросам экспериментальных правовых режимов. Для рассмотрения инициативного предложения определяется одна организация предпринимательского сообщества, за исключением случая рассмотрения инициативного предложения в отношении экспериментального правового режима по направлению, предусмотренному пунктом 4 части 2 статьи 1 настоящего Федерального закона. Банк России вправе определить одну или несколько организаций, представляющих предпринимательское сообщество по вопросам экспериментальных правовых режимов по данному направлению. В этом случае определенная Банком России организация участвует в правоотношениях по указанному направлению в порядке, установленном настоящим Федеральным законом для организации предпринимательского сообщества, если иное не установлено Банком России³.

¹ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

² ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

³ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

Организация связи — юридическое лицо, осуществляющее деятельность в области связи в качестве основного вида деятельности. Положения настоящего Федерального закона, регулирующие деятельность организаций связи, применяются соответственно к индивидуальным предпринимателям, осуществляющим деятельность в области связи в качестве основного вида деятельности¹.

Органы дознания — государственные органы и должностные лица, уполномоченные в соответствии с настоящим Кодексом (УПК РФ) осуществлять дознание и другие процессуальные полномочия².

Органы управления единой государственной системой предупреждения и ликвидации чрезвычайных ситуаций — органы, создаваемые для координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, организаций в области защиты населения и территорий от чрезвычайных ситуаций и сил, привлекаемых для предупреждения и ликвидации чрезвычайных ситуаций³.

Отбор и передача на хранение или уничтожение (Disposition) — совокупность процессов, включающих экспертизу ценности, отбор, передачу на хранение или уничтожение документов, осуществляемых в соответствии с правилами или другими инструментами⁴.

Ответственный исполнитель — ответственный исполнитель — координатор комплексной программы, комплексного проекта, являющийся федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере, соответствующей направлениям реализации комплексной программы, комплексного проекта, или иным главным распорядителем средств федерального бюджета в сфере научно-технической или производственной деятельности, соответствующей направлениям реализации комплексной программы, комплексного проекта,

¹ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

² Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

³ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

⁴ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

отвечающим за их реализацию и достижение целевых показателей¹.

Отрасль промышленности — совокупность субъектов, осуществляющих деятельность в сфере промышленности, в рамках одной или нескольких классификационных группировок одного или нескольких видов экономической деятельности в соответствии с Общероссийским классификатором видов экономической деятельности².

Освоение производства промышленной продукции — мероприятия, обеспечивающие подготовку субъектов деятельности в сфере промышленности к выпуску ранее не производимой ими промышленной продукции или существенному увеличению количества ранее производимой промышленной продукции и включающие в себя подготовку к вводу в эксплуатацию основных средств и их ввод в эксплуатацию, разработку и отработку технологических процессов, овладение практическими навыками производства промышленной продукции³.

Основная память — оперативная память центрального процессора или ее часть, представляющая единое пространство памяти⁴.

Основные средства (Facility) — физические средства или оборудование, способствующие выполнению действий, например здания, инструменты, принадлежности⁵.

Особо опасные, технически сложные сооружения связи — сооружения связи, проектной документацией которых предусмотрены такие характеристики, как высота от семидесяти пяти до ста метров и (или) заглубление подземной части (полностью или частично) ниже планировочной отметки земли от пяти до десяти метров⁶.

¹ Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

² Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

³ Там же.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁶ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

Остаточный риск (Residual risk) — риск, который остается после обработки рисков¹.

Остаточный риск (Residual risk) — риск, остающийся после его обработки².

Отечественная продукция — товары, работы, услуги, а также программное обеспечение, которые полностью произведены или подвергнуты достаточной обработке (переработке) на территории РФ³. **Примечание.** При определении продукции, произведенной в РФ, рекомендуется руководствоваться в том числе Требованиями к промышленной продукции, предъявляемыми в целях ее отнесения к продукции, произведенной в РФ, утвержденными постановлением Правительства РФ от 17 июля 2015 г. № 719, а также официальными отраслевыми реестрами отечественной продукции, которые ведутся федеральными органами исполнительной власти.

Офисное программное обеспечение — офисный пакет, почтовые приложения, органайзер, средства просмотра, интернет-браузер, редактор презентаций, табличный редактор, текстовый редактор, сведения о которых включены в единый реестр российских программ для электронных вычислительных машин и баз данных, а также соответствующие дополнительным требованиям к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, утвержденным постановлением Правительства Российской Федерации от 23 марта 2017 г. № 325 «Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин

¹ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие Приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

² ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

³ Пункт 8 Методических рекомендаций по подготовке корпоративных планов импортозамещения государственными корпорациями, государственными компаниями, акционерными обществами, в уставном капитале которых доля участия Российской Федерации превышает 50 процентов, организациями, реализующими инвестиционные проекты, включенные в реестр инвестиционных проектов в соответствии с решением Правительственной комиссии по импортозамещению, утвержденных распоряжением Минэкономразвития России от 11 августа 2016 г. № 219Р-АУ.

и баз данных»¹. **Офисное программное обеспечение (Программное обеспечение офисное)** — к офисному программному обеспечению относятся операционная система, коммуникационное программное обеспечение, офисный пакет, почтовые приложения, органайзер, средства просмотра, интернет-браузер, редактор презентаций, табличный редактор, текстовый редактор, программное обеспечение файлового менеджера, справочно-правовая система, программное обеспечение системы электронного документооборота и средства антивирусной защиты. Офисное программное обеспечение состоит из автономного и (или) сетевого программного обеспечения и клиентского программного обеспечения. Офисное программное обеспечение может представлять собой совокупность взаимосвязанных программных продуктов, соответствующих классификатору программ для электронных вычислительных машин и баз данных в соответствии с законодательством РФ².

Официальная статистическая информация — сводная агрегированная документированная информация о количественной стороне массовых социальных, экономических, демографических, экологических и других общественных процессов в Российской Федерации, формируемая субъектами официального статистического учета в соответствии с официальной статистической методологией³.

Официальный сайт государственного органа или органа местного самоуправления (далее — официальный сайт) — сайт в информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), содержащий информацию о деятельности государственного органа или органа местного самоуправления, электронный адрес которого включает доменное имя, права на которое принадлежат государственному органу или органу местного самоуправления. Федеральным законом может быть предусмотрено создание единого портала, на котором размещаются официальные сайты нескольких государственных органов⁴.

¹ Постановление Правительства РФ от 8 июня 2018 г. № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности». Пункт 3, подпункт «а» — извлечение.

² Пункт 3 Дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российской программной безопасности, утвержденным постановлением Правительства Российской Федерации от 23 марта 2017 г. № 325 // СЗ РФ. 2017. № 14. Ст. 2062.

³ Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Статья 2 — извлечение.

⁴ Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Статья 1 — извлечение.

Официальный статистический учет — деятельность, направленная на проведение в соответствии с официальной статистической методологией федеральных статистических наблюдений и обработку данных, полученных в результате этих наблюдений, и осуществляемая в целях формирования официальной статистической информации¹.

Охраняемые сведения — сведения, составляющие государственную и иную охраняемую законом тайну².

Оценивание риска (Risk evaluation) — процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости³.

Оценка информационного риска — общий процесс анализа информационного риска и его оценивания⁴.

Оценка риска (Risk assessment) — общий процесс анализа риска и его оценивания⁵.

Оценка соответствия — прямое или косвенное определение соблюдения требований, предъявляемых к объекту⁶.

Оценка соответствия требованиям по защите информации — прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации⁷.

¹ Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Статья 2 — извлечение.

² Положение о государственном лицензировании деятельности в области защиты информации (утверждено решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

³ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

⁴ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27.12.2006 № 373-ст). Пункт 2 — извлечение.

⁵ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

⁶ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

⁷ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

Оценка рисков (Risk assessment) — процесс, включающий в себя идентификацию рисков, анализ рисков и оценивание рисков¹.

Очередной финансовый год — год, следующий за текущим финансовым годом².

Очередь автоматизированной системы — часть АС, для которой в техническом задании на создание АС в целом установлены отдельные сроки ввода и набор реализуемых функций³.

П

Пакет прикладных программ — система прикладных программ, предназначенная для решения задач определенного класса⁴.

Память данных — функциональная часть вычислительной машины или системы обработки информации, предназначенная для приема, хранения и выдачи данных⁵.

Паразитное электромагнитное излучение — электромагнитное излучение, являющееся результатом паразитной генерации в электрических цепях технических средств обработки информации⁶.

Пароль (Password) — идентификатор субъекта доступа, который является его (субъекта) секретом⁷.

¹ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

² Приказ Минкомсвязи России от 30 декабря 2016 г. № 745 «Об утверждении рекомендаций по согласованию с Министерством связи и массовых коммуникаций Российской Федерации предлагаемых главными распорядителями средств федерального бюджета изменений в сводную бюджетную роспись федерального бюджета и лимиты бюджетных обязательств по бюджетным ассигнованиям, предусмотренным на закупку товаров, работ, услуг в сфере информационно-коммуникационных технологий». Пункт 2 Рекомендаций — извлечение.

³ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁶ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

⁷ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

Паспорт Программы — документ, включающий в себя цели, целевые и дополнительные показатели и методики их расчета, задачи, результаты и перечень федеральных проектов Программы, общие сведения о федеральных проектах Программы, обеспечивающих достижение целей, целевых и дополнительных показателей, сроки реализации и объем финансового обеспечения Программы, информацию о кураторе, руководителе и администраторе Программы, а также иные сведения¹.

Паспорт федерального проекта Программы — документ, включающий в себя наименование федерального проекта Программы, его цели и показатели, в том числе с указанием значений по субъектам Российской Федерации, методики расчета показателей, задачи и результаты, вехи, контрольные точки (события) и мероприятия, обеспечивающие достижение целей и показателей, сроки реализации и объемы финансового обеспечения федерального проекта Программы, информацию о федеральном органе исполнительной власти, ответственном за реализацию федерального проекта Программы (далее — ответственный федеральный орган исполнительной власти), центре компетенций федерального проекта Программы (далее — центр компетенций), рабочей группе федерального проекта Программы (далее — рабочая группа) и руководителя федерального проекта Программы, а также иные сведения².

Педагог — педагогический работник, выполняющий в образовательной организации или организации, осуществляющей обучение, обязанности по обучению и воспитанию обучающихся³.

Передача информации, составляющей коммерческую тайну — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности⁴.

Перечень задач — официально утвержденный перечень текущих и перспективных задач Заказчика, требующих инновационного (высокотехнологичного) решения⁵.

¹ Пункт 3 Положения о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации», утвержденного постановлением Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации». Извлечение.

² Там же.

³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁴ Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Статья 3 — извлечение.

⁵ Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/Д01и «О направлении методических материалов» (вместе с Методическими мате-

- Перечень инновационной, высокотехнологичной продукции** — перечень продукции, отвечающей задачам, требующим инновационного (высокотехнологичного) решения, и критериям отнесения продукции к инновационной, и потенциально пригодных, применимых к внедрению на объектах Заказчика¹.
- Перечень сведений, составляющих государственную тайну**, — совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством².
- Первичные статистические данные** — документированная информация по формам федерального статистического наблюдения, получаемая от респондентов, или информация, документируемая непосредственно в ходе федерального статистического наблюдения³.
- Период преимущественного продления** — период времени после истечения срока регистрации доменного имени, в течение которого за прежним администратором сохраняется право продления этого срока⁴.
- Периодическое печатное издание** — газета, журнал, альманах, бюллетень, иное издание, имеющее постоянное наименование (название), текущий номер и выходящее в свет не реже одного раза в год⁵.
- Перевод денежных средств** — действия оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика⁶.
- Персональная ЭВМ** — настольная микро-ЭВМ, имеющая эксплуатационные характеристики бытового прибора и универсальные функциональные возможности⁷.

риалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

¹ Там же.

² Закон Российской Федерации о государственной тайне от 21 июля 1993 г. № 5485-1. Статья 2 — извлечение.

³ Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Статья 2 — извлечение.

⁴ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81), подпункт 1.1. Извлечение.

⁵ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

⁶ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁷ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)¹.

Плановый период — два финансовых года, следующие за очередным финансовым годом².

Платежная система — совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств, включающая оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств³.

Платежная система иностранная — совокупность организаций, присоединившихся к правилам платежной системы, организованной в соответствии с иностранным законодательством, и взаимодействующих по правилам платежной системы (участники иностранной платежной системы), в соответствии с которыми иностранный банк (иностранная кредитная организация) может выступать в качестве плательщика и получателя средств по переводам денежных средств участников иностранной платежной системы (иностранный центральный платежный клиринговый контрагент)⁴.

Платежная услуга — услуга по переводу денежных средств, услуга почтового перевода и услуга по приему платежей⁵.

Платежные клиринговые позиции — суммы денежных средств, подлежащих списанию и зачислению расчетным центром по банковским счетам участников платежной системы⁶.

Платежный клиринговый центр — организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках платежной системы прием к исполнению распоряжений участников платежной системы об осуществлении перевода

¹ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

² Приказ Минкомсвязи России от 30 декабря 2016 г. № 745 «Об утверждении рекомендаций по согласованию с Министерством связи и массовых коммуникаций Российской Федерации предлагаемых главными распорядителями средств федерального бюджета изменений в сводную бюджетную роспись федерального бюджета и лимиты бюджетных обязательств по бюджетным ассигнованиям, предусмотренным на закупку товаров, работ, услуг в сфере информационно-коммуникационных технологий». Пункт 2 Рекомендаций — извлечение.

³ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁴ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁵ Там же.

⁶ Там же.

денежных средств и выполнение иных действий, предусмотренных настоящим Федеральным законом (от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»)¹.

Побочное электромагнитное излучение — электромагнитное излучение, наблюдаемое при работе технических средств обработки информации².

Подведомственная государственному органу или органу местного самоуправления организация — государственное или муниципальное учреждение либо унитарное предприятие, созданные соответственно государственным органом Российской Федерации, органом государственной власти субъекта Российской Федерации, органом местного самоуправления³.

Подготовка населения в области защиты от чрезвычайных ситуаций — система мероприятий по обучению населения действиям при угрозе возникновения и возникновении чрезвычайных ситуаций природного и техногенного характера⁴.

Поддержка сведений о доменном имени — действия регистратора по внесению, изменению и удалению сведений в Реестре, относящихся к доменному имени и его администратору⁵.

Подконтрольная эксплуатация — эксплуатация с целью получения дополнительной информации⁶.

Подсистема (Subsystem) — один или более компонентов автоматизированной системы, которые допускают их выполнение отдельно от остальной системы⁷.

¹ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

² ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

³ Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

⁴ Федеральный закон от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера». Статья 1 — извлечение.

⁵ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

⁶ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁷ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

Подтверждение соответствия — документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров¹.

Поисковая система — информационная система, осуществляющая по запросу пользователя поиск в сети «Интернет» информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети «Интернет» для доступа к запрашиваемой информации, расположенной на сайтах в сети «Интернет», принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами².

Показатель защищенности средств вычислительной техники (Protection criterion of computer systems) — характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники³.

Показатель эффективности автоматизированной системы — мера или характеристика для оценки эффективности АС⁴.

Показатель эффективности защиты информации — мера или характеристика для оценки эффективности защиты информации⁵.

Поклоение ЭВМ — классификационная группа ЭВМ, объединяющая ЭВМ по используемой технологии реализации ее устройств, а также по уровню развития функциональных свойств и программного

¹ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

² Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

³ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Госстанкомиссии России от 30 марта 1992 г.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁵ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

обеспечения и характеризующая определенный период в развитии промышленности средств вычислительной техники¹.

Положение — положение о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции².

Положение о применимости (Statement of applicability) — документированное предписание, определяющее цели и меры управления, соответствующие и применимые к системе менеджмента информационной безопасности организации. **Примечание.** Цели и меры управления основываются на результатах и выводах процессов оценки и обработки рисков, на требованиях законодательных или нормативных актов, на обязательствах по контракту и бизнес-требованиях организации по отношению к информационной безопасности³.

Получатель государственной поддержки — российская организация, структурным подразделением которой является лидирующий исследовательский центр⁴.

Получатель гранта — российская организация, за исключением государственного (муниципального) учреждения, соответствующая требованиям⁵, в частности: получатель гранта не находится в про-

¹ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

² Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/Д01 и «О направлении методических материалов» (вместе с Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

³ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст. Пункт 3 — извлечение.

⁴ Пункт 2 Правил предоставления субсидий из федерального бюджета на государственную поддержку программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий, утвержденных постановлением правительства РФ от 3 мая 2019 г. № 551. Извлечение.

⁵ Требования к получателям грантов предусмотрены пунктом 15 Правил предоставления субсидий из федерального бюджета на поддержку проектов по преобразованию приоритетных отраслей экономики и социальной сферы на основе внедрения отечественных продуктов, сервисов и платформенных решений, созданных на базе «сквозных» цифровых технологий, утвержденных постановлением Правительства РФ от 3 мая 2019 г. № 550.

цессе ликвидации или реорганизации; получатель гранта обладает статусом налогового резидента РФ; в отношении получателя гранта не возбуждено производство по делу о несостоятельности (банкротстве) в соответствии с законодательством РФ о несостоятельности (банкротстве); получатель гранта не имеет неисполненной обязанности по уплате налогов, сборов, страховых взносов, пеней, штрафов и процентов, подлежащих уплате в соответствии с законодательством РФ о налогах и сборах¹.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами — получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций².

Пользователи официальной статистической информацией — государственные органы, органы МСУ, юридические и физические лица, обращающиеся к системе государственной статистики или субъектам официальной статистического учета за получением необходимой им статистической информации и (или) пользующиеся такой информацией³.

Пользователь (User) — лицо или группа лиц, извлекающих пользу из системы в процессе ее применения. **Примечание.** Роль пользователя и роль оператора может выполняться одновременно или последовательно одним и тем же человеком или организацией⁴.

Пользователь — лицо, заказывающее или использующее услуги, связанные с регистрацией доменных имен⁵.

¹ Пункт 4 Правил предоставления субсидий из федерального бюджета на поддержку проектов по преобразованию приоритетных отраслей экономики и социальной сферы на основе внедрения отечественных продуктов, сервисов и платформенных решений, созданных на базе «сквозных» цифровых технологий. Утверждены постановлением Правительства РФ от 3 мая 2019 г. № 550. Извлечение.

² Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

³ Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Статья 2 — извлечение.

⁴ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁵ Правила регистрации доменных имен в доменах .RU и .RF (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

- Пользователь автоматизированной системы** — лицо, участвующее в функционировании АС или использующее результаты ее функционирования¹.
- Пользователь информацией** — гражданин (физическое лицо), организация (юридическое лицо), общественное объединение, осуществляющие поиск информации о деятельности государственных органов и органов местного самоуправления. Пользователями информацией являются также государственные органы, органы местного самоуправления, осуществляющие поиск указанной информации в соответствии с настоящим Федеральным законом².
- Пользователь радиочастотным спектром** — лицо, которому выделена полоса радиочастот либо присвоены (назначены) радиочастота или радиочастотный канал³.
- Пользователь системы обработки информации** — юридическое или фактическое лицо, применяющее систему обработки информации⁴.
- Пользователь услугами связи** — лицо, заказывающее и (или) использующее услуги связи⁵.
- Пользовательское оборудование (оконечное оборудование)** — технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей⁶.
- Помехоустойчивость автоматизированной системы** — свойство АС, характеризующееся способностью выполнять свои функции в условиях воздействия помех, в частности от электромагнитных полей⁷.
- Поставщик (Supplier)** — организация или лицо, которые вступают в соглашение с приобретающей стороной на поставку продукта или услуги. Примечания. 1. Поставщиком может быть подрядчик, про-

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Статья 1 — извлечение.

³ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁶ Там же.

⁷ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

изводитель, торговец или продавец. 2. Иногда приобретающая сторона и поставщик являются частью одной и той же организации¹.

Портал государственных и муниципальных услуг — государственная информационная система, обеспечивающая предоставление государственных и муниципальных услуг в электронной форме, а также доступ заявителей к сведениям о государственных и муниципальных услугах, предназначенным для распространения с использованием информационно-телекоммуникационной сети «Интернет» и размещенным в государственных и муниципальных информационных системах, обеспечивающих ведение реестров государственных и муниципальных услуг².

Портфель проектов (Project portfolio) — совокупность проектов, направленных на достижение стратегических целей организации³.

Поставщик инновационного решения (Поставщик, Заявитель) — организация, осуществляющая разработку и/или производство и/или сбыт инновационной, высокотехнологичной продукции⁴.

Постановление — любое решение, за исключением приговора, вынесенное судьей единолично; решение, вынесенное президиумом суда при пересмотре соответствующего судебного решения, вступившего в законную силу; решение прокурора, руководителя следственного органа, следователя, дознавателя, вынесенное при производстве предварительного расследования, за исключением обвинительного заключения, обвинительного акта или обвинительного постановления⁵.

Потенциально опасный объект — объект, на котором расположены здания и сооружения повышенного уровня ответственности, либо

¹ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

² Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/Д01и «О направлении методических материалов» (вместе с Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

⁵ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

объект, на котором возможно одновременное пребывание более пяти тысяч человек¹.

«Почтовая служба» (комплекс программ) — специальное программное обеспечение, используемое в системе межведомственного электронного документооборота и предназначенное для организации почтового обмена электронными сообщениями по защищенным каналам связи².

Права логического доступа — набор действий, разрешенных для выполнения субъектом доступа над ресурсом доступа с использованием соответствующей учетной записи³.

Правила отбора и передачи (Disposition authority) — инструмент, который определяет действия по отбору и передаче отдельных документов на хранение или уничтожение⁴.

Правила платежной системы — документ (документы), содержащий (содержащие) условия участия в платежной системе, осуществления перевода денежных средств, оказания услуг платежной инфраструктуры и иные условия, определяемые оператором платежной системы в соответствии с настоящим Федеральным законом (от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе») ⁵.

Правила разграничения доступа (Security policy) — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа⁶.

Правовая защита информации — защита информации правовыми методами, включающая в себя разработку законодательных и норма-

¹ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

² Распоряжение Правительства РФ от 2 октября 2009 г. № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти». Извлечение.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2017). Пункт 3 — извлечение.

⁴ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

⁵ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁶ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

тивных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением¹.

Правовое обеспечение автоматизированной системы — совокупность правовых норм, регламентирующих правовые отношения при функционировании АС и юридический статус результатов ее функционирования. Примечание. Правовое обеспечение реализуют в организационном обеспечении АС².

Предварительный национальный стандарт — документ в области стандартизации, который утвержден национальным органом Российской Федерации по стандартизации и срок действия которого ограничен³.

Преднамеренное силовое электромагнитное воздействие на информацию — несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем⁴.

Предложение — рекомендация гражданина по совершенствованию законов и иных нормативных правовых актов, деятельности государственных органов и органов местного самоуправления, развитию общественных отношений, улучшению социально-экономической и иных сфер деятельности государства и общества⁵.

Предоплаченная карта — платежная карта, предоставляемая клиенту оператором электронных денежных средств, используемая для перевода электронных денежных средств, а также для осуществления иных операций, предусмотренных статьей 7 настоящего Федерального закона (27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»)⁶.

¹ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

⁴ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁵ Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации». Статья 4 — извлечение.

⁶ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

Предоставление государственных и муниципальных услуг в электронной форме — предоставление государственных и муниципальных услуг с использованием информационно-телекоммуникационных технологий, включая использование единого портала государственных и муниципальных услуг и (или) региональных порталов государственных и муниципальных услуг, в том числе осуществление в рамках такого предоставления электронного взаимодействия между государственными органами, органами местного самоуправления, организациями и заявителями. В целях предоставления государственных и муниципальных услуг в электронной форме могут использоваться другие средства информационно-телекоммуникационных технологий в случаях и порядке, которые определяются Правительством Российской Федерации¹.

Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц².

Предоставление информации, составляющей коммерческую тайну — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций³.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц⁴.

Председательствующий — судья, который руководит судебным заседанием при коллегиальном рассмотрении уголовного дела, а также судья, рассматривающий уголовное дело единолично⁵.

Представление — акт реагирования прокурора на судебное решение, вносимый в порядке, установленном УПК РФ⁶.

Предупреждение чрезвычайных ситуаций — комплекс мероприятий, проводимых заблаговременно и направленных на максимально возможное уменьшение риска возникновения чрезвычайных ситуаций, а также на сохранение здоровья людей, снижение разме-

¹ Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Статья 2 — извлечение.

² Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

³ Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Статья 3 — извлечение.

⁴ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

⁵ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁶ Там же.

ров ущерба окружающей среде и материальных потерь в случае их возникновения¹.

Прерывание — операция процессора, состоящая в регистрации предшествующего прерыванию состояния процессора и установлении нового состояния. Примечание. Прерывание является реакцией процессора на некоторые условия, возникшие в процессоре или вне его².

Претендент — лицо, имеющее намерение стать субъектом экспериментального правового режима³.

Приговор — решение о невинности или виновности подсудимого и назначении ему наказания либо об освобождении его от наказания, вынесенное судом первой или апелляционной инстанции⁴.

Приемочная документация на автоматизированную систему — документация, фиксирующая сведения, подтверждающие готовность АС к приемке ее в эксплуатацию, соответствие АС требованиям нормативных документов⁵.

Признак классификации уязвимостей — свойство или характеристика уязвимостей, по которым производится классификация⁶.

Применение меры пресечения — процессуальные действия, осуществляемые с момента принятия решения об избрании меры пресечения до ее отмены или изменения⁷.

Принятие риска (Risk acceptance) — решение по принятию риска⁸.

¹ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

² ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

³ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение.

⁷ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁸ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

Приобретающая сторона (Acquirer) — заинтересованная сторона, которая приобретает или получает продукт или услугу от поставщика.
Примечание. Другими широко используемыми терминами, обозначающими это понятие, являются покупатель, заказчик, владелец, плательщик или внешний/внутренний спонсор¹.

Приобретение (Acquisition) — процесс получения системы, продукта или услуги².

Присвоение (назначение) радиочастоты или радиочастотного канала — решение в письменной форме на использование конкретной радиочастоты или радиочастотного канала с указанием конкретного радиоэлектронного средства, целей и условий такого использования³.

Присяжный заседатель — лицо, привлеченное в установленном настоящим Кодексом (УПК РФ) порядке для участия в судебном разбирательстве и вынесения вердикта⁴.

Проблема, задача (Problem) — трудность, неопределенность или иначе реализуемое и нежелательное событие, множество событий, условие или ситуация, которые требуют исследования и корректирующего воздействия⁵.

Провайдер хостинга — лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет»⁶.

Программа деятельности лидирующего исследовательского центра — совокупность взаимосвязанных мероприятий, направленных на разработку и реализацию дорожных карт развития перспективных «сквозных» цифровых технологий и заключающихся в выполнении научных исследований и опытно-конструкторских разработок совместно с участниками консорциума на базе лидирующего исследовательского центра и передаче получателем государственной поддержки прав на полученные в ходе указанных исследований и разработок результаты интеллектуальной деятельности участникам консорциума для их внедрения в экономическую деятельность

¹ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

² Там же.

³ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁵ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁶ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

для цифровой трансформации приоритетных отраслей экономики и социальной сферы¹.

Программа экспериментального правового режима — акт специального регулирования, определяющий условия экспериментального правового режима и утверждаемый в соответствии с настоящим Федеральным законом нормативным правовым актом Правительства Российской Федерации (далее — акт Правительства Российской Федерации), а по направлению, предусмотренному пунктом 4 части 2 статьи 1 настоящего Федерального закона, — нормативным актом Банка России (далее также — акт Банка России)².

Программная закладка — преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недеklarированных возможностей программного обеспечения. **Примечание.** Программная закладка может быть реализована в виде вредоносной программы или программного кода³.

Программная совместимость автоматизированных систем — частная совместимость АС, характеризующая возможность работы программ одной системы в другой и обмена программами, необходимыми при взаимодействии АС⁴.

Программное воздействие — несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ⁵.

Программное изделие в автоматизированной системе — программное средство, изготовленное, прошедшее испытания установленного

¹ Пункт 2 Правил предоставления субсидий из федерального бюджета на государственную поддержку программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий, утвержденных постановлением правительства РФ от 3 мая 2019 г. № 551. Извлечение.

² Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

³ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁵ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

вида и поставляемое как продукция производственно-технического назначения для применения в АС¹.

Программное обеспечение автоматизированной системы — совокупность программ на носителях данных и программных документов, предназначенная для отладки, функционирования и проверки работоспособности АС².

Программное обеспечение в сфере информационной безопасности — программное обеспечение, соответствующее требованиям законодательства РФ в сфере обеспечения информационной безопасности и относящееся в соответствии с классификатором программ для электронных вычислительных машин и баз данных к классу «средства обеспечения информационной безопасности», сведения о котором включены в единый реестр российских программ для электронных вычислительных машин и баз данных³.

Программное обеспечение для ведения бюджетного учета — программное обеспечение, обеспечивающее автоматизацию функций, необходимых для ведения бюджетного учета в соответствии с законодательством РФ, сведения о котором включены в единый реестр российских программ для электронных вычислительных машин и баз данных⁴.

Программное обеспечение несанкционированного доступа в компьютерные сети — программное обеспечение, специально разработанное или модифицированное для того, чтобы избежать обнаружения средствами контроля или уничтожить защитные контрмеры ЭВМ или других сетевых устройств и осуществляющее любые из следующих функций: а) извлечение данных или информации из ЭВМ или сетевых устройств либо видоизменение системы или данных пользователя; или б) изменение стандартного режима работы программы или процесса обработки данных, позволяющее выполнять инструкции, получаемые извне⁵.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Там же.

³ Постановление Правительства РФ от 8 июня 2018 № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности». Пункт 3, подпункт «а» — извлечение.

⁴ Постановление Правительства РФ от 8 июня 2018 г. № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности». Пункт 3, подпункт «а» — извлечение.

⁵ Примечание. Программное обеспечение несанкционированного доступа в компьютерные сети не включает в себя любое из следующего: а) гипервизоры (программы управления операционными системами), программы отладки или программы

Программное обеспечение офисное — определение термина раскрыто при определении термина «офисное программное обеспечение».

Программно-методический комплекс системы автоматизированного проектирования — взаимосвязанная совокупность компонентов программного, информационного и методического обеспечения системы автоматизированного проектирования, включая, при необходимости, компоненты математического и лингвистического обеспечения, необходимая для получения законченного проектного решения по объекту проектирования или выполнения унифицированной процедуры¹.

Программно-технический комплекс автоматизированной системы — продукция, представляющая собой совокупность средств вычислительной техники, программного обеспечения и средств создания и заполнения машинной информационной базы при вводе системы в действие достаточных для выполнения одной или более задач АС².

Программные закладки — преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации³.

Программный продукт — программное обеспечение и соответствующая документация, функционально обеспечивающие решение таких задач, как: автоматизированное проектирование; проведение инженерного анализа; управление станками; управление инженер-

средства обратного проектирования; б) программное обеспечение технических средств защиты авторских прав; в) программное обеспечение, разработанное для установки производителями, сетевыми администраторами или пользователями с целью отслеживания ресурсов или восстановления системы. В соответствии с Указом Президента РФ от 21 июля 2014 г. № 519 «О внесении изменений в Список товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль, утвержденный Указом Президента Российской Федерации от 17 декабря 2011 г. № 1661». Пункт 87.1 — извлечение.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114). Пункт 2 — извлечение.

ными данными; поддержка технологии цифрового двойника изделия, цифрового двойника технологического процесса; симуляция и моделирование производства; управление жизненным циклом изделия (продукции); управление производственными процессами; планирование потребности в материалах; промышленная автоматика и автоматизированные системы управления технологическими процессами; управление процессами в российской организации, включая системы планирования ресурсами российской организации; управление производственными активами российской организации; мониторинг состояния оборудования; технологии обработки и анализа больших данных; управление техническим обслуживанием и ремонтом технологического оборудования; планирование производства; управление процессами послепродажного обслуживания¹.

Продление регистрации доменного имени — внесение в Реестр сведений о продлении срока регистрации доменного имени².

Продукт, продукция (Product) — результат процесса. **Примечание.** Имеются четыре согласованные исходные категории продукта (продукции): аппаратные средства (например, машинная механическая часть); программные средства (например, компьютерная программа); услуги (например, транспортные) и обработанные материалы (например, смазка)³.

Продукция — результат деятельности, представленный в материально-вещественной форме и предназначенный для дальнейшего использования в хозяйственных и иных целях; риск — вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда⁴.

¹ Пункт 2 Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции, утвержденных постановлением Правительства РФ от 30 апреля 2019 г. № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции». Извлечение.

² Правила регистрации доменных имен в доменах .RU и .RF (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

Продукция — товары и/или работы и/или услуги и/или иные объекты гражданских прав, приобретаемые заказчиком на возмездной основе¹.

Продукция средства массовой информации — тираж или часть тиража отдельного номера периодического печатного издания, отдельный выпуск телеканала, радиоканала, радиопрограммы, телепрограммы, кинохроникальной программы, тираж или часть тиража аудио- или видеозаписи программы, отдельный выпуск либо обновление сетевого издания, отдельный выпуск иного средства массовой информации².

Проект (Project) — усилия с определенными датами начала и окончания, предпринятые для создания продукции или услуг в соответствии с заданными ресурсами и требованиями. **Примечание.** Проект может рассматриваться как уникальный процесс, включающий в себя скоординированные и управляемые виды деятельности, и может быть комбинацией видов деятельности из процессов проекта и технических процессов, определенных в настоящем стандарте³. **Проект** — комплекс взаимосвязанных мероприятий, направленных на получение уникальных результатов в условиях временных и ресурсных ограничений⁴. **Проект** — комплекс взаимосвязанных мероприятий, направленных на получение уникальных результатов в условиях временных и ресурсных ограничений⁵.

Проект государственно-частного партнерства, проект муниципально-частного партнерства (далее также — проект) — проект, планируемый для реализации совместно публичным партнером и частным

¹ Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/ДО1и «О направлении методических материалов» (вместе с Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

² Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Пункт 3 Положения о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации», утвержденного постановлением Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации». Извлечение.

⁵ Пункт 3 Положения об организации проектной деятельности в Правительстве Российской Федерации, в ред. постановления Правительства РФ от 31 октября 2018 г. № 1288 (ред. от 30.07.2019) «Об организации проектной деятельности в Правительстве Российской Федерации». Извлечение.

партнером на принципах государственно-частного партнерства, муниципально-частного партнерства¹.

Проектирование (Design, noun) — результат процесса проектирования по определению системных элементов, взаимодействий и других характеристик рассматриваемой системы в соответствии с требованиями и архитектурой. **Примечания.** 1. Чтобы поддерживать соответствующую реализацию архитектуры, формируется информация, которая является существенной, включая спецификацию системных элементов и их отношения. 2. Проект обеспечивает детальный уровень реализации физической структуры, поведения, временных соотношений и другие атрибуты системных элементов².

Проектировать (Design, verb) — процесс определения системных элементов, взаимодействий и других характеристик рассматриваемой системы в соответствии с требованиями и архитектурой³.

Проектная деятельность — деятельность, связанная с инициированием, подготовкой, реализацией и завершением проектов⁴.

Проектное решение в САПР — описание в заданной форме объекта проектирования или его части, необходимое и достаточное для определения дальнейшего направления проектирования⁵.

Проектно-сметная документация на АС — часть документации на АС, разрабатываемая для выполнения строительных и монтажных работ, связанных с созданием АС⁶.

¹ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

² ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Пункт 3 Положения об организации проектной деятельности в Правительстве Российской Федерации, в ред. постановления Правительства РФ от 31 октября 2018 г. № 1288 (ред. от 30.07.2019) «Об организации проектной деятельности в Правительстве Российской Федерации». Извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ 34.201-89 «Государственный стандарт Союза ССР. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (утв. постановлением Госстандарта СССР от 24 марта 1989 г. № 664). Приложение 1 — извлечение.

Проектный документ в САПР — документ, выполненный по заданной форме, в котором представлено одно или несколько проектных решений¹.

Производственно-технологический процесс (технологический комплекс) — совокупность функционально взаимосвязанных средств технологического оснащения, включая технические средства и технологии, необходимых для выполнения производственных процессов или операций².

Прокурор — Генеральный прокурор Российской Федерации и подчиненные ему прокуроры, их заместители и иные должностные лица органов прокуратуры, участвующие в уголовном судопроизводстве и наделенные соответствующими полномочиями федеральным законом о прокуратуре³.

Промежуточное судебное решение — все определения и постановления суда, за исключением итогового судебного решения⁴.

Промышленная инфраструктура — совокупность объектов недвижимого имущества, объектов транспортной инфраструктуры и коммунальной инфраструктуры, необходимых для осуществления деятельности в сфере промышленности⁵.

Промышленная политика — комплекс правовых, экономических, организационных и иных мер, направленных на развитие промышленного потенциала Российской Федерации, обеспечение производства конкурентоспособной промышленной продукции⁶.

Промышленная продукция — товары, произведенные в результате осуществления деятельности в сфере промышленности⁷.

Промышленная продукция, не имеющая произведенных в Российской Федерации аналогов — промышленная продукция, которая отвечает

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Пункт 8 Методических рекомендаций по подготовке корпоративных планов импортозамещения государственными корпорациями, государственными компаниями, акционерными обществами, в уставном капитале которых доля участия Российской Федерации превышает 50 процентов, организациями, реализующими инвестиционные проекты, включенные в реестр инвестиционных проектов в соответствии с решением Правительственной комиссии по импортозамещению, утвержденным распоряжением Минэкономразвития России от 11 августа 2016 г. № 219Р-АУ.

³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁴ Там же.

⁵ Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

⁶ Там же.

⁷ Там же.

критериям, предусмотренным пунктом 2 части 1 статьи 6 настоящего Федерального закона, и не может быть заменена на продукцию, произведенную на территории Российской Федерации и имеющую схожие технические и эксплуатационные характеристики, позволяющие ей выполнять те же функции и быть коммерчески взаимозаменяемой¹.

Промышленное производство (промышленность) — определенная на основании Общероссийского классификатора видов экономической деятельности совокупность видов экономической деятельности, относящихся к добыче полезных ископаемых, обрабатывающему производству, обеспечению электрической энергией, газом и паром, кондиционированию воздуха, водоснабжению, водоотведению, организации сбора и утилизации отходов, а также ликвидации загрязнений².

Промышленность (промышленное производство) — определенная на основании Общероссийского классификатора видов экономической деятельности совокупность видов экономической деятельности, относящихся к добыче полезных ископаемых, обрабатывающему производству, обеспечению электрической энергией, газом и паром, кондиционированию воздуха, водоснабжению, водоотведению, организации сбора и утилизации отходов, а также ликвидации загрязнений³.

Промышленный кластер — совокупность субъектов деятельности в сфере промышленности, связанных отношениями в указанной сфере вследствие территориальной близости и функциональной зависимости и размещенных на территории одного субъекта Российской Федерации или на территориях нескольких субъектов Российской Федерации⁴.

Промышленный (индустриальный) парк — совокупность объектов промышленной инфраструктуры, предназначенных для создания промышленного производства или модернизации промышленного производства и управляемых управляющей компанией — коммерческой или некоммерческой организацией, созданной в соответствии с законодательством Российской Федерации⁵.

Промышленный технопарк — объекты промышленной инфраструктуры и технологической инфраструктуры, предназначенные для осуществления субъектами деятельности в сфере промышленности промышленного производства, и (или) научно-технической деятельности, и (или) инновационной деятельности в целях освоения производства промышленной продукции и коммерциализации полученных науч-

¹ Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

² Там же.

³ Там же.

⁴ Там же.

⁵ Там же.

но-технических результатов и управляемые управляющей компанией — коммерческой или некоммерческой организацией, созданной в соответствии с законодательством Российской Федерации¹.

Простая функция автоматизированной системы управления технологическим процессом — функция АСУ технологическим процессом, не разложимая на другие функции системы².

Профессиональный стандарт — характеристика квалификации, необходимой работнику для осуществления определенного вида профессиональной деятельности, в том числе выполнения определенной трудовой функции³.

Процесс (Process) — совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующая входы в выходы⁴.

Процесс создания автоматизированной системы — совокупность работ от формирования исходных требований к системе до ввода в действие⁵.

Процессор — функциональная часть вычислительной машины или системы обработки информации, предназначенная для интерпретации программ⁶.

Процессор ввода-вывода — процессор, выполняющий операции обмена данными между центральным процессором и периферийными устройствами⁷.

Процессуальное действие — следственное, судебное или иное действие, предусмотренное УПК РФ⁸.

¹ Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ. Статья 195.1, часть вторая — извлечение.

⁴ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁷ Там же.

⁸ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

Процессуальное решение — решение, принимаемое судом, прокурором, следователем, дознавателем в порядке, установленном УПК РФ¹.

Прямое соглашение — гражданско-правовой договор, заключенный между публичным партнером, частным партнером и финансирующим лицом или финансирующими лицами (далее также — финансирующее лицо) в целях регулирования условий и порядка их взаимодействия в течение срока реализации соглашения, а также при изменении и прекращении соглашения².

Публичный партнер — Российская Федерация, от имени которой выступает Правительство Российской Федерации или уполномоченный им федеральный орган исполнительной власти, либо субъект Российской Федерации, от имени которого выступает высший исполнительный орган государственной власти субъекта Российской Федерации или уполномоченный им орган исполнительной власти субъекта Российской Федерации, либо муниципальное образование, от имени которого выступает глава муниципального образования или иной уполномоченный орган местного самоуправления в соответствии с уставом муниципального образования³.

Р

Рабочая документация на автоматизированную систему — комплект проектных документов на АС, разрабатываемый на стадии «Рабочая документация», содержащий взаимоувязанные решения по системе в целом, ее функциям, всем видам обеспечения АС, достаточные для комплектации, монтажа, наладки и функционирования АС, ее проверки и обеспечения работоспособности⁴.

Рабочая документация на автоматизированную систему — часть документации на АС, необходимой для изготовления, строительства, монтажа и наладки автоматизированной системы в целом, а также входящих в систему программно-технических, программно-мето-

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

³ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

дических комплексов и компонентов технического, программного и информационного обеспечения¹.

Рабочий процесс (Work process) — одно или несколько последовательных действий, необходимых для создания результата, соответствующего правилам управления².

Радиоканал, телеканал — сформированная в соответствии с сеткой вещания и выходящая в свет (эфир) под постоянным наименованием и с установленной периодичностью совокупность теле-, радиопрограмм и (или) соответственно иных аудиовизуальных, звуковых сообщений и материалов³.

Радиопомеха — воздействие электромагнитной энергии на прием радиоволн, вызванное одним или несколькими излучениями, в том числе радиацией, индукцией, и проявляющееся в любом ухудшении качества связи, ошибках или потерях информации, которых можно было бы избежать при отсутствии воздействия такой энергии⁴.

Радиочастота — частота электромагнитных колебаний, устанавливаемая для обозначения единичной составляющей радиочастотного спектра⁵.

Радиочастотный спектр — упорядоченная совокупность радиочастот в установленных Международным союзом электросвязи пределах, которые могут быть использованы для функционирования радиоэлектронных средств или высокочастотных устройств⁶.

Радиоэлектронные средства — технические средства, предназначенные для передачи и (или) приема радиоволн, состоящие из одного или нескольких передающих и (или) приемных устройств либо комбинации таких устройств и включающие в себя вспомогательное оборудование⁷.

¹ ГОСТ 34.201-89 «Государственный стандарт Союза ССР. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (утв. постановлением Госстандарта СССР от 24 марта 1989 г. № 664). Приложение 1 — извлечение.

² ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

³ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение; Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

⁴ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁵ Там же.

⁶ Там же.

⁷ Там же.

Разглашение информации, составляющей коммерческую тайну — действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору¹.

Развитие автоматизированной системы — целенаправленное улучшение характеристик или расширение функций АС².

Разрабатываемый компонент — адаптер системы электронного документооборота, который является специализированным программным обеспечением, разрабатываемым для каждого типа системы электронного документооборота. Адаптер системы электронного документооборота предназначен для преобразования передаваемых или получаемых данных, входящих в состав электронных сообщений, в формат представления данных, используемый в системе электронного документооборота или в стандартный формат данных при обмене электронными сообщениями³.

Распределение полос радиочастот — определение предназначения полос радиочастот посредством записей в Таблице распределения полос радиочастот между радиослужбами Российской Федерации, на основании которых выдается разрешение на использование конкретной полосы радиочастот, а также устанавливаются условия такого использования⁴.

Распределенный реестр цифровых транзакций — формируемая на определенный момент времени систематизированная база цифровых транзакций, которые хранятся, одновременно создаются и обновляются на всех носителях у всех участников реестра на основе заданных алгоритмов, обеспечивающих ее тождественность у всех пользователей реестра⁵.

¹ Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Статья 3 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Распоряжение Правительства РФ от 2 октября 2009 г. № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти». Извлечение.

⁴ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁵ Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц¹.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц².

Распространение продукции средства массовой информации — продажа, подписка, доставка, раздача периодического печатного издания, аудио- или видеозаписи программы, вещание телеканала, радиоканала (телевизионное вещание, радиовещание), вещание телепрограммы, радиoproграммы в составе соответственно телеканала, радиоканала, демонстрация кинохроникальной программы, предоставление доступа к сетевому изданию, иные способы распространения³.

Распространитель — лицо, осуществляющее распространение продукции средства массовой информации по договору с редакцией, издателем или на иных законных основаниях⁴.

Рассматриваемая система (System-of-interest) — система, жизненный цикл которой рассматривается в рамках настоящего стандарта⁵.

Расчетные услуги — исполнение распоряжений участников платежной системы посредством списания и зачисления денежных средств по банковским счетам участников платежной системы, а также направление подтверждений, касающихся исполнения распоряжений участников платежной системы⁶.

Расчетный центр — организация, созданная в соответствии с законодательством Российской Федерации, если иное не предусмотрено настоящим Федеральным законом, и обеспечивающая в рамках платежной системы исполнение распоряжений участников платежной системы посредством списания и зачисления денежных средств по банковским счетам участников платежной системы, а также направление подтверждений, касающихся исполнения распоряжений участников платежной системы (далее — расчетные услуги)⁷.

¹ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

² Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

³ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

⁴ Там же.

⁵ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁶ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁷ Там же.

Реабилитация — порядок восстановления прав и свобод лица, незаконно или необоснованно подвергнутого уголовному преследованию, и возмещения причиненного ему вреда¹.

Реабилитированный — лицо, имеющее в соответствии с настоящим Кодексом (УПК РФ) право на возмещение вреда, причиненного ему в связи с незаконным или необоснованным уголовным преследованием².

Реальная эксплуатация — эксплуатация в сложившихся в эксплуатирующей организации условиях³.

Региональная организация по стандартизации — организация, членами (участниками) которой являются национальные органы (организации) по стандартизации государств, входящих в один географический регион мира и (или) группу стран, находящихся в соответствии с международными договорами в процессе экономической интеграции⁴.

Региональная отчетность — отчетность, собираемая органами государственной власти субъектов Российской Федерации, за исключением административных данных⁵.

Региональный проект — проект, обеспечивающий достижение целей, показателей и результатов федерального проекта, мероприятия которого относятся к законодательно установленным полномочиям субъекта Российской Федерации, а также к вопросам местного значения муниципальных образований, расположенных на территории указанного субъекта Российской Федерации⁶. **Региональный проект** — реализуемый получателем гранта ограниченный по времени и ресурсам комплекс мероприятий, соответствующих требованиям, установленным Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации по согласованию с Министерством финансов Российской Федерации и одобренным президиумом Правительственной

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Там же.

³ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁴ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

⁵ Распоряжение Правительства РФ от 17 декабря 2019 г. № 3074-р «Концепция создания цифровой аналитической платформы». Пункт 1 — извлечение.

⁶ Пункт 3 Положения об организации проектной деятельности в Правительстве Российской Федерации, в ред. постановления Правительства РФ от 31 октября 2018 г. № 1288 (ред. от 30.07.2019) «Об организации проектной деятельности в Правительстве Российской Федерации». Извлечение.

комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, имеющих высокую социально-экономическую значимость для субъекта Российской Федерации, направленных на разработку и (или) внедрение отечественных продуктов, сервисов и платформенных решений, созданных на базе «сквозных» цифровых технологий, во взаимосвязи с приоритетами, технологиями и субтехнологиями, определенными дорожными картами по направлениям развития «сквозных» цифровых технологий¹.

Региональный проект Программы — проект, обеспечивающий достижение целей, показателей и результатов федерального проекта Программы, мероприятия которого относятся к законодательно установленным полномочиям субъекта Российской Федерации, а также к вопросам местного значения муниципальных образований, расположенных на территории указанного субъекта Российской Федерации².

Региональный свод правил — свод правил, принятый региональной организацией по стандартизации³.

Региональный стандарт — стандарт, принятый региональной организацией по стандартизации⁴.

Регистратор — юридическое лицо, аккредитованное Координатором для регистрации доменных имен в доменах .RU и/или .РФ⁵.

Регистратор-донор — регистратор, передающий регистратору-реципиенту поддержку сведений о доменном имени⁶.

Регистратор-реципиент — регистратор, принимающий от регистратора-донора поддержку сведений о доменном имени⁷.

¹ Пункт 4 Правил предоставления субсидий из федерального бюджета на поддержку проектов по преобразованию приоритетных отраслей экономики и социальной сферы на основе внедрения отечественных продуктов, сервисов и платформенных решений, созданных на базе «сквозных» цифровых технологий. Утверждены постановлением Правительства РФ от 3 мая 2019 г. № 550. Извлечение.

² Пункт 3 Положения о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации», утвержденного постановлением Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации». Извлечение.

³ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

⁴ Там же.

⁵ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

⁶ Там же.

⁷ Там же.

Регистрация доменного имени — внесение в Реестр сведений о доменном имени, его администраторе и иных сведений, установленных Правилами¹.

Регистрация событий защиты информации (регистрация) — фиксация данных о совершенных субъектами доступа действиях или данных о событиях защиты информации².

Регламентирующие документы Координатора — официальные документы Координатора, регулирующие деятельность, связанную с регистрацией доменных имен второго уровня в доменах верхнего уровня .RU и .РФ, и/или содержащие обязательные для исполнения правила и принципы регистрации доменных имен, устанавливающие основные права и обязанности администраторов доменных имен и регистраторов и т. п., к коим относятся настоящие Правила и Приложения к ним, Положение об аккредитации, Соглашение об аккредитации, Требования к аккредитованной организации (Регистратору)³.

Регламентный информационный ресурс — нормативно установленный информационный ресурс⁴.

Регулирующий орган — федеральный орган исполнительной власти, осуществляющий функции по выработке государственной политики и нормативному правовому регулированию по одному из направлений, предусмотренных частью 2 статьи 1 настоящего Федерального закона, а по направлению, предусмотренному пунктом 4 части 2 статьи 1 настоящего Федерального закона, — Банк России⁵.

Регулятивная песочница — специально согласованный режим проработки и пилотирования решений, в том числе регуляторных, для определения эффективной модели взаимодействия и построения бизнес-процессов в какой-либо новой сфере. «Регулятивную песочницу» целесообразно использовать для проработки механизмов

¹ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

² ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2017). Пункт 3 — извлечение.

³ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

⁴ Проект в редакции от 4 июля 2018 г. Федерального закона «О систематизации и гармонизации информации в Российской Федерации». Статья 2 — извлечение.

⁵ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

и правил регулирования экономических процессов в рамках цифровых инициатив и проектов¹.

Редакция средства массовой информации — организация, учреждение, предприятие либо гражданин, объединение граждан, осуществляющие производство и выпуск средства массовой информации².

Реестр — база данных Координатора, содержащая сведения о зарегистрированных доменных именах второго уровня, их администраторах и другие необходимые сведения³.

Реестр обращений — реестр, в котором размещаются все заявки, поступившие от Поставщиков, а также отражается информация о статусе инновационного (высокотехнологичного) решения. Формат Реестра обращений устанавливается Заказчиком. Также Заказчик устанавливает состав и содержание публичной и непубличной частей Реестра обращений⁴.

Реестр цифровых транзакций — формируемая на определенный момент времени систематизированная база цифровых записей⁵.

Режим пакетной обработки — режим выполнения совокупности задач, при котором все они выполняются системой обработки информации в основном автоматически без синхронизации с событиями вне этой СОИ, в частности, без связи с лицами, представившими задание для выполнения⁶.

Режим разделения времени — мультипрограммирование, при котором ресурсы системы обработки информации предоставляются каждому процессу из группы процессов обработки информации, находящихся в СОИ, на интервалы времени, длительность и очередность

¹ Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». Раздел 1. Определения — извлечение.

² Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

³ Правила регистрации доменных имен в доменах .RU и .RF (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

⁴ Пункт 2 <Письма> Минэкономразвития России от 29 декабря 2018 г. № 39283-СГ/Д01и «О направлении методических материалов» (вместе с Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции, Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации).

⁵ Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

⁶ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

представления которых определяется управляющей программой этой СОО с целью обеспечения одновременной работы процессов этой группы в интерактивном режиме¹.

Режим реального времени — режим обработки информации, при котором обеспечивается взаимодействие системы обработки информации с внешними по отношению к ней процессами в темпе, соизмеримом со скоростью протекания этих процессов².

Режим функционирования органов управления и сил единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций — определяемые в зависимости от обстановки, прогнозирования угрозы чрезвычайной ситуации и возникновения чрезвычайной ситуации порядок организации деятельности органов управления и сил единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций и основные мероприятия, проводимые указанными органами и силами в режиме повседневной деятельности, при введении режима повышенной готовности или чрезвычайной ситуации³.

Режимные объекты — объекты, на которых ведутся работы с использованием сведений, составляющих государственную тайну, и для функционирования которых установлены специальные меры безопасности⁴.

Результат проектирования в САПР — проектное решение (совокупность проектных решений), удовлетворяющее заданным требованиям, необходимое для создания объекта проектирования⁵.

Результаты оперативно-розыскной деятельности — сведения, полученные в соответствии с федеральным законом об оперативно-розыскной деятельности, о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда⁶.

¹ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

² Там же.

³ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

⁴ Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне». Примечания, пункт 3 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

Реквизиты документа — файл формата XML определенной структуры с указанным составом элементов и их атрибутов¹.

Ремонт — по ГОСТ 18322-78. Ремонт изделий может сопровождаться его модернизацией. Для специальных видов техники некоторые виды ремонта могут не входить в состав эксплуатации².

Реплика — замечание участника прений сторон относительно сказанного в речах других участников³.

Ресурс (Resource) — актив, который используется или потребляется в ходе выполнения процесса. **Примечания.** 1. Ресурсы могут включать в себя разнообразные объекты, такие как персонал, оборудование, основные средства, инструменты, а также коммунальные услуги: энергию, воду, топливо и инфраструктуру средств связи. 2. Ресурсы могут быть многократно используемыми, возобновляемыми или расходуемыми⁴.

Ресурс доступа — объект информатизации, представляющий собой совокупность информации и программного обеспечения (ПО) обработки информации. Примечание — В составе основных типов ресурсов доступа рекомендуется как минимум рассматривать: АС; базы данных; сетевые файловые ресурсы; виртуальные машины, предназначенные для размещения серверных компонентов АС; виртуальные машины, предназначенные для размещения АРМ пользователей и эксплуатационного персонала; ресурсы доступа, относящиеся к сервисам электронной почты; ресурсы доступа, относящиеся к WEB-сервисам финансовой организации в сетях Интранет и Интернет⁵.

Ресурс нумерации — совокупность или часть вариантов нумерации, которые возможно использовать в сетях связи⁶.

¹ Распоряжение Правительства РФ от 2 октября 2009 г. № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти». Извлечение.

² ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁴ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁵ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2017). Пункт 3 — извлечение.

⁶ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

Ресурс персональных данных — база данных или иная совокупность персональных данных (ПДн) многих субъектов ПДн, объединенных общими целями обработки, обрабатываемых финансовой организацией с использованием или без использования объектов информатизации, в том числе АС¹.

Решение процессуальное — решение, принимаемое судом, прокурором, следователем, дознавателем в порядке, установленном УПК РФ².

Риск (Risk) — эффект неопределенности в целях, задачах. **Примечания.** 1. Под эффектом неопределенности понимается отклонение от ожидаемого — позитивное и/или негативное. Позитивный эффект рассматривается также как возможности. 2. Цели, задачи могут быть различными по содержанию (в области финансов, здоровья и безопасности, среды и т. п.) и дифференцированы по различным уровням (стратегическим, общеорганизационным, относящимся к разработке проекта, конкретной продукции и процессу). 3. Риск часто характеризуют путем описания возможного события и его последствий или их сочетания. 4. Риск часто представляют в терминах комбинации последствий возможного события (включая изменения обстоятельств) и соответствующей вероятности наступления этого события. 5. Неопределенность — состояние хотя бы частичной неполноценности информации, необходимой для понимания или познания события, его последствий и вероятности наступления этого события³.

Риск (Risk) — потенциальная возможность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей активов или группы активов организаций. **Примечание.** Риск измеряется в терминах сочетания вероятности события и его последствий⁴.

¹ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2017). Пункт 3 — извлечение.

² Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

Родственники — все иные лица, за исключением близких родственников, состоящие в родстве¹.

Розыскные меры — меры, принимаемые дознавателем, следователем, а также органом дознания по поручению дознавателя или следователя для установления лица, подозреваемого в совершении преступления².

Роль защиты информации — заранее определенная совокупность функций и задач субъекта доступа, в том числе работника финансовой организации, связанных с применением организационных и (или) технических мер защиты информации³.

Роль логического доступа (роль) — заранее определенная совокупность функций и задач субъекта доступа, для выполнения которых необходим определенный набор прав логического доступа⁴.

Российская организация — юридическое лицо, образованное в соответствии с законодательством Российской Федерации и осуществляющее в качестве основного или дополнительного вида деятельности деятельность по разработке компьютерного программного обеспечения, оказанию консультационных услуг в этой области, а также в сфере информационных технологий в соответствии с Общероссийским классификатором видов экономической деятельности⁵.

Руководитель следственного органа — должностное лицо, возглавляющее соответствующее следственное подразделение, а также его заместитель⁶.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Там же.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2017). Пункт 3 — извлечение.

⁴ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2017). Пункт 3 — извлечение.

⁵ Пункт 2 Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции, утвержденных постановлением Правительства РФ от 30 апреля 2019 г. № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции». Извлечение.

⁶ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

С

Сайт в сети «Интернет» — совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет») по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»¹.

Сайт Координатора — официальный сайт Координатора в сети Интернет, расположенный по адресу <http://cctld.ru> или <http://кц.рф>².

Санкционированный доступ к информации (Authorized access to information) — доступ к информации, не нарушающий правила разграничения доступа³.

Сбор — обязательный взнос, взимаемый с организаций и физических лиц, уплата которого является одним из условий совершения в отношении плательщиков сборов государственными органами, органами местного самоуправления, иными уполномоченными органами и должностными лицами юридически значимых действий, включая предоставление определенных прав или выдачу разрешений (лицензий)⁴.

Свидетельский иммунитет — право лица не давать показания против себя и своих близких родственников, а также в иных случаях, предусмотренных УПК РФ⁵.

Свод правил — документ в области стандартизации, в котором содержатся технические правила и (или) описание процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации продукции и который применяется на добровольной основе в целях соблюдения требований технических регламентов⁶.

¹ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

² Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

³ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁴ Налоговый кодекс Российской Федерации (часть первая) от 31 июля 1998 г. № 146-ФЗ. Статья 8 — извлечение.

⁵ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁶ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

Свод правил иностранного государства — свод правил, принятый компетентным органом иностранного государства¹.

Сводная бюджетная роспись — документ, который составляется и ведется финансовым органом (органом управления государственным внебюджетным фондом) в соответствии с Бюджетным кодексом Российской Федерации в целях организации исполнения бюджета по расходам бюджета и источникам финансирования дефицита бюджета².

Секрет производства (информация, составляющая коммерческую тайну) — сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны³.

Семейство ЭВМ — группа ЭВМ, представляющих параметрический ряд, имеющих единую архитектуру и, в большинстве случаев, одинаковую конструктивно-технологическую базу и характеризующихся полной или ограниченной некоторыми условиями программной совместимостью⁴.

Сервер DNS — программно-аппаратный комплекс, обеспечивающий трансляцию доменных имен в сетевые адреса (IP-адреса)⁵.

Серверные компоненты виртуализации — совокупность гипервизора, технических средств, необходимых для функционирования гипервизора, технических средств, предназначенных для управления

¹ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

² Приказ Минкомсвязи России от 30 декабря 2016 г. № 745 «Об утверждении рекомендаций по согласованию с Министерством связи и массовых коммуникаций Российской Федерации предлагаемых главными распорядителями средств федерального бюджета изменений в сводную бюджетную роспись федерального бюджета и лимиты бюджетных обязательств по бюджетным ассигнованиям, предусмотренным на закупку товаров, работ, услуг в сфере информационно-коммуникационных технологий». Пункт 2 Рекомендаций — извлечение.

³ Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне». Статья 3 — извлечение.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

и администрирования гипервизора, ПО, предназначенного для предоставления доступа к виртуальным машинам с АРМ пользователей (например, брокер соединений)¹.

Сервисные подсистемы — информационные системы, реализующие прикладные функции информационно-технологической поддержки решения задач, указанных в пункте 4 настоящего Положения²,

¹ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2017). Пункт 3 — извлечение.

² Примечание. Задачи, указанные в п. 4 Положения:

а) учет мероприятий по созданию, развитию, модернизации, эксплуатации информационных систем и компонентов информационно-коммуникационной инфраструктуры, осуществляемых ФОИВ и органами управления государственными внебюджетными фондами (далее — мероприятия по информатизации), и мониторинг хода реализации мероприятий по информатизации;

б) планирование и обеспечение проектного управления реализацией ФОИВ и органами управления государственными внебюджетными фондами мероприятий по информатизации;

в) информационно-аналитическое и методическое обеспечение субъектов системы координации, в том числе в части мониторинга соблюдения требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства РФ от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

г) обеспечение проведения Министерством связи и массовых коммуникаций Российской Федерации оценки мероприятий по информатизации и планов информатизации в соответствии с постановлением Правительства РФ от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов»;

д) осуществление контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» к размещению технических средств информационных систем, используемых субъектами системы координации, и требований, указанных в подпункте «в» настоящего пункта;

е) планирование и реализация мероприятий по информатизации в отношении информационных систем и компонентов информационно-коммуникационной инфраструктуры, информация о которых размещена в системе координации, а также обеспечение согласованного взаимодействия участников планирования;

ж) мониторинг и анализ эффективности и результативности создания, развития и эксплуатации ФОИВ и органами управления государственными внебюджетными фондами информационных систем и компонентов информационно-коммуникационной инфраструктуры на всех этапах их существования;

з) сбор, обработка и хранение разработанных государственными органами, органами управления государственными внебюджетными фондами и органами МСУ

включая информационную систему управления ведомственной и региональной информатизацией, информационную систему «Электронный регион», федеральную государственную информационную систему национального фонда алгоритмов и программ для электронных вычислительных машин, федеральную государственную информационную систему учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов¹.

Сертификат защиты (Protection certificate) — документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных².

Сертификат ключа проверки электронной подписи — электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи³.

Сертификат соответствия — документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров⁴.

в результате создания и развития информационных систем алгоритмов и (или) программ для ЭВМ в национальный фонд алгоритмов и программ для ЭВМ;

и) обеспечение предоставления субъектам системы координации содержащихся в национальном фонде алгоритмов и (или) программ для ЭВМ для использования при внедрении информационных технологий в их деятельность;

к) обработка и анализ сведений об уровне информатизации ФОИВ, исполнительной власти субъектов РФ и органов МСУ;

л) осуществление контроля за выполнением субъектами РФ обязательств, предусмотренных соглашением о предоставлении субсидий на реализацию проектов, направленных на становление информационного общества в субъектах РФ, а также за соблюдением субъектами РФ условий предоставления указанных субсидий;

м) мониторинг выполнения проектов в сфере информатизации в субъектах РФ;

н) распространение общедоступной информации, содержащейся в системе координации, в том числе в форме открытых данных.

¹ Постановление Правительства РФ от 14 ноября 2015 г. № 1235 «О федеральной государственной информационной системе координации информатизации» (вместе с «Положением о федеральной государственной информационной системе координации информатизации»). Пункт 14 части III Положения — извлечение.

² Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

³ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

⁴ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

Сертификат квалифицированный ключа проверки электронной подписи (далее — **квалифицированный сертификат**) — сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее — **уполномоченный федеральный орган**)¹.

Сертификация — форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров².

Сертификация уровня защиты (Protection level certification) — процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите³.

Сетевая атака — компьютерная атака с использованием протоколов межсетевого взаимодействия⁴.

Сетевое издание — сайт в информационно-телекоммуникационной сети «Интернет», зарегистрированный в качестве средства массовой информации в соответствии с настоящим Законом⁵.

Сетевой адрес — идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему⁶.

Сети связи нового поколения — технологические системы, предназначенные для подключения к сети «Интернет» пятого поколения в целях использования в устройствах интернета вещей и индустриального интернета⁷.

¹ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

² Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

³ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁴ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение.

⁵ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации».

⁶ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁷ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

Сеть связи — технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи¹.

Силы обеспечения информационной безопасности — государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности².

Силы обеспечения национальной безопасности — Вооруженные Силы Российской Федерации, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба, а также федеральные органы государственной власти, принимающие участие в обеспечении национальной безопасности государства на основании законодательства Российской Федерации³.

Система — совокупность элементов, объединенная связями между ними и обладающая определенной целостностью⁴.

Система (System) — комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей. **Примечания.** 1. Система может рассматриваться как какой-то продукт или как предоставляемые услуги, обеспечивающие этот продукт. 2. На практике, интерпретация данного термина зачастую уточняется с помощью ассоциативного существительного, например система самолета. В некоторых случаях слово система может заменяться контекстно зависимым синонимом, например самолет, хотя это может впоследствии затруднить восприятие системных принципов⁵.

Система взаимодействия — система взаимодействия представляет собой федеральную государственную информационную систему,

¹ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

² Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

³ Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». Пункт 6.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Приложение 1 — извлечение.

⁵ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

включающую информационные базы данных, в том числе содержащие сведения об используемых органами и организациями программных и технических средствах, обеспечивающих возможность доступа через систему взаимодействия к их информационным системам (далее — электронные сервисы); о программных и технических средствах, обеспечивающих единый документированный способ взаимодействия информационных систем органов и организаций посредством технологии очередей электронных сообщений, обеспечивающей взаимодействие программ в асинхронном режиме, не требующей установки между ними прямой связи и гарантирующей получение передаваемых электронных сообщений (далее — единый электронный сервис); об истории движения в системе взаимодействия электронных сообщений; а также программные и технические средства, обеспечивающие взаимодействие, позволяющие осуществлять мониторинг системы взаимодействия; соблюдения процедур, предусмотренных техническими требованиями к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия; предоставлять информационно-методическую поддержку органам и организациям в части использования ими системы взаимодействия, иных информационных систем, включенных в инфраструктуру, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме и подключенных к системе взаимодействия¹.

Система государственной статистики — государственная федеральная информационная статистическая система, представляющая собой совокупность позволяющих осуществлять официальный статистический учет первичных статистических данных и административных данных, формируемой на их основе в соответствии с официальной статистической методологией официальной статистической информации и обеспечивающих формирование такой информации информационных технологий и технических средств².

¹ Постановление Правительства РФ от 19 ноября 2014 г. № 1222 (ред. от 28.03.2017) «О дальнейшем развитии единой системы межведомственного электронного взаимодействия». Пункт 2 — извлечение.

² Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Статья 2 — извлечение.

Система защиты государственной тайны — совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях¹.

Система защиты информации — совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации².

Система защиты информации — совокупность мер защиты информации, применение которых направлено на непосредственное обеспечение защиты информации, процессов применения указанных мер защиты информации, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты информации³.

Система защиты информации от несанкционированного доступа (System of protection from unauthorized access to information) — комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах⁴.

Система защиты секретной информации (Secret information security system) — комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах⁵.

Система как объект оценки (System target of evaluation) — автоматизированная система, которая эксплуатируется в соответствии с рекомендациями по эксплуатации, включая технические и организа-

¹ Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне». Статья 2 — извлечение.

² ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2017). Пункт 3 — извлечение.

⁴ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁵ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

ционные меры обеспечения безопасности, и является предметом оценки. **Примечание.** Организационные меры обеспечения безопасности образуют часть эксплуатационной среды. Они не оцениваются по критериям оценки в соответствии со стандартами серии ИСО/МЭК 15408¹.

Система локальной автоматики — функцию управления технологическим объектом управления или его частью, либо функцию система устройств автоматики, автономно реализующая АС управления технологическим процессом контроля за ТОУ или его частью².

Система межведомственного электронного документооборота — федеральная информационная система, обеспечивающая в автоматизированном режиме защищенный обмен электронными сообщениями, в том числе сообщениями, содержащими информацию, отнесенную к сведениям, составляющим служебную тайну, между Администрацией Президента Российской Федерации, Аппаратом Правительства Российской Федерации и федеральными органами исполнительной власти, а также иными федеральными органами государственной власти³.

Система менеджмента информационной безопасности (Information security management system) — часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности. **Примечание.** Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы⁴.

¹ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Распоряжение Правительства РФ от 2 октября 2009 г. № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти». Извлечение.

⁴ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

Система обеспечения информационной безопасности — совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности¹.

Система обеспечения национальной безопасности — силы и средства обеспечения национальной безопасности².

Система обеспечения национальной безопасности — совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов государственной власти и органов местного самоуправления и находящихся в их распоряжении инструментов³.

Система обработки информации — совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации⁴.

Система организации и управления защитой информации — совокупность мер защиты информации, применение которых направлено на обеспечение полноты и качества защиты информации, предназначенных для планирования, реализации, контроля и совершенствования процессов системы защиты информации⁵.

Система разграничения доступа (Security policy realization) — совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах⁶.

¹ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

² Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». Пункт 6.

³ Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». Раздел 1, пункт 6 — извлечение.

⁴ ГОСТ Р 51275-2006 «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст). Пункт 3 — извлечение. ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁶ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

Система сертификации — совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом; стандарт — документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать правила и методы исследований (испытаний) и измерений, правила отбора образцов, требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения¹.

Система хранения данных виртуализации (система хранения данных) — совокупность технических средств, предназначенных для хранения данных, используемых при реализации виртуализации, в том числе образов виртуальных машин и данных, обрабатываемых виртуальными машинами².

Система эксплуатации — совокупность изделий, средств эксплуатации, исполнителей и устанавливающей правила их взаимодействия документации, необходимых и достаточных для выполнения задач эксплуатации. Составной частью системы эксплуатации является система технического обслуживания и ремонта техники³.

Система электронного документооборота — система автоматизации делопроизводства и документооборота в федеральном органе исполнительной власти, обеспечивающая возможности внутреннего электронного документооборота⁴.

Систематизация информации — упорядочивание объектов систематизации по сходству или различию присущих им признаков, в резуль-

¹ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

² ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

³ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁴ Распоряжение Правительства РФ от 2 октября 2009 г. № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти». Извлечение.

тате которого осуществляется формирование и ведение информационного ресурса¹.

Системная инженерия (Systems engineering) — междисциплинарный подход, управляющий полным техническим и организаторским усилием, требуемым для преобразования ряда потребностей заинтересованных сторон, ожиданий и ограничений в решение и для поддержки этого решения в течение его жизни².

Системный элемент (System element) — представитель совокупности элементов, образующих систему. **Пример.** Системный элемент может представлять собой технические и программные средства, данные, людей, процессы (например, процессы для обеспечения услуг пользователям), процедуры (например, инструкции оператору), средства, материалы и природные объекты (например, вода, живые организмы, минералы) или любые их сочетания. **Примечание.** Системный элемент является отдельной частью системы, которая может быть создана для полного выполнения заданных требований³.

«Сквозная» цифровая технология — часть технологического процесса производства товаров, оказания услуг и выполнения работ, представляющая собой совокупность процессов и методов поиска, сбора, хранения, обработки, предоставления и распространения информации, обеспечивающих в ходе хозяйственной деятельности по производству (поставке) товаров, оказанию услуг и выполнению работ: повышение результативности, точности или иных значимых характеристик технологического процесса; повышение качества или иных значимых характеристик производимых (поставляемых) товаров, оказываемых услуг и выполняемых работ (в том числе за счет сокращения брака); снижение издержек при производстве (поставке) товаров, оказании услуг и выполнении работ⁴.

¹ Проект в редакции от 4 июля 2018 г. Федерального закона «О систематизации и гармонизации информации в Российской Федерации». Статья 2 — извлечение.

² ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Пункт 2 Правил предоставления субсидий из федерального бюджета на государственную поддержку программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий, утвержденных постановлением правительства РФ от 3 мая 2019 г. № 551. Извлечение.

Сквозные технологии — технологии, которые примеряются во всех отраслях, это цифровые, квантовые, робототехника, нейротехнологии и так далее¹.

Смарт-контракт — договор в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых транзакций в распределенном реестре цифровых транзакций в строго определенной таким договором последовательности и при наступлении определенных им обстоятельств².

Следователь — должностное лицо, уполномоченное осуществлять предварительное следствие по уголовному делу, а также иные полномочия, предусмотренные УПК РФ³.

Следователь-криминалист — должностное лицо, уполномоченное осуществлять предварительное следствие по уголовному делу, а также участвовать по поручению руководителя следственного органа в производстве отдельных следственных и иных процессуальных действий или производить отдельные следственные и иные процессуальные действия без принятия уголовного дела к своему производству⁴.

Снятие с эксплуатации — событие, фиксирующее невозможность или нецелесообразность дальнейшего использования по назначению и ремонта изделия и документально оформленное в установленном порядке⁵.

Снятие с эксплуатации (выведение из эксплуатации), списание (Retirement) — прекращение активной поддержки эксплуатирующей и сопровождающей организацией, частичная или полная замена новой системой или инсталляция обновленной системы⁶.

Событие информационной безопасности (Information security event) — идентифицированное возникновение состояния системы, услуги

¹ Послание Президента Российской Федерации Федеральному Собранию от 1 декабря 2016 г.

² Статья 2 Федерального закона «О цифровых финансовых активах». Проект № 419059-7.

³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁵ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁶ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью¹.

Совместимость автоматизированных систем — комплексное свойство двух или более АС, характеризующее их способностью взаимодействовать при функционировании. Примечание. Совместимость АС включает техническую, программную, информационную, организационную, лингвистическую и, при необходимости, метрологическую совместимость².

Совместный конкурс — конкурс, который проводится в порядке, установленном настоящим Федеральным законом, двумя и более публичными партнерами в целях реализации проекта и по итогам которого каждый публичный партнер заключает соглашение с победителем совместного конкурса или иным лицом, имеющим право в соответствии с настоящим Федеральным законом на заключение такого соглашения³.

Совокупный годовой объем закупок — утвержденный на соответствующий финансовый год общий объем финансового обеспечения для осуществления заказчиком закупок в соответствии с настоящим Федеральным законом, в том числе для оплаты контрактов, заключенных до начала указанного финансового года и подлежащих оплате в указанном финансовом году⁴.

Современный функциональный эквивалент сети связи — минимальный набор современных средств связи, обеспечивающий качество и существующий объем услуг, оказываемых в сети связи⁵.

Согласие — разрешение руководителя следственного органа на производство следователем или разрешение прокурора на произ-

¹ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

⁴ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

⁵ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

водство дознавателем соответствующих следственных и иных процессуальных действий и на принятие ими процессуальных решений¹.

Соглашение (Agreement) — взаимное признание сроков и условий, в соответствии с которыми осуществляются рабочие отношения.

Пример. Контракт, меморандум о соглашении².

Соглашение о государственно-частном партнерстве, соглашение о муниципально-частном партнерстве (далее также — соглашение) — гражданско-правовой договор между публичным партнером и частным партнером, заключенный на срок не менее чем три года в порядке и на условиях, которые установлены настоящим Федеральным законом³.

Содержание под стражей — пребывание лица, задержанного по подозрению в совершении преступления, либо обвиняемого, к которому применена мера пресечения в виде заключения под стражу, в следственном изоляторе либо ином месте, определяемом федеральным законом⁴.

Соискатель лицензии — юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии⁵.

Соисполнитель — соисполнитель комплексной программы, комплексного проекта, являющийся федеральным органом исполнительной власти и (или) иным главным распорядителем средств федерального бюджета, отвечающим за реализацию комплексной программы, комплексного проекта и достижение их целевых показателей⁶.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

³ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁵ Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». Статья 3 — извлечение.

⁶ Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

- Сообщение автоматизированной системы** — сведения в виде законченного блока данных, передаваемые при функционировании АС¹.
- Сообщение о преступлении** — заявление о преступлении, явка с повинной, рапорт об обнаружении преступления².
- Сооружения связи** — объекты инженерной инфраструктуры (в том числе линейно-кабельные сооружения связи), созданные или приспособленные для размещения средств связи, кабелей связи³.
- Сопровождение автоматизированной системы** — деятельность по оказанию услуг, необходимых для обеспечения устойчивого функционирования или развития АС⁴.
- Составная функция автоматизированной системы управления технологическим процессом** — совокупность двух или более простых функций АС управления технологическим процессом. **Примечания.** 1. Простые функции объединяются по общности цели, роли в процессе управления, используемой информации и другим признакам. 2. Совокупность всех функций АСУТП можно рассматривать как одну составную функцию⁵.
- Специализированная организация** — юридическое лицо, привлекаемое заказчиком в соответствии со статьей 40 настоящего Федерального закона⁶.
- Специализированная ЭВМ** — ЭВМ, имеющая функциональные возможности и конструктивные особенности, позволяющие использовать ее для эффективного решения ограниченного класса задач в определенных условиях окружающей среды⁷.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

³ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

⁷ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

- Специализированная электронная площадка** — соответствующая установленным в соответствии с пунктами 1 и 3 части 2 статьи 24.1 настоящего Федерального закона требованиям информационная система, доступ к которой осуществляется с использованием защищенных каналов связи и на которой проводятся закрытые конкурентные способы определения поставщиков (подрядчиков, исполнителей) в электронной форме¹.
- Специальное программное обеспечение автоматизированной системы** — часть программного обеспечения, представляющая собой совокупность программ, разработанных при создании данной АС².
- Специальное регулирование** — нормативное правовое регулирование, установленное в соответствии с настоящим Федеральным законом программой экспериментального правового режима, отличающееся от общего регулирования и устанавливаемое в случаях, предусмотренных иными федеральными законами, в отношении определенного круга лиц — участников экспериментального правового режима на срок действия экспериментального правового режима и, если иное не предусмотрено экспериментальным правовым режимом, на определенной территории³.
- Специализированное средство массовой информации** — средство массовой информации, для регистрации или распространения продукции которого настоящим Законом⁴ установлены специальные правила⁵.
- Специализированное учреждение для несовершеннолетних** — специализированный государственный орган, обеспечивающий исправление несовершеннолетних и созданный в соответствии с федеральным законом⁶.
- Специализированные технические средства оповещения и информирования населения в местах массового пребывания людей** — специально созданные технические устройства, осуществляющие прием, об-

¹ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

⁴ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации».

⁵ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

⁶ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

работку и передачу аудио- и (или) аудиовизуальных, а также иных сообщений об угрозе возникновения, о возникновении чрезвычайных ситуаций и правилах поведения населения¹.

Специальная проверка — проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств².

Специальное исследование объекта защиты информации — исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации³.

Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации⁴.

Сравнительное преимущество — преимущество в использовании средств бюджетов бюджетной системы Российской Федерации, необходимых для реализации проекта, перед использованием средств бюджетов бюджетной системы Российской Федерации, необходимых для реализации государственного контракта, муниципального контракта, при условии, что цена товара, работы, услуги, количество товара, объем работы или услуги, качество поставляемого товара, выполняемой работы, оказываемой услуги, иные характеристики товара, работы, услуги при реализации проекта равны цене товара, работы, услуги, количеству товара, объему работы или услуги, качеству поставляемого товара, выполняемой работы, оказываемой услуги, иным характеристикам товара, работы, услуги при реализации государственного контракта, муниципального контракта⁵.

Средства доверенной третьей стороны — программные и (или) аппаратные средства, используемые для оказания услуг доверенной третьей стороной, прошедшие процедуру подтверждения соответ-

¹ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

² ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

³ Там же.

⁴ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁵ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

ствия требованиям, установленным в соответствии с настоящим Федеральным законом¹.

Средства защиты информации — технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации².

Средства контроля — программное обеспечение или аппаратные средства, которые контролируют поведение системы или процессы, происходящие в устройстве. Они включают в себя антивирусные продукты, конечные продукты обеспечения безопасности, продукты обеспечения персональной безопасности, системы обнаружения взлома, системы предотвращения взлома либо аппаратные или программные средства межсетевой защиты³.

Средства обеспечения информационной безопасности — правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности⁴.

Средства обеспечения национальной безопасности — технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая телекоммуникационные каналы, используемые в системе обеспечения национальной безопасности для сбора, формирования, обработки, передачи или приема информации о состоянии национальной безопасности и мерах по ее укреплению⁵.

Средства связи — технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей

¹ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2, пункт 18 — извлечение.

² Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне». Статья 2 — извлечение.

³ В соответствии с Указом Президента РФ от 21 июля 2014 г. № 519 «О внесении изменений в Список товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль, утвержденный Указом Президента Российской Федерации от 17 декабря 2011 г. № 1661» — извлечение (пункт 87.1).

⁴ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

⁵ Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». Пункт 6.

связи, включая технические системы и устройства с измерительными функциями¹.

Средства удостоверяющего центра — программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра².

Средства эксплуатации — здания, сооружения, технические устройства, в том числе инструмент, запасные части и эксплуатационные материалы, необходимые для эксплуатации изделия. К техническим устройствам относят машины, приборы, приспособления и т.п.³

Средства электронной подписи — шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций — создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи⁴.

Средство защиты информации — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации⁵.

Средство защиты от несанкционированного доступа (Protection facility) — программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа⁶.

Средство контроля эффективности защиты информации — средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации⁷.

Средство коллективного доступа — окончное оборудование, предназначенное для предоставления неограниченному кругу лиц воз-

¹ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

² Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

³ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁴ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

⁵ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁶ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁷ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

возможности пользования услугами связи с использованием пользовательского оборудования абонента или без него¹.

Средство криптографической защиты информации (Cryptographic information protection facility) — средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности².

Средство массовой информации — периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа³, иная форма периодического распространения массовой информации под постоянным наименованием (названием)⁴.

Средство физической защиты информации — средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации⁵.

Стадия создания автоматизированной системы — одна из частей процесса создания АС, установленная нормативными документами и заканчивающаяся выпуском документации на АС, содержащей описание полной, в рамках заданных требований, модели АС на заданном для данной стадии уровне, или изготовлением несерийных компонентов АС, или приемкой АС в промышленную эксплуатацию⁶.

Стандарт иностранного государства — стандарт, принятый национальным (компетентным) органом (организацией) по стандартизации иностранного государства⁷.

¹ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

² Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

³ Под радио-, теле-, видео-, кинохроникальной программой понимается совокупность периодических аудио-, аудиовизуальных сообщений и материалов (передач), имеющая постоянное наименование (название) и выходящая в свет (в эфир) не реже одного раза в год. Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

⁴ Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

⁵ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁶ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁷ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

Стандартизация — деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг¹.

Стадия (Stage) — период в пределах жизненного цикла некоторой сущности, который относится к состоянию ее описания или реализации. **Примечания.** 1. В настоящем стандарте принято, что стадии относятся к основному развитию и достижению контрольных точек в течение жизненного цикла этой сущности. 2. Стадии могут быть взаимно перекрывающимися².

Статический анализ исходных текстов программ — совокупность методов контроля (не) соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных текстов программ³.

Степень опасности уязвимости — мера (сравнительная величина), характеризующая подверженность информационной системы уязвимости и ее влияние на нарушение свойств безопасности информации (конфиденциальность, целостность, доступность)⁴.

Стоп-лист — перечень символьных обозначений, регистрация которых в качестве доменных имен недоступна⁵.

Сторона (Party) — организация, вовлеченная в соглашение. **Примечание.** В настоящем стандарте стороны, входящие в соглашение, называются приобретающей стороной и поставщиком⁶.

¹ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

² ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

³ Руководящий документ. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» Утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114. Пункт 2 — извлечение.

⁴ ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение.

⁵ Правила регистрации доменных имен в доменах .RU и .RF (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

⁶ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

Стороны — участники уголовного судопроизводства, выполняющие на основе состязательности функцию обвинения (уголовного преследования) или защиты от обвинения¹.

Сторона защиты — обвиняемый, а также его законный представитель, защитник, гражданский ответчик, его законный представитель и представитель².

Сторона обвинения — прокурор, а также следователь, руководитель следственного органа, дознаватель, частный обвинитель, потерпевший, его законный представитель и представитель, гражданский истец и его представитель³.

Страница сайта в сети «Интернет» (далее также — интернет-страница) — часть сайта в сети «Интернет», доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет»⁴.

Стратегические национальные приоритеты — важнейшие направления обеспечения национальной безопасности, по которым реализуются конституционные права и свободы граждан Российской Федерации, осуществляются устойчивое социально-экономическое развитие и охрана суверенитета страны, ее независимости и территориальной целостности⁵.

Стратегические национальные приоритеты Российской Федерации — важнейшие направления обеспечения национальной безопасности⁶.

Структура архитектуры (Architecture framework) — условности, принципы и практики для описания архитектур, установленные в пределах заданной области применения и/или объединения заинтересованных сторон. **Примеры.** 1. Обобщенная стандартная архитектура предприятия и методологии (GERAM) [ГОСТ Р ИСО 15704-2008] является некоторой структурой архитектуры. 2. Эталонная модель открытой распределенной обработки (RM-ODP) [ГОСТ Р ИСО/МЭК 10746] является некоторой структурой архитектуры⁷.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Там же.

³ Там же.

⁴ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

⁵ Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». Пункт 6.

⁶ Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». Раздел I, пункт 6 — извлечение.

⁷ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

Структура информационного ресурса — совокупность сведений о составе информации, образующей информационный ресурс, множественности представлений объекта систематизации в информационном ресурсе, областях значений и правилах формирования информации в информационном ресурсе¹.

Субъект доступа (Access subject) — лицо или процесс, действия которого регламентируются правилами разграничения доступа².

Субъект доступа — работник финансовой организации или иное лицо, осуществляющий физический и (или) логический доступ, или программный сервис, осуществляющий логический доступ. **Примечание.** В составе основных типов субъектов доступа в настоящем стандарте как минимум рассматриваются следующие:

- пользователи — субъекты доступа, в том числе клиенты финансовой организации, осуществляющие доступ к объектам и (или) ресурсам доступа с целью использования финансовых услуг, предоставляемых информационной инфраструктурой финансовой организации;
- эксплуатационный персонал — субъекты доступа, в том числе представители подрядных организаций, которые решают задачи обеспечения эксплуатации и (или) администрирования объектов и (или) ресурсов доступа, для которых необходимо осуществление логического доступа, включая задачи, связанные с эксплуатацией и администрированием технических мер защиты информации;
- технический (вспомогательный) персонал — субъекты доступа, в том числе представители подрядных организаций, решающие задачи, связанные с обеспечением эксплуатации объектов доступа, для выполнения которых не требуется осуществление логического доступа, или выполняющие хозяйственную деятельность и осуществляющие физический доступ к объектам доступа без цели их непосредственного использования;
- программные сервисы — процессы выполнения программ в информационной инфраструктуре, осуществляющие логический доступ к ресурсам доступа³.

¹ Проект в редакции от 4 июля 2018 г. Федерального закона «О систематизации и гармонизации информации в Российской Федерации». Статья 2 — извлечение.

² Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

Субъект экспериментального правового режима — государственный орган или орган местного самоуправления (по направлению, предусмотренному пунктом 7 части 2 статьи 1 настоящего Федерального закона), юридическое лицо, индивидуальный предприниматель, осуществляющие деятельность в соответствии с программой экспериментального правового режима¹.

Субъекты деятельности в сфере промышленности — юридические лица, индивидуальные предприниматели, осуществляющие деятельность в сфере промышленности на территории Российской Федерации, на континентальном шельфе Российской Федерации, в исключительной экономической зоне Российской Федерации².

Субъекты критической информационной инфраструктуры — государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей³.

Субъекты официального статистического учета — федеральные органы государственной власти, иные федеральные государственные органы, Центральный банк Российской Федерации (Банк России), осуществляющие формирование официальной статистической информации в установленной сфере деятельности в соответствии с законодательством Российской Федерации⁴.

¹ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

² Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

³ Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Статья 2 — извлечение.

⁴ Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Статья 2 — извлечение.

- Суд** — любой суд общей юрисдикции, рассматривающий уголовное дело по существу и выносящий решения, предусмотренные УПК РФ¹.
- Суд первой инстанции** — суд, рассматривающий уголовное дело по существу и правомочный выносить приговор, а также принимать решения в ходе досудебного производства по уголовному делу².
- Суд второй инстанции** — суд апелляционной инстанции³.
- Судебная экспертиза** — экспертиза, производимая в порядке, установленном УПК РФ⁴.
- Судебное заседание** — процессуальная форма осуществления правосудия в ходе досудебного и судебного производства по уголовному делу⁵.
- Судебное разбирательство** — судебное заседание судов первой, второй, кассационной и надзорной инстанций⁶.
- Судебное решение** — приговор, определение, постановление, вынесенные при производстве по уголовному делу в судах первой и второй инстанций; определение и постановление, вынесенные при производстве по уголовному делу в суде кассационной инстанции; постановление, вынесенное при производстве по уголовному делу в суде надзорной инстанции⁷.
- Судебное решение итоговое** — приговор, иное решение суда, вынесенное в ходе судебного разбирательства, которым уголовное дело разбирается по существу⁸.
- Судебное решение промежуточное** — все определения и постановления суда, за исключением итогового судебного решения⁹.
- Судья** — должностное лицо, уполномоченное осуществлять правосудие¹⁰.
- Супер-ЭВМ** — ЭВМ, относящаяся к классу вычислительных машин, имеющих самую высокую производительность, которая может быть достигнута на данном этапе развития технологии и в основном предназначенных для решения сложных научно-технических задач¹¹.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Там же.

³ Там же.

⁴ Там же.

⁵ Там же.

⁶ Там же.

⁷ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁸ Там же.

⁹ Там же.

¹⁰ Там же.

¹¹ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

Существующие компоненты — система электронного документооборота, система межведомственного электронного документооборота¹.

Схема классификации деловых операций (Business classification scheme) — инструмент для связи документов с контекстом их создания².

Схема метаданных (Schema) — логический план, показывающий отношения между элементами метаданных, как правило, посредством установления правил использования и управления метаданными, особенно касающихся семантики, синтаксиса и степени обязательности данных³.

Схема подтверждения соответствия — перечень действий участников подтверждения соответствия, результаты которых рассматриваются ими в качестве доказательств соответствия продукции и иных объектов установленным требованиям⁴.

Т

Текущий образ виртуальной машины — образ виртуальной машины в определенный (текущий) момент времени ее функционирования⁵.

Текущий финансовый год — год, в котором осуществляется исполнение бюджета, составление и рассмотрение проекта бюджета на очередной финансовый год (очередной финансовый год и плановый период)⁶.

¹ Распоряжение Правительства РФ от 2 октября 2009 г. № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти». Извлечение.

² ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

³ Там же.

⁴ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

⁵ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁶ Приказ Минкомсвязи России от 30 декабря 2016 г. № 745 «Об утверждении рекомендаций по согласованию с Министерством связи и массовых коммуникаций Российской Федерации предлагаемых главными распорядителями средств федерального бюджета изменений в сводную бюджетную роспись федерального бюджета

Телеканал, радиоканал — сформированная в соответствии с сеткой вещания и выходящая в свет (эфир) под постоянным наименованием и с установленной периодичностью совокупность теле-, радиопрограмм и (или) соответственно иных аудиовизуальных, звуковых сообщений и материалов¹.

Территория, подверженная риску возникновения быстроразвивающихся опасных природных явлений и техногенных процессов — участок земельного, водного или воздушного пространства либо критически важный или потенциально опасный объект производственного и социального значения, отнесенные к указанной территории путем прогнозирования угрозы возникновения чрезвычайных ситуаций и оценки социально-экономических последствий чрезвычайных ситуаций².

Техника защиты информации — средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации³.

Технический центр — юридическое лицо, уполномоченное Координатором для оказания услуг доступа к Реестрам доменных имен в доменах верхнего уровня, администрирование которых осуществляет Координатор⁴.

Технологически независимые программное обеспечение и сервис — программное обеспечение и сервис, которые могут быть использованы на всей территории Российской Федерации, обеспечены гарантийной и технической поддержкой российских организаций, не имеют принудительного обновления и управления из-за рубежа, модернизация которых осуществляется российскими организациями на территории Российской Федерации и которые не осуществ-

и лимиты бюджетных обязательств по бюджетным ассигнованиям, предусмотренным на закупку товаров, работ, услуг в сфере информационно-коммуникационных технологий». Пункт 2 Рекомендаций — извлечение.

¹ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение; Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Статья 2 — извлечение.

² Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

³ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁴ Правила регистрации доменных имен в доменах .RU и .RF (утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81). Подпункт 1.1 — извлечение.

вляют несанкционированную передачу информации, в том числе технологической¹.

Техническая защита информации — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств².

Техническая мера защиты информации — мера защиты информации, реализуемая с помощью применения аппаратных, программных, аппаратно-программных средств и (или) систем³.

Техническая совместимость автоматизированных систем — частная совместимость АС, характеризующаяся возможностью взаимодействия технических средств этих систем⁴.

Техническая учетная запись — учетная запись, используемая для осуществления логического доступа программными сервисами⁵.

Техническая эксплуатация — часть эксплуатации, включающая транспортирование, хранение, техническое обслуживание и ремонт изделия⁶.

Технические меры безопасности (Technical controls) — меры безопасности информационной системы, которые реализуются и выполняются самой информационной системой через механизмы, содер-

¹ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

² ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁵ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁶ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

жащиеся в аппаратных, программных или программно-аппаратных компонентах системы¹.

Технический проект автоматизированной системы — комплект проектных документов на АС, разрабатываемый на стадии «Технический проект», утвержденный в установленном порядке, содержащий основные проектные решения по системе в целом, ее функциям и всем видам обеспечения АС и достаточный для разработки рабочей документации на АС².

Технический регламент — документ, который принят международным договором Российской Федерации, подлежащим ратификации в порядке, установленном законодательством Российской Федерации, или в соответствии с международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации)³.

Технические средства системы обработки информации — все оборудование, включая носители данных, предназначенное для автоматизированной обработки информации⁴.

Техническое задание на автоматизированную систему — документ, оформленный в установленном порядке и определяющий цели создания АС, требования к АС и основные исходные данные,

¹ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

необходимые для ее разработки, а также план-график создания АС¹.

Техническое обеспечение автоматизированной системы — совокупность всех технических средств, используемых при функционировании АС².

Техническое обслуживание — комплекс операций по подготовке изделия к использованию по назначению, хранению и транспортированию, и приведению его в исходное состояние после этих процессов, не связанных с поддержанием надежности изделия³.

Техническое обслуживание — по ГОСТ 18322-78. Технологическое обслуживание является составной частью использования по назначению, транспортирования и хранения. В некоторых случаях технологическое обслуживание может проводиться в процессе использования по назначению, транспортирования и хранения, например очистка ковша экскаватора от налипшего грунта, очистка изделий, хранящихся на открытой площадке, от снега и т.п.⁴

Техническое обслуживание объекта соглашения (далее также — техническое обслуживание) — мероприятия, направленные на поддержание объекта соглашения в исправном, безопасном, пригодном для его эксплуатации состоянии и осуществление его текущего или капитального ремонта⁵.

Техническое регулирование — правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, экс-

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² Там же.

³ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁴ Там же.

⁵ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

плуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия¹.

Техническое средство обработки информации (ТСОИ) — техническое средство, предназначенное для приема, накопления, хранения, поиска, преобразования, отображения и передачи информации по каналам связи².

Технологическая инфраструктура — совокупность объектов недвижимого имущества и оборудования, необходимых для осуществления научно-технической деятельности или инновационной деятельности³.

Технологическая структура организации — иерархический перечень бизнес-процессов организации, увязанных с используемыми технологическими комплексами⁴.

Технологический объект управления — объект управления, включающий технологическое оборудование и реализуемый в нем технологический процесс⁵.

Технологический процесс финансовой организации (технологический процесс) — набор взаимосвязанных операций с информацией и (или) объектами информатизации, используемых при функционировании финансовой организации и (или) необходимых для предоставления финансовых услуг⁶.

¹ Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

² Положение о государственном лицензировании деятельности в области защиты информации (утверждено решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

³ Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

⁴ Пункт 8 Методических рекомендаций по подготовке корпоративных планов импортозамещения государственными корпорациями, государственными компаниями, акционерными обществами, в уставном капитале которых доля участия Российской Федерации превышает 50 процентов, организациями, реализующими инвестиционные проекты, включенные в реестр инвестиционных проектов в соответствии с решением Правительственной комиссии по импортозамещению, утвержденных распоряжением Минэкономразвития России от 11 августа 2016 г. № 219Р-АУ.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии

Технология обработки (передачи) информации в информационной системе (информационная технология) — процесс, метод поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов¹.

Технологический комплекс (производственно-технологический процесс) — совокупность функционально взаимосвязанных средств технологического оснащения, включая технические средства и технологии, необходимых для выполнения производственных процессов или операций².

Технопарк промышленный — объекты промышленной инфраструктуры и технологической инфраструктуры, предназначенные для осуществления субъектами деятельности в сфере промышленности промышленного производства, и (или) научно-технической деятельности, и (или) инновационной деятельности в целях освоения производства промышленной продукции и коммерциализации полученных научно-технических результатов и управляемые управляющей компанией — коммерческой или некоммерческой организацией, созданной в соответствии с законодательством Российской Федерации³.

Технорабочий проект автоматизированной системы — комплект проектных документов АС, утвержденный в установленном порядке и содержащий решения в объеме технического проекта и рабочей документации на АС⁴.

Типовое проектное решение в САПР — проектное решение, предназначенное для повторного использования при проектировании⁵.

от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

¹ ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение.

² Пункт 8 Методических рекомендаций по подготовке корпоративных планов импортозамещения государственными корпорациями, государственными компаниями, акционерными обществами, в уставном капитале которых доля участия Российской Федерации превышает 50 процентов, организациями, реализующими инвестиционные проекты, включенные в реестр инвестиционных проектов в соответствии с решением Правительственной комиссии по импортозамещению, утвержденных распоряжением Минэкономразвития России от 11 августа 2016 г. № 219Р-АУ.

³ Федеральный закон от 31 декабря 2014 г. № 488-ФЗ «О промышленной политике в Российской Федерации». Статья 3 — извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные

Токен — вид цифрового финансового актива, который выпускается юридическим лицом или индивидуальным предпринимателем (далее — эмитент) с целью привлечения финансирования и учитывается в реестре цифровых транзакций¹.

Точка доступа — средство коллективного доступа, предназначенное для предоставления неограниченному кругу лиц возможности пользования услугами связи по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети «Интернет» с использованием пользовательского оборудования абонента².

Точка зрения на архитектуру (Architecture viewpoint) — рабочий продукт, устанавливающий условия конструирования, интерпретации и использования архитектурного представления для структуризации определенных системных интересов³.

Точка обмена трафиком — совокупность технических и программных средств и (или) сооружений связи, с использованием которых собственник или иной их владелец обеспечивает возможность для соединения и пропуска в неизменном виде трафика между сетями связи, если собственник или иной владелец сетей связи имеет уникальный идентификатор совокупности средств связи и иных технических средств в информационно-телекоммуникационной сети «Интернет»⁴.

Транзакция (Transaction) — наименьшая единица рабочего процесса обмена информацией и/или другими ресурсами между двумя или более участниками или системами⁵.

Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу вла-

системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

¹ Статья 2 Федерального закона «О цифровых финансовых активах». Проект № 419059-7.

² Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

³ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁴ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Подпункт 28.5 статьи 2 — извлечение.

⁵ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

сти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу¹.

Трансграничный перевод денежных средств — перевод денежных средств, при осуществлении которого плательщик либо получатель средств находится за пределами Российской Федерации, и (или) перевод денежных средств, при осуществлении которого плательщика или получателя средств обслуживает иностранный центральный (национальный) банк или иностранный банк².

Трансляция телеканалов и (или) радиоканалов — прием и доставка до пользовательского оборудования (оконечного оборудования) сигнала, посредством которого осуществляется распространение телеканалов и (или) радиоканалов, или прием и передача в эфир данного сигнала³.

Транспортирование при эксплуатации — перемещение изделия в заданном состоянии с применением, при необходимости, транспортных и грузоподъемных средств, начинающееся с погрузки и кончающееся разгрузкой на месте назначения⁴.

Трафик — нагрузка, создаваемая потоком вызовов, сообщений и сигналов, поступающих на средства связи⁵.

Требование (Requirement) — утверждение, которое переводит или выражает какую-то потребность и связанные с ней ограничения и условия⁶.

Требование по защите информации — установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации⁷.

¹ Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

² Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

³ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁴ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁵ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁶ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

⁷ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

Трудовая функция — работа по должности в соответствии со штатным расписанием, профессии, специальности с указанием квалификации; конкретный вид поручаемой работнику работы¹.

Трудовая функция — система трудовых действий в рамках обобщенной трудовой функции².

Трудовое действие — процесс взаимодействия работника с предметом труда, при котором достигается определенная задача³.

Туманные вычисления — информационно-технологическая модель системного уровня для расширения облачных функций хранения, вычисления и сетевого взаимодействия, в которой обработка данных осуществляется на конечном оборудовании (компьютеры, мобильные устройства, датчики, смарт-узлы и другое) в сети, а не в «облаке»⁴.

У

Уголовное преследование — процессуальная деятельность, осуществляемая стороной обвинения в целях изобличения подозреваемого, обвиняемого в совершении преступления⁵.

Уголовное судопроизводство — досудебное и судебное производство по уголовному делу⁶.

Уголовный закон — Уголовный кодекс Российской Федерации.

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации⁷.

Угроза информационной безопасности Российской Федерации (далее — информационная угроза) — совокупность действий и факторов, соз-

¹ Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ. Абзац 3 части 2 статьи 57 — извлечение.

² Приказ Минтруда России от 29 апреля 2013 г. № 170н «Об утверждении методических рекомендаций по разработке профессионального стандарта». Пункт 2 — извлечение.

³ Там же.

⁴ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁵ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁶ Там же.

⁷ ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение; ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

дающих опасность нанесения ущерба национальным интересам в информационной сфере¹.

Угроза национальной безопасности — прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства².

Угроза национальной безопасности — совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам³.

Удаленный доступ работника финансовой организации (удаленный доступ) — логический доступ работников финансовых организаций, реализуемый из-за пределов вычислительных сетей финансовых организаций⁴.

Удостоверяющий центр — юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом (Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи») ⁵.

Универсальные услуги связи — услуги связи, оказание которых любому пользователю услугами связи на всей территории Российской Федерации в заданный срок, с установленным качеством и по доступной цене является обязательным для операторов универсального обслуживания⁶.

Унифицированная процедура в автоматизированной системе — общая часть различных автоматизированных функций или задач, представляющая собой формализованную совокупность их одинаковых действий⁷.

¹ Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Пункт 2 — извлечение.

² Указ Президента РФ от 12 мая 2009 г. № 537 (ред. от 01.07.2014) «О Стратегии национальной безопасности Российской Федерации до 2020 года». Пункт 6.

³ Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». Раздел I, пункт 6 — извлечение.

⁴ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М., ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁵ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

⁶ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁷ ГОСТ Р 34.003-90. «Межгосударственный стандарт. Информационная техно-

Уничтожение (Destruction) — процесс уничтожения или удаления документов без какой-либо возможности их восстановления¹.

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных².

Уполномоченное учреждение — См. Уполномоченный орган, уполномоченное учреждение³.

Уполномоченный орган — федеральный орган исполнительной власти, уполномоченный Правительством Российской Федерации на осуществление полномочий, предусмотренных частью 2 статьи 16 настоящего Федерального закона, орган исполнительной власти субъекта Российской Федерации, уполномоченный высшим исполнительным органом государственной власти субъекта Российской Федерации на осуществление полномочий, предусмотренных частью 2 статьи 17 настоящего Федерального закона, орган местного самоуправления, уполномоченный в соответствии с уставом муниципального образования на осуществление полномочий, предусмотренных частью 2 статьи 18 настоящего Федерального закона⁴.

Уполномоченный орган — определенный Правительством Российской Федерации федеральный орган исполнительной власти в сфере промышленной политики⁵.

Уполномоченный орган — федеральный орган исполнительной власти, уполномоченный Правительством Российской Федерации на осуществление функций по нормативному правовому регулированию и полномочий, предусмотренных настоящим Федеральным законом, по вопросам экспериментальных правовых режимов, а по

логия. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27.12.1990 № 3399). Пункт 7 — извлечение.

¹ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26.03.2019 № 101-ст). Пункт 3 — извлечение.

² Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3 — извлечение.

³ См.: Уполномоченный орган, уполномоченное учреждение.

⁴ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

⁵ Федеральный закон от 31.12.2014 № 488-ФЗ «О промышленной политике в Российской Федерации», статья 3 — извлечение.

направлению, предусмотренному пунктом 4 части 2 статьи 1 настоящего Федерального закона, — Банк России¹.

Уполномоченный орган, уполномоченное учреждение — государственный орган, муниципальный орган, казенное учреждение, на которые возложены полномочия, предусмотренные статьей 26 настоящего Федерального закона².

Управление — совокупность целенаправленных действий, включающая оценку ситуации и состояния объекта управления, выбор управляющих воздействий и их реализацию³.

Управление документами (Records management) — область управления, обеспечивающая эффективное и систематическое создание, получение, сохранение, использование, передачу на хранение или уничтожение документов, включая процессы ввода в систему и хранения доказательств и информации о деловой деятельности и транзакции (обмене информацией) в виде документов⁴.

Управление инцидентами защиты информации — деятельность по своевременному обнаружению инцидентов защиты информации, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий от инцидентов защиты информации для финансовой организации и (или) ее клиентов, а также на снижение вероятности повторного возникновения инцидентов защиты информации⁵.

Управление сетью связи — совокупность организационно-технических мероприятий, направленных на обеспечение функционирования сети связи, в том числе регулирование трафика⁶.

¹ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

² Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

³ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27.12.1990 № 3399). Приложение 1 — извлечение.

⁴ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

⁵ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М., ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁶ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

Управленческие меры безопасности (Management controls) — меры безопасности информационной системы, направленные на менеджмент рисков и менеджмент информационной безопасности информационных систем. **Примечание.** Меры безопасности — меры защиты и контрмеры¹.

Управляющая функция автоматизированной системы управления технологическим процессом — функция АСУ технологическим процессом, включающая получение информации о состоянии технологического объекта управления, оценку информации, выбор управляющих воздействий и их реализацию².

Уровень защиты информации — определенная совокупность мер защиты информации, входящих в состав системы защиты информации и системы организации и управления защитой информации, применяемых совместно в пределах контура безопасности для реализации политики (режима) защиты информации, соответствующей критичности (важности) защищаемой информации бизнес-процессов и (или) технологических процессов финансовой организации³.

Уровень полномочий субъекта доступа (Subject privilege) — совокупность прав доступа субъекта доступа⁴.

Уровень реагирования на чрезвычайную ситуацию (далее — уровень реагирования) — состояние готовности органов управления и сил единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций к ликвидации чрезвычайной ситуации, требующее от органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций принятия дополнительных мер по защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера.

¹ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М., ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁴ Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

чайной ситуации в зависимости от классификации чрезвычайных ситуаций и характера развития чрезвычайной ситуации¹.

Услуга (Service) — выполнение действий, работы или обязанностей.

Примечание. Услуга самодостаточна, последовательна, дискретна и может быть составлена из других услуг².

Услуги платежного клиринга — прием к исполнению распоряжений участников платежной системы об осуществлении перевода денежных средств и выполнение иных действий, предусмотренных настоящим Федеральным законом (от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»³.

Услуга по пропуску трафика — деятельность, направленная на удовлетворение потребности операторов связи в пропуске трафика между взаимодействующими сетями электросвязи⁴.

Услуга присоединения — деятельность, направленная на удовлетворение потребности операторов связи в организации взаимодействия сетей электросвязи, при котором становятся возможными установление соединения и передача информации между пользователями взаимодействующих сетей электросвязи⁵.

Услуга связи — деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений⁶.

Услуги контентные — вид услуг связи, которые технологически неразрывно связаны с услугами подвижной радиотелефонной связи и направлены на повышение их потребительской ценности (в том числе услуги по предоставлению абонентам возможности получать на пользовательское (оконечное) оборудование в сетях связи справочную, развлекательную и (или) иную дополнительно оплачиваемую информацию, участвовать в голосовании, играх, конкурсах и аналогичных мероприятиях) и стоимость оказания которых оплачивается абонентом оператору связи, с которым у абонента заключен договор об оказании услуг связи⁷.

¹ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

² ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

³ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁴ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

⁵ Там же.

⁶ Там же.

⁷ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

Устройство управления системы обработки информации — устройство, предназначенное для выполнения функции управления в системе обработки информации в целом или ее отдельными частями¹.

Устройство связи с объектом — устройство, предназначенное для ввода сигналов с объекта в АС и вывода сигналов на объект².

Условия эксплуатации — совокупность факторов, действующих на изделие при его эксплуатации. К внешним факторам, действующим на изделие в процессе эксплуатации, относятся природные условия, тепловые, химические и механические воздействия, запыленность, влажность и т.п.³

Устойчивость автоматизированной системы управления военного назначения — комплексное свойство автоматизированной системы управления военного назначения, характеризующее живучестью, помехоустойчивостью и надежностью АСУ⁴.

Участник закупки — любое юридическое лицо независимо от его организационно-правовой формы, формы собственности, места нахождения и места происхождения капитала, за исключением юридического лица, местом регистрации которого является государство или территория, включенные в утверждаемый в соответствии с подпунктом 1 пункта 3 статьи 284 Налогового кодекса Российской Федерации перечень государств и территорий, предоставляющих льготный налоговый режим налогообложения и (или) не предусматривающих раскрытия и предоставления информации при проведении финансовых операций (офшорные зоны) в отношении юридических лиц (далее — офшорная компания), или любое физическое лицо, в том числе зарегистрированное в качестве индивидуального предпринимателя⁵.

Участник экспериментального правового режима — субъект экспериментального правового режима, а также лицо, вступившее в право-

¹ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. Постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

² ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

³ ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

⁴ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27.12.1990 № 3399). Пункт 7 — извлечение.

⁵ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

отношения с субъектом экспериментального правового режима в рамках указанного режима¹.

Участники комплексной программы — органы государственной власти, научные и образовательные организации, иные организации различных форм собственности, институты развития².

Участники комплексного проекта — органы государственной власти, научные и образовательные организации, иные организации различных форм собственности, институты развития³.

Участники консорциума — совокупность партнерских организаций лидирующего исследовательского центра независимо от формы собственности и организационно-правовой формы, с которыми российской организацией, структурным подразделением которой является лидирующий исследовательский центр, заключены гражданско-правовые договоры о сотрудничестве в целях совместной реализации мероприятий программы деятельности лидирующего исследовательского центра⁴.

Участники платежной системы — организации, присоединившиеся к правилам платежной системы в целях оказания услуг по переводу денежных средств⁵.

Участники реестра цифровых транзакций — лица, осуществляющие цифровые транзакции в соответствии с правилами ведения реестра цифровых транзакций⁶.

¹ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

² Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

³ Пункт 2 Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 19 февраля 2019 г. № 162.

⁴ Пункт 2 Правил предоставления субсидий из федерального бюджета на государственную поддержку программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий, утвержденных постановлением правительства РФ от 3 мая 2019 г. № 551. Извлечение.

⁵ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁶ Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

Участники уголовного судопроизводства — лица, принимающие участие в уголовном процессе¹.

Участники электронного взаимодействия — осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане².

Учетная запись — логический объект (информация), существующий в пределах одного или нескольких ресурсов доступа и представляющий субъекта доступа в его (их) пределах³.

Уязвимость (Vulnerability) — недостатки или слабости в проекте или реализации информационной системы, включая меры обеспечения безопасности, которые могут быть преднамеренно или непреднамеренно использованы для оказания неблагоприятного воздействия на активы организации или ее функционирование⁴.

Уязвимость — недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации⁵.

Уязвимость архитектуры — уязвимость, появившаяся в процессе проектирования информационной системы⁶.

Уязвимость кода — уязвимость, появившаяся в процессе разработки программного обеспечения⁷.

Уязвимость конфигурации — уязвимость, появившаяся в процессе задания конфигурации (применения параметров настройки) программного обеспечения и технических средств информационной системы⁸.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

² Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

³ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М., ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

⁴ ГОСТ Р ИСО/МЭК ТО 19791-2008 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие приказом Ростехрегулирования от 18 декабря 2008 г. № 525-ст). Пункт 3 — извлечение.

⁵ ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение.

⁶ Там же.

⁷ Там же.

⁸ Там же.

Уязвимость информационной системы (брешь) — свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации¹.

Уязвимость многофакторная — уязвимость, появившаяся в результате наличия нескольких недостатков различных типов².

Уязвимость организационная — уязвимость, появившаяся в связи с отсутствием (или недостатками) организационных мер защиты информации в информационной системе и (или) несоблюдением правил эксплуатации системы защиты информации информационной системы, требований организационно-распорядительных документов по защите информации и (или) несвоевременном выполнении соответствующих действий должностным лицом (работником) или подразделением, ответственными за защиту информации³.

Ф

Фактический маршрут выполнения функциональных объектов — последовательность фактически выполняемых функциональных объектов при определенных условиях (входных данных)⁴.

Фактор, воздействующий на защищаемую информацию — явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней⁵.

Федеральная информационная адресная система — федеральная государственная информационная система, обеспечивающая формирование, ведение и использование государственного адресного реестра⁶.

¹ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

² ГОСТ Р 56546-2015 «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» (утв. и введен в действие приказом Росстандарта от 19 августа 2015 г. № 1181-ст). Пункт 3 — извлечение.

³ Там же.

⁴ Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114). Пункт 2 — извлечение.

⁵ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁶ Федеральный закон от 28 декабря 2013 г. № 443-ФЗ «О федеральной информационной адресной системе и о внесении изменений в Федеральный закон «Об общих принципах организации местного самоуправления в Российской Федерации». Статья 2 — извлечение.

Федеральная государственная информационная система «Единая система нормативной справочной информации» (ФГИС ЕНСИ) — система обеспечения автоматизированного формирования, актуализации и использования реестра базовых государственных информационных ресурсов, а также обеспечивающая размещение, хранение и актуализацию информации технического характера, используемую в межведомственном электронном взаимодействии для обеспечения единообразного представления объектов информационного обмена, сведения о которых содержатся в государственных и муниципальных информационных ресурсах и используются в деятельности органов государственной власти и органов МСУ при исполнении государственных и муниципальных функций и предоставлении государственных и муниципальных услуг в электронном виде, и которая функционирует с учетом требований к информационной среде в сфере систематизации и кодирования информации¹.

Федеральное статистическое наблюдение — сбор первичных статистических данных и административных данных субъектами официального статистического учета².

Федеральный орган исполнительной власти по регулированию контрактной системы в сфере закупок — федеральный орган исполнительной власти, уполномоченный на осуществление функций по выработке государственной политики и нормативно-правовому регулированию в сфере закупок³.

Федеральный проект — проект, обеспечивающий достижение целей, целевых и дополнительных показателей, выполнение задач национального проекта и (или) достижение иных целей и показателей, выполнение иных задач по поручению и (или) указанию Президента Российской Федерации, поручению Председателя Правительства Российской Федерации, Правительства Российской Федера-

¹ Пункт 2 Положения о федеральной государственной информационной системе «Единая система нормативной справочной информации» согласно приложению № 1 к приказу Минкомсвязи России от 19.01.2015 № 7 «Об утверждении Положения о федеральной государственной информационной системе «Единая система нормативной справочной информации», а также Перечня нормативной справочной информации, подлежащей размещению в федеральной государственной информационной системе «Единая система нормативной справочной информации».

² Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Статья 2 — извлечение.

³ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

ции, решению Совета, президиума Совета, поручению куратора соответствующего национального проекта¹.

Федеральный проект Программы — проект, обеспечивающий достижение целей, целевых и дополнительных показателей, выполнение задач Программы, а также достижение иных целей и показателей, выполнение иных задач по поручению и указанию Президента Российской Федерации, поручению Председателя Правительства Российской Федерации, Правительства Российской Федерации, решениям Совета, президиума Совета, Комиссии, президиума Комиссии и поручению куратора Программы².

Физическая защита информации — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. **Примечания.** 1. Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты. 2. К объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации³.

Физический доступ к объекту доступа (физический доступ) — доступ к объекту доступа, включая доступ в помещение, в котором расположен объект доступа, позволяющий осуществить физическое воздействие на него⁴.

Финансирующее лицо — юридическое лицо либо действующее без образования юридического лица по договору о совместной деятельно-

¹ Пункт 3 Положения об организации проектной деятельности в Правительстве Российской Федерации, в ред. постановления Правительства РФ от 31 октября 2018 г. № 1288 (ред. от 30.07.2019) «Об организации проектной деятельности в Правительстве Российской Федерации». Извлечение.

² Пункт 3 Положения о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации», утвержденного постановлением Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации». Извлечение.

³ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁴ ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

сти объединение двух и более юридических лиц, предоставляющие заемные средства частному партнеру для реализации соглашения на условиях возвратности, платности, срочности¹.

Форма подтверждения соответствия — определенный порядок документального удостоверения соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров².

Функциональное устройство системы обработки информации — функционально законченная часть технических средств системы обработки информации³.

Функциональный объект — элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы. В качестве функциональных объектов могут выступать процедуры, функции, ветви, операторы и т.п.⁴

Функция (Function) — мероприятия, выполнение которых обеспечивает достижение стратегических целей деловой структуры⁵.

Функция автоматизированной системы — совокупность действий АС, направленная на достижение определенной цели⁶.

¹ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

² Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Статья 2 — извлечение.

³ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁴ Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114). Пункт 2 — извлечение.

⁵ ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. приказом Росстандарта от 26 марта 2019 г. № 101-ст). Пункт 3 — извлечение.

⁶ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

X

Характеристика проекта (Design characteristic) — атрибуты проекта или отличительные свойства, которые принадлежат оцениваемому описанию продукции или услуги¹.

Хранение при эксплуатации — содержание не используемого по назначению изделия в заданном состоянии в отведенном для его размещения месте с обеспечением сохранности в течение заданного срока².

Ц

Целостность (Integrity) — свойство сохранять правильность и полноту активов³.

Целостность информации (Information integrity) — способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)⁴.

Цель деятельности — желаемый результат процесса деятельности⁵.

Цель защиты информации — заранее намеченный результат защиты информации. **Примечание.** Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию⁶.

¹ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

² ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

³ ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 375-ст). Пункт 3 — извлечение.

⁴ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Приложение 1 — извлечение.

⁶ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

Цель процесса (Process purpose) — устремления высокого уровня в выполнении процесса и вероятные выходы эффективной реализации процесса. **Примечание.** Необходимо, чтобы реализация процесса обеспечивала ощутимую пользу заинтересованным сторонам¹.

Централизованное управление техническими мерами защиты информации — управление средствами и системами, реализующими технические меры защиты информации, множественно размещаемыми на АРМ пользователей и эксплуатационного персонала. **Примечание.** В составе функций централизованного управления рассматриваются:

- автоматизированная установка и обновление ПО технических мер защиты информации, получаемых из единого (эталонного) источника;
- автоматизированное обновление сигнатурных баз в случае их использования, получаемых из единого (эталонного) источника, с установленной периодичностью;
- автоматизированное установление параметров настроек технических мер защиты информации, получаемых из единого (эталонного) источника;
- контроль целостности ПО технических мер защиты информации, параметров настроек технических мер защиты информации и сигнатурных баз при осуществлении их автоматизированной установки и (или) обновлении;
- контроль целостности единого (эталонного) источника ПО технических мер защиты информации, параметров настроек технических мер защиты информации и сигнатурных баз;
- централизованный сбор данных регистрации о событиях защиты информации, формируемых техническими мерами защиты информации².

Центральный платежный клиринговый контрагент — платежный клиринговый центр, выступающий в соответствии с настоящим Федеральным законом плательщиком и получателем средств по переводам денежных средств участников платежной системы³.

¹ ГОСТ Р 57193-2016 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие приказом Росстандарта от 31 октября 2016 г. № 1538-ст). Раздел 4 — извлечение.

² ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 882-ст «Об утверждении национального стандарта». М.: ФГУП «Стандартинформ», 2017. Пункт 3 — извлечение.

³ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

Центральный процессор — процессор, выполняющий в данной вычислительной машине или системе обработки информации основные функции по обработке информации и управлению работой других частей вычислительной машины или системы¹.

Цифровая запись — информация о цифровых финансовых активах, зафиксированная в реестре цифровых транзакций².

Цифровые инновации — новые или существенно улучшенные продукт (товар, результат выполнения работы, услуга, охраняемый результат интеллектуальной деятельности) или процесс, новый метод продаж или новый организационный метод в деловой практике, организации рабочих мест или во внешних связях, введенные в употребление, созданные или используемые по направлениям, предусмотренным частью 2 статьи 1 настоящего Федерального закона, с применением технологий, перечень которых утверждается Правительством Российской Федерации, а по направлению, предусмотренному пунктом 4 части 2 статьи 1 настоящего Федерального закона, — Центральным банком Российской Федерации (далее — Банк России)³.

Цифровая платформа — система средств, поддерживающая использование цифровых процессов, ресурсов и сервисов значительным количеством субъектов цифровой экосистемы и обеспечивающая возможность их бесшовного взаимодействия⁴.

Цифровая платформа — совокупность информационных технологий и технических средств, обеспечивающих взаимодействие субъектов хозяйственной деятельности в сфере промышленности⁵.

Цифровая повестка — круг актуальных для Союза (Евразийского экономического союза) вопросов по цифровой трансформации в рамках развития интеграции, укрепления единого экономического простран-

¹ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

² Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

³ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» — (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

⁴ Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». Раздел 1. Определения — извлечение.

⁵ Пункт 2 Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологической промышленной продукции, утвержденных постановлением Правительства РФ от 30 апреля 2019 г. № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологической промышленной продукции». Извлечение.

ства и углубления сотрудничества государств-членов, определенный в Заявлении о цифровой повестке Евразийского экономического союза от 26 декабря 2016 года и настоящих Основных направлениях¹.

Цифровая транзакция — действие или последовательность действий, направленных на создание, выпуск, обращение цифровых финансовых активов².

Цифровая трансформация — проявление качественных, революционных изменений, заключающихся не только в отдельных цифровых преобразованиях, но в принципиальном изменении структуры экономики, в переносе центров создания добавленной стоимости в сферу выстраивания цифровых ресурсов и сквозных цифровых процессов. В результате цифровой трансформации осуществляется переход на новый технологический и экономический уклад, а также происходит создание новых отраслей экономики³.

Цифровая экономика — часть экономики, в которой процессы производства, распределения, обмена и потребления прошли цифровые преобразования с использованием информационно-коммуникационных технологий⁴.

Цифровая экономика — хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг⁵.

Цифровая экосистема — открытая устойчивая система, включающая субъекты цифровой экосистемы (физических, юридических, виртуальных и пр.), а также связи и отношения этих субъектов в цифровой форме на основе сервисов цифровой платформы⁶.

¹ Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». Раздел 1. Определения — извлечение.

² Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

³ Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». Раздел 1. Определения — извлечение.

⁴ Там же.

⁵ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁶ Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». Раздел 1. Определения — извлечение.

- Цифровое преобразование** — комплекс мероприятий, нацеленных на трансформацию бизнес-процессов в соответствии с их цифровой моделью¹.
- Цифровое пространство** — пространство, интегрирующее цифровые процессы, средства цифрового взаимодействия, информационные ресурсы, а также совокупность цифровых инфраструктур, на основе норм регулирования, механизмов организации, управления и использования².
- Цифровой актив** — совокупность информации в цифровой форме и средств по ее обработке, собранная на основе конкурентной бизнес-модели, использование которой приводит к получению экономических выгод³.
- Цифровой кошелек** — программно-техническое средство, которое позволяет хранить информацию о цифровых записях. Цифровой кошелек может обеспечивать доступ к реестру цифровых транзакций⁴.
- Цифровой профиль** — совокупностью сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в единой системе идентификации и аутентификации⁵.
- Цифровой финансовый актив** — имущество в электронной форме, созданное с использованием криптографических средств. Право собственности на данное имущество удостоверяется путем внесения цифровых записей в реестр цифровых транзакций. К цифровым финансовым активам относятся криптовалюта, токен. Цифровые финансовые активы не являются законным средством платежа на территории Российской Федерации⁶.
- Цифровые инновации** — новые или существенно улучшенные продукты (товары, результаты работ, услуги, охраняемые результаты интеллектуальной деятельности), вводимые в гражданский оборот, созданные или используемые по направлениям, указанным в части 2 статьи 1 настоящего федерального закона, с применени-

¹ Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». Раздел 1. Определения — извлечение.

² Там же.

³ Там же.

⁴ Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

⁵ Пункт 1 статьи 14.2 Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» в ред. проекта № 260319.

⁶ Статья 2 Федерального закона «О цифровых финансовых активах» — Проект № 419059-7.

ем технологий, перечень которых утверждается Правительством Российской Федерации¹.

Цифровые права — названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу².

Ч

Частный обвинитель — потерпевший или его законный представитель и представитель по уголовным делам частного обвинения³.

Частный партнер — российское юридическое лицо, с которым в соответствии с настоящим Федеральным законом заключено соглашение⁴.

Чрезвычайная ситуация — обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей среде, значительные материальные потери и нарушение условий жизнедеятельности людей⁵.

Ш

Шифровальные средства — средства, реализующие криптографические алгоритмы преобразования информации; аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации (в т. ч. и входящие в системы и комплексы защиты информации от несанкционированного доступа), циркулирующей в технических средствах, при ее обработке,

¹ Статья 2 проекта Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» — fz_160719 (дата обращения: 17.07.2019). Извлечение.

² Пункт 1 статьи 141.1 части первой Гражданского кодекса Российской Федерации.

³ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁴ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

⁵ Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 г. № 68-ФЗ. Статья 1 — извлечение.

хранении и передаче по каналам связи, включая шифровальную технику; средства, реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и «электронной подписи»; аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации¹.

Штатная эксплуатация — см. «Нормальная эксплуатация»².

Э

ЭВМ общего назначения — ЭВМ, относящаяся к классу вычислительных машин, занимающих по шкале производительности широкий диапазон и предназначенных для решения широкого класса задач примерно одинаковой технико-экономической эффективностью. Примечание. Как правило, ЭВМ общего назначения устанавливаются на вычислительных центрах³.

Экосистема цифровой экономики — партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан⁴.

Экспериментальный правовой режим — применение в отношении участников экспериментального правового режима в течение определенного периода времени специального регулирования в сфере цифровых инноваций по направлениям, предусмотренным частью 2 статьи 1 настоящего Федерального закона⁵.

¹ Положение о государственном лицензировании деятельности в области защиты информации (утверждено решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

² ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

³ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁴ Пункт 4 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

⁵ Проект Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» — (Законопроект № 922869-7, дата обращения: 18 марта 2020 г.), статья 2 — извлечение.

Эксперт, экспертная организация — обладающее специальными познаниями, опытом, квалификацией в области науки, техники, искусства или ремесла физическое лицо, в том числе индивидуальный предприниматель, либо юридическое лицо (работники юридического лица должны обладать специальными познаниями, опытом, квалификацией в области науки, техники, искусства или ремесла), которые осуществляют на основе договора деятельность по изучению и оценке предмета экспертизы, а также по подготовке экспертных заключений по поставленным заказчиком, участником закупки вопросам в случаях, предусмотренных настоящим Федеральным законом¹.

Экспертная площадка — организуемый Евразийской экономической комиссией для обсуждения и детальной проработки инициатив и проектов формат работы представителей государственных органов, бизнес-сообществ государств-членов с участием центров компетенций, научных организаций, предприятий и других экспертов².

Экспертиза документа по защите информации — рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение. **Примечание.** Экспертиза документа по защите информации может включать в себя научно-техническую, правовую, метрологическую, патентную и терминологическую экспертизы³.

Экспертиза судебная — экспертиза, производимая в порядке, установленном УПК РФ⁴.

Экспертное учреждение — государственное судебно-экспертное или иное учреждение, которому поручено производство судебной экспертизы в порядке, установленном УПК РФ⁵.

Эксплуатационная документация на автоматизированную систему — часть рабочей документации на АС, предназначенная для использования при эксплуатации системы, определяющая правила

¹ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

² Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». Раздел 1. Определения — извлечение.

³ ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

⁴ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

⁵ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. Статья 5 — извлечение.

действия персонала и пользователей системы при ее функционировании, проверке и обеспечении ее работоспособности¹.

Эксплуатация — стадия жизненного цикла изделия, на которой реализуется, поддерживается и восстанавливается его качество. Примечание. Эксплуатация изделия включает в себя в общем случае использование по назначению, транспортирование, техническое обслуживание и ремонт (для специальных видов техники номенклатура видов ремонта, входящих в эксплуатацию, устанавливается в отраслевой нормативно-технической документации). Под жизненным циклом изделия понимают совокупность разработки, изготовления, обращения, эксплуатации и утилизации изделия от начала исследования возможности его создания до окончания применения. Отличительной особенностью эксплуатации является использование или ожидание использования изделия по назначению².

Эксплуатация объекта соглашения — использование объекта соглашения в целях осуществления деятельности, предусмотренной таким соглашением, по производству товаров, выполнению работ, оказанию услуг в порядке и на условиях, которые определены соглашением³.

Электронная вычислительная машина — вычислительная машина, основные функциональные устройства которой выполнены на электронных компонентах⁴.

Электронная площадка — сайт в информационно-телекоммуникационной сети «Интернет», соответствующий установленным в соответствии с пунктами 1 и 2 части 2 статьи 24.1 настоящего Федерального закона требованиям, на котором проводятся конкурентные способы определения поставщиков (подрядчиков, исполнителей) в электронной форме, за исключением закрытых способов определения поставщиков (подрядчиков, исполнителей) в электронной форме⁵.

¹ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

² ГОСТ 25866-83 «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. постановлением Госстандарта СССР от 13 июля 1983 г. № 3105). Извлечение.

³ Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Статья 3 — извлечение.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Статья 3 — извлечение.

- Электронная подпись** — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, и которая используется для определения лица, подписывающего информацию¹.
- Электронное сообщение** — информация, переданная или полученная пользователем информационно-телекоммуникационной сети².
- Электронное средство платежа** — средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств³.
- Электронные денежные средства** — денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность и (или) деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций⁴.
- Электронный документ** — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных

¹ Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Статья 2 — извлечение.

² Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

³ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

⁴ Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». Статья 3 — извлечение.

машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах¹.

Электромагнитная совместимость — способность радиоэлектронных средств и (или) высокочастотных устройств функционировать с установленным качеством в окружающей электромагнитной обстановке и не создавать недопустимые радиопомехи другим радиоэлектронным средствам и (или) высокочастотным устройствам².

Электросвязь — любое излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам³.

Эмуляция — имитация функционирования одного устройства посредством другого устройства или устройств вычислительной машины, при которой имитирующее устройство воспринимает те же данные, выполняет ту же программу и достигает того же результата, что и имитируемое⁴.

Эргономическое обеспечение автоматизированной системы — совокупность реализованных решений в АС по согласованию психологических, психофизиологических, антропометрических, физиологических характеристик и возможностей пользователей АС с техническими характеристиками комплекса средств автоматизации АС и параметрами рабочей среды на рабочих местах персонала АС⁵.

Этап создания автоматизированной системы — часть стадии создания АС, выделенная по соображениям единства характера работ и (или) завершающего результата или специализации исполнителей⁶.

Эффективность автоматизированной системы — свойство АС, характеризующее степень достижения целей, поставленных при ее создании. Примечание. К видам эффективности АС, например, относят экономическую, техническую, социальную и др.

¹ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 2 — извлечение.

² Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Статья 2 — извлечение.

³ Там же.

⁴ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

Эффективность защиты информации — степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты; **контроль эффективности защиты информации** — проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты¹.

Эффективность защиты информации — степень соответствия результатов защиты информации цели защиты информации².

Я

Ядро защиты (диспетчер доступа) (Security kernel) — технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа³.

Язык программирования (Programming language) — язык, предназначенный для представления программ. **Примечание.** К традиционным языкам программирования процедурного типа относят, как правило, языки для представления программ в виде последовательности предписания⁴.

Язык проектирования в САПР — язык, используемый в системе автоматизированного проектирования и предназначенный для представления и преобразования описаний при проектировании⁵.

Ячейка памяти — минимальная адресуемая область памяти данных⁶.

¹ Положение о государственном лицензировании деятельности в области защиты информации (утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10) (с изменениями и дополнениями от 24 июня 1997 г. № 60). Пункт 1.2. — извлечение.

² ГОСТ Р 50922-2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст). Пункт 2 — извлечение.

³ Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения». Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

⁴ ГОСТ 28397-89 (ИСО 2382-15-85 «Межгосударственный стандарт. Языки программирования. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 21 декабря 1989 г. № 3961). Подпункт 4 пункта 6 — извлечение.

⁵ ГОСТ Р 34.003-90 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399). Пункт 7 — извлечение.

⁶ ГОСТ 15971-90 «Системы обработки информации. Термины и определения» (утв. постановлением Госстандарта СССР от 26 октября 1990 г. № 2698). Пункт 5 — извлечение.

ПРИЛОЖЕНИЯ

Приложение 1

Перечень основных нормативных правовых актов по вопросам регулирования цифровой экономики и информационной безопасности

Нормативный правовой акт (далее — НПА) — это письменный официальный документ, принятый (изданный) в определенной форме правотворческим органом в пределах его компетенции и направленный на установление, изменение или отмену правовых норм. В свою очередь, под правовой нормой принято понимать общеобязательное государственное предписание постоянного или временного характера, рассчитанное на многократное применение¹.

Следует отметить, что правила подготовки НПА ФОИВ и их государственной регистрации утверждены постановлением Правительства РФ от 13.08.1997 № 1009, действующим по состоянию на текущую дату в редакции от 31 октября 2018 г. (далее Постановление № 1009).

Согласно Постановлению № 1009 НПА издаются ФОИВ в виде постановлений, приказов, распоряжений, правил, инструкций и положений. Издание НПА в виде писем и телеграмм не допускается.

В этом же Постановлении отмечается, что структурные подразделения и территориальные органы ФОИВ не вправе издавать НПА и что НПА может быть издан совместно несколькими ФОИВ или одним из них по согласованию с другими.

В Постановлении № 1009 подчеркивается, что в процессе работы над проектом НПА должны быть изучены относящиеся к теме проекта законодательство РФ, договоры о разграничении предметов ведения и полномочий между органами государственной власти РФ и органами государственной власти субъектов РФ, практика применения соответствующих НПА, научная литература и материалы периодической печати по рассматриваемому вопросу, а также данные социологических и иных исследований, если таковые проводились.

¹ Постановление ГД ФС РФ от 11 ноября 1996 г. № 781-П ГД «Об обращении в Конституционный Суд Российской Федерации». Извлечение.

Правовую экспертизу проектов подготовленных НПА может осуществлять Минюст России в соответствии с заключенными договорами между ФОИВ и Минюст России.

Разъяснения о применении правил подготовки НПА ФОИВ и их государственной регистрации утверждены Приказом Минюста России 04.05.2007 № 88, который по состоянию на текущую дату действует в редакции от 26 мая 2009 г.

При этом важно отметить, что в Указе Президента РФ от 15.03.2000 № 511 (ред. от 28.06.2005) «О классификаторе правовых актов» порядок подготовки и рассмотрения проектов НПА классифицирован под номером 010.140.020.

Что касается порядка раскрытия ФОИВ информации о подготовке проектов НПА и результатах их общественного обсуждения, то он утвержден постановлением Правительства РФ от 25.08.2012 № 851 (ред. от 31.10.2018).

В целях анализа достижения целей регулирования, определения и оценки фактических положительных и отрицательных последствий принятия НПА, а также выявления в них положений, необоснованно затрудняющих ведение предпринимательской и иной экономической деятельности или приводящих к возникновению необоснованных расходов бюджетов бюджетной системы РФ предусмотрена оценка их фактического воздействия. Порядок проведения такой оценки утвержден постановлением Правительства РФ от 30.01.2015 № 83 (ред. от 29.08.2018).

Как отмечается в этом Постановлении оценка фактического воздействия НПА проводится в двух случаях, в частности, в отношении НПА, при разработке проектов которых проводилась оценка регулирующего воздействия; и второй случай — в отношении НПА по решению Президента РФ, Правительства РФ, Правительственной комиссии по проведению административной реформы (далее — Комиссия) или подкомиссии по оценке фактического воздействия НПА при Комиссии.

В настоящем издании приведен перечень действующих НПА по вопросам правового регулирования цифровой экономики и информационной безопасности.

НПА представлены в следующей последовательности:

1. Кодексы Российской Федерации.
2. Федеральные законы.
 - 2.1. Проекты Федеральных законов.
3. Законы.
 - 3.1. Законы РСФСР.
 - 3.2. Законы Российской Федерации.
4. Указы Президента Российской Федерации.
5. Распоряжения Президента Российской Федерации.
6. Послания Президента Российской Федерации.
7. Постановления Правительства Российской Федерации.

8. Распоряжения Правительства Российской Федерации.
9. Основные направления деятельности Правительства Российской Федерации.
10. Руководящие документы ФОИВ.
 - 10.1. Документы ФСБ России.
 - 10.2. Документы ФСО России.
 - 10.3. Документы ФСТЭК России/Государственной технической комиссии при Президенте Российской Федерации/Федерального агентства правительственной связи и информации при Президенте Российской Федерации.
 - 10.4. Документы Счетной палаты Российской Федерации.
11. Приказы Мининформсвязи/Минкомсвязи России.
 - 11.1. Приказы Роскомнадзора.
12. Приказы МИД России.
13. Приказы, распоряжения и письма Минэкономразвития России.
 - 13.1. Приказы Минэкономразвития России.
 - 13.2. Распоряжения Минэкономразвития России.
 - 13.3. Письма Минэкономразвития России.
 - 13.4. Приказы Росстата.
14. Приказы Минфина России.
 - 14.1. Приказы Казначейства России.
15. Приказы Минтруда России.
16. Приказы Минпромторга России.
 - 16.1. Приказы Федерального агентства по техническому регулированию и метрологии (Росстандарт).
17. Приказы Минсельхоза России.
18. Приказы Минобрнауки и Минпросвещения России.
 - 18.1. Приказы Минобрнауки России.
 - 18.2. Приказы Минпросвещения России.
19. Приказы Ростехнадзора.
20. Совместные приказы ФОИВ.
 - 20.1. Приказы Минкомсвязи России/ФСО России.
 - 20.2. Приказы МИД России/МВД России/ФСБ России.
 - 20.3. Приказы МИД России/МО России, Минприроды России, Минфина России, МВД России, ФСБ России и других ФОИВ.
21. Приказы МВД России.
22. Приказы Генпрокуратуры России.
23. Приказы Минюста России.
24. Приказы Минэнерго России.
25. ГОСТы, межгосударственные и национальные стандарты.
 - 25.1. Рабочие документы (Методические указания).
26. Решения Высшего Евразийского экономического совета.
27. Постановления правительства Москвы.
28. Законы и постановления правительства Московской области.

29. Положения Банка России.
30. Паспорта федеральных проектов в рамках национальной программы «Цифровая экономика Российской Федерации».
31. Дорожные карты развития «сквозной» цифровой технологии.
32. Регистрация доменных имен.

Конкретные НПА, относящиеся к правовому регулированию правоотношений в сфере цифровой экономики и информационной безопасности, приведены в соответствующих разделах в хронологическом порядке¹.

Выбранный подход к их представлению обусловлен необходимостью осуществления мониторинга действующего законодательства в данной предметной области в наиболее удобной форме.

1. Кодексы Российской Федерации

Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ.
Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ.

Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ.

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ.

Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ.

Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ.

2. Федеральные законы

Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности».

Федеральный закон от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера».

Федеральный закон от 03.04.1995 № 40-ФЗ «О федеральной службе безопасности».

Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг».

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».

Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

¹ Включение в данный перечень конкретных НПА осуществлен автором исходя из наличия в них соответствующих положений, касающихся правоотношений в цифровой экономике и обеспечения информационной безопасности и носит субъективный характер.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

Федеральный закон от 29.11.2007 № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации».

Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

Федеральный закон от 21.11.2011 № 325-ФЗ «Об организованных торгах».

Федеральный закон от 03.12.2011 № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса».

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

Федеральный закон от 28.12.2013 № 443-ФЗ «О федеральной информационной адресной системе и о внесении изменений в Федеральный закон «Об общих принципах организации местного самоуправления в Российской Федерации».

Федеральный закон от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации».

Федеральный закон от 31.12.2014 № 488-ФЗ «О промышленной политике в Российской Федерации».

Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации».

Федеральный закон от 13.07.2015 № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации».

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Федеральный закон от 27.12.2019 № 478-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части внедрения реестровой модели предоставления государственных услуг по лицензированию отдельных видов деятельности».

2.1. Проекты Федеральных законов

Федеральный закон «О систематизации и гармонизации информации в Российской Федерации» — проект в редакции от 04.05.2018.

«Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» — проект № 922869-7 внесен Правительством РФ в ГД Федерального собрания РФ 16 марта 2020 г. № 2133п-П10 (дата обращения 18.03.2020).

Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации — fz_160719 (дата обращения: 17.07.2019).

3. Законы

3.1. Законы РСФСР

Закон РСФСР от 22.03.1991 № 948-1 «О конкуренции и ограничении монополистической деятельности на товарных рынках».

3.2. Законы Российской Федерации

Закон Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации».

Закон Российской Федерации от 05.03.1992 № 2446-1 «О безопасности».

Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне».

4. Указы Президента Российской Федерации

Указ Президента РФ от 28.06.1993 № 966 «О Концепции правовой информатизации России».

Указ Президента РФ от 14.03.1995 № 272 «О дополнительных мерах по повышению эффективности работы Министерства иностранных дел Российской Федерации».

Указ Президента РФ от 03.04.1995 № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне».

Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

Указ Президента РФ от 15.03.2000 № 511 «О классификаторе правовых актов».

Указ Президента РФ от 11.07.2004 № 865 «Вопросы Министерства иностранных дел Российской Федерации».

Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».

Указ Президента РФ от 25.08.2010 № 1060 «О совершенствовании государственного управления в сфере информационных технологий».

Указ Президента РФ от 08.11.2011 № 1478 «О координирующей роли Министерства иностранных дел Российской Федерации в проведении единой внешнеполитической линии Российской Федерации».

Указ Президента РФ от 17.12.2011 № 1661 «Об утверждении списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль».

Указ Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Указ Президента РФ от 21.07.2014 № 519 «О внесении изменений в Список товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль, утвержденный Указом Президента Российской Федерации от 17 декабря 2011 г. № 1661».

Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети “Интернет” и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети “Интернет”»).

Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации».

Указ Президента РФ от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации».

Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

Указ Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Указ Президента РФ от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

Указ Президента РФ от 15.05.2018 № 215 «О структуре федеральных органов исполнительной власти».

Указ Президента РФ от 29.06.2018 № 378 «О Национальном плане противодействия коррупции на 2018–2020 годы».

Указ Президента РФ от 19.07.2018 № 444 «Об упорядочении деятельности совещательных и консультативных органов при Президенте Российской Федерации» (вместе с «Положением о Совете при Президенте Российской Федерации по стратегическому развитию и национальным проектам»).

Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»).

5. Распоряжения Президента Российской Федерации

Распоряжение Президента РФ от 24.09.1992 № 536-рп «О мерах по созданию системы правовой информатизации».

Распоряжение Президента РФ от 16.04.2005 № 151-рп «О перечне должностных лиц органов государственной власти и организаций, подлежащих полномочиями по отнесению сведений к государственной тайне».

6. Послания Президента Российской Федерации

Послание Президента Российской Федерации Федеральному Собранию от 01.12.2016.

7. Постановления Правительства Российской Федерации

1991¹

Постановление Правительства РСФСР от 05.12.1991 № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

¹ Здесь и далее указаны года принятия постановлений Правительства РФ. Ссылка обусловлена большим количеством постановлений.

1993

Постановление Правительства РФ от 28.04.1993 № 385 «Об образовании межведомственной комиссии по участию Российской Федерации в Межправительственной программе ЮНЕСКО по информатике».

1995

Постановление Правительства РФ от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».

Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации».

Постановление Правительства РФ от 23.10.1995 № 1029 «Вопросы финансового и материального положения Министерства иностранных дел Российской Федерации».

1997

Постановление Правительства РФ от 13.08.1997 № 1009 «Об утверждении Правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации».

2002

Постановление Правительства РФ от 10.04.2002 № 228 «О мерах по повышению эффективности использования федерального имущества, закрепленного в хозяйственном ведении федеральных государственных унитарных предприятий» (вместе с «Правилами разработки и утверждения программ деятельности и определения подлежащей перечислению в федеральный бюджет части прибыли федеральных государственных унитарных предприятий»).

2003

Постановление Правительства РФ от 15.08.2003 № 500 «О федеральном информационном фонде технических регламентов и стандартов и единой информационной системе по техническому регулированию».

Постановление Правительства РФ от 05.11.2003 № 673 «Об опубликовании и размере платы за опубликование документов о разработке, обсуждении и экспертной оценке проектов технических регламентов, проектов законодательных, иных нормативных правовых актов и нормативных документов в области технического регулирования».

2004

Постановление Правительства РФ от 01.06.2004 № 260 «О Регламенте Правительства Российской Федерации и Положении об Аппарате Правительства Российской Федерации».

Постановление Правительства РФ от 03.12.2004 № 739 «О полномочиях федеральных органов исполнительной власти по осуществлению прав собственника имущества федерального государственного унитарного предприятия».

Постановление Правительства РФ от 15.12.2004 № 791 «Об утверждении Правил финансирования за счет средств федерального бюджета расходов в области технического регулирования».

2006

Постановление Правительства РФ от 09.08.2006 № 476 «О создании акционерного общества «Российский Инвестиционный фонд информационно-коммуникационных технологий».

2008

Постановление Правительства РФ от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации».

Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2009

Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»).

Постановление Правительства РФ от 22.09.2009 № 754 «Об утверждении Положения о системе межведомственного электронного документооборота».

Постановление Правительства РФ от 25.12.2009 № 1088 «О государственной автоматизированной информационной системе «Управление»» (вместе с «Положением о государственной автоматизированной информационной системе «Управление»»).

2010

Постановление Правительства РФ от 15.05.2010 № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения».

Постановление Правительства РФ от 24.05.2010 № 365 «О координации мероприятий по использованию информационно-комму-

никационных технологий в деятельности государственных органов» (вместе с «Положением о координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов», «Правилами подготовки планов информатизации государственных органов и отчетов об их выполнении»).

Постановление Правительства РФ от 26.05.2010 № 367 «О единой межведомственной информационно-статистической системе» (вместе с «Положением о единой межведомственной информационно-статистической системе»).

Постановление Правительства РФ от 01.06.2010 № 391 «О порядке создания государственной информационной системы в области энергосбережения и повышения энергетической эффективности и условий для ее функционирования» (вместе с «Правилами создания государственной информационной системы в области энергосбережения и повышения энергетической эффективности и условий для ее функционирования»).

Постановление Правительства РФ от 02.08.2010 № 588 «Об утверждении Порядка разработки, реализации и оценки эффективности государственных программ Российской Федерации».

Постановление Правительства РФ от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия» (вместе с «Положением о единой системе межведомственного электронного взаимодействия»).

2011

Постановление Правительства РФ от 16.05.2011 № 373 «О разработке и утверждении административных регламентов осуществления государственного контроля (надзора) и административных регламентов предоставления государственных услуг» (вместе с «Правилами разработки и утверждения административных регламентов осуществления государственного контроля (надзора)», «Правилами разработки и утверждения административных регламентов предоставления государственных услуг», «Правилами проведения экспертизы проектов административных регламентов осуществления государственного контроля (надзора) и административных регламентов предоставления государственных услуг»).

Постановление Правительства РФ от 08.06.2011 № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» (вместе с «Положением об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме»).

Постановление Правительства РФ от 24.10.2011 № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)» (вместе с «Положением о федеральной государственной информационной системе «Федеральный реестр государственных и муниципальных услуг (функций)», «Правилами ведения федеральной государственной информационной системы “Федеральный реестр государственных и муниципальных услуг (функций)”», «Положением о федеральной государственной информационной системе “Единый портал государственных и муниципальных услуг (функций)”», «Требованиями к региональным порталам государственных и муниципальных услуг (функций)»).

Постановление Правительства РФ от 28.11.2011 № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

Постановление Правительства РФ от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (вместе с «Требованиями к федеральной государственной информационной системе “Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме”»).

Постановление Правительства Российской Федерации от 5 декабря 2011 г. № 995 «Об осуществлении бюджетных инвестиций в проектирование и строительство объектов капитального строительства — центров обработки данных, подведомственных Федеральной налоговой службе».

Постановление Правительства РФ от 28.12.2011 № 1184 «О мерах по обеспечению перехода федеральных органов исполнительной власти, государственных корпораций, наделенных соответствующими федеральными законами полномочиями по предоставлению государственных услуг, и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде» (вместе с «Правилами обеспечения перехода федеральных органов исполнительной власти, государственных корпораций, наделенных соответствующими федеральными законами полномочиями по предоставлению государственных услуг, и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде при предоставлении государственных услуг»).

2012

Постановление Правительства РФ от 26.01.2012 № 24 «О государственной информационной системе в области средств массовой информации» (вместе с «Правилами создания и функционирования государственной информационной системы в области средств массовой информации»).

Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»).

Постановление Правительства РФ от 09.02.2012 № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» (вместе с «Правилами использования усиленной квалифицированной электронной подписи органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой», «Требованиями к обеспечению совместимости средств электронной подписи при организации электронного взаимодействия органов исполнительной власти и органов местного самоуправления между собой»).

Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Постановление Правительства РФ от 25.04.2012 № 394 «О мерах по совершенствованию использования информационно-коммуникационных технологий в деятельности государственных органов».

Постановление Правительства РФ от 26.06.2012 № 644 «О федеральной государственной информационной системе учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов».

Постановление Правительства РФ от 25.08.2012 № 851 «О порядке раскрытия федеральными органами исполнительной власти информации о подготовке проектов нормативных правовых актов и результатах их общественного обсуждения» (вместе с «Правилами раскрытия федеральными органами исполнительной власти информации о подготовке проектов нормативных правовых актов и результатах их общественного обсуждения»).

Постановление Правительства РФ от 06.09.2012 № 890 «О мерах по совершенствованию электронного документооборота в органах государственной власти».

Постановление Правительства РФ от 10.09.2012 № 909 «Об определении официального сайта Российской Федерации в информационно-телекоммуникационной сети “Интернет” для размещения информации о проведении торгов и внесении изменений в некоторые акты Правительства Российской Федерации».

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства РФ от 16.11.2012 № 1172 «О полномочиях федеральных органов исполнительной власти в области государственной поддержки инновационной деятельности».

Постановление Правительства РФ от 22.12.2012 № 1382 «О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» (вместе с «Правилами присоединения информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме»).

2013

Постановление Правительства РФ от 30.01.2013 № 62 «О национальном фонде алгоритмов и программ для электронных вычислительных машин» (вместе с «Положением о национальном фонде алгоритмов и программ для электронных вычислительных машин»).

Постановление Правительства РФ от 10.07.2013 № 584 «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (вместе с «Пра-

вилами использования федеральной государственной информационной системы “Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме”»).

Постановление Правительства РФ от 10.07.2013 № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных» (вместе с «Правилами отнесения информации к общедоступной информации, размещаемой государственными органами и органами местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных», «Правилами определения периодичности размещения в информационно-телекоммуникационной сети “Интернет” в форме открытых данных общедоступной информации о деятельности государственных органов и органов местного самоуправления, сроков ее обновления, обеспечивающих своевременность реализации и защиты пользователями своих прав и законных интересов, а также иных требований к размещению указанной информации в форме открытых данных», «Правилами обязательного размещения органами государственной власти субъектов Российской Федерации и органами местного самоуправления общедоступной информации о деятельности органов государственной власти субъектов Российской Федерации и органов местного самоуправления, созданной указанными органами или поступившей к ним при осуществлении полномочий по предметам ведения Российской Федерации и полномочий Российской Федерации по предметам совместного ведения Российской Федерации и субъектов Российской Федерации, переданных для осуществления органам государственной власти субъектов Российской Федерации или органам местного самоуправления, в информационно-телекоммуникационной сети “Интернет” в форме открытых данных»).

Постановление Правительства РФ от 26.12.2013 № 1293 «О федеральной государственной информационной системе “Федеральный портал государственной службы и управленческих кадров” и о создании на ее базе пилотной версии единой информационной системы управления кадровым составом государственной гражданской службы Российской Федерации».

2014

Постановление Правительства РФ от 15.04.2014 № 298 «Об утверждении государственной программы Российской Федерации “Содействие занятости населения”».

Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации “Информационное общество”».

Постановление Правительства РФ от 15.04.2014 № 316 «Об утверждении государственной программы Российской Федерации “Экономическое развитие и инновационная экономика”».

Постановление Правительства РФ от 15.04.2014 № 328 «Об утверждении государственной программы Российской Федерации “Развитие промышленности и повышение ее конкурентоспособности”».

Постановление Правительства РФ от 15.04.2014 № 330 «Об утверждении государственной программы Российской Федерации “Развитие внешнеэкономической деятельности”».

Постановление Правительства РФ от 15.04.2014 № 325-10 «Об утверждении государственной программы Российской Федерации “Внешнеполитическая деятельность”».

Постановление Правительства РФ от 14.05.2014 № 434 «О радиочастотной службе» (вместе с «Положением о радиочастотной службе»).

Постановление Правительства РФ от 31.07.2014 № 741 «Об определении федерального органа исполнительной власти, уполномоченного на установление требований к оборудованию и программно-техническим средствам, используемым организатором распространения информации в информационно-телекоммуникационной сети “Интернет” в эксплуатируемых им информационных системах».

Постановление Правительства РФ от 14.11.2014 № 1194 «О международно-правовой защите присвоения (назначения) радиочастот или радиочастотных каналов и порядке использования на территории Российской Федерации спутниковых сетей связи, находящихся под юрисдикцией иностранных государств, а также о внесении изменений в некоторые акты Правительства Российской Федерации».

Постановление Правительства РФ от 19.11.2014 № 1222 «О дальнейшем развитии единой системы межведомственного электронного взаимодействия».

Постановление Правительства РФ от 24.11.2014 № 1240 «О некоторых вопросах по обеспечению использования сети передачи данных органов власти».

Постановление Правительства РФ от 25.12.2014 № 1494 «Об утверждении Правил обмена документами в электронном виде при организации информационного взаимодействия».

2015

Постановление Правительства РФ от 30.01.2015 № 83 «О проведении оценки фактического воздействия нормативных правовых актов, а также о внесении изменений в некоторые акты Правительства Российской Федерации» (вместе с «Правилами проведения оценки фактического воздействия нормативных правовых актов»).

Постановление Правительства РФ от 17.06.2015 № 602 «О некоторых мерах по совершенствованию информатизации в сфере кадрового обеспечения государственных органов и органов местного самоуправления».

Постановление Правительства РФ от 30.06.2015 № 658 «О государственной интегрированной информационной системе управления общественными финансами “Электронный бюджет” (вместе с «Положением о государственной интегрированной информационной системе управления общественными финансами “Электронный бюджет”»).

Постановление Правительства РФ от 06.07.2015 № 675 «О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона «Об информации, информационных технологиях и о защите информации» (вместе с «Правилами осуществления контроля за размещением технических средств информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями, государственными и муниципальными учреждениями, на территории Российской Федерации», «Правилами осуществления контроля за соблюдением требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»).

Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

Постановление Правительства РФ от 17.07.2015 № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации».

Постановление Правительства РФ от 23.07.2015 № 748 «О создании, развитии и эксплуатации аналитической информационной системы обеспечения открытости деятельности федеральных органов исполнительной власти, размещенной в информационно-телекоммуникационной сети “Интернет” (www.programs.gov.ru)» (вместе с «Положением о создании, развитии и эксплуатации аналитической информационной системы обеспечения открытости деятельности федеральных органов исполнительной власти, размещенной в информационно-телекоммуникационной сети “Интернет” (www.programs.gov.ru)»).

Постановление Правительства РФ от 04.08.2015 № 785 «О Правительственной комиссии по импортозамещению» (вместе с «Положением о Правительственной комиссии по импортозамещению»).

Постановление Правительства Российской Федерации от 04.09.2015 № 789 «Об утверждении Правил разработки, корректировки, осуществления мониторинга и контроля реализации основных направлений деятельности Правительства Российской Федерации».

Постановление Правительства РФ от 14.11.2015 № 1235 «О федеральной государственной информационной системе координации

информатизации» (вместе с «Положением о федеральной государственной информационной системе координации информатизации»).

Постановление Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (вместе с «Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств — членов Евразийского экономического союза, за исключением Российской Федерации», «Порядком подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств (за исключением программного обеспечения, включенного в единый реестр программ для электронных вычислительных машин и баз данных из государств — членов Евразийского экономического союза, за исключением Российской Федерации), для целей осуществления закупок для обеспечения государственных и муниципальных нужд»).

2016

Постановление Правительства РФ от 26.03.2016 № 236 «О требованиях к предоставлению в электронной форме государственных и муниципальных услуг».

Постановление Правительства РФ от 05.05.2016 № 392 «О приоритетных направлениях использования и развития информационно-коммуникационных технологий в федеральных органах исполнительной власти и органах управления государственными внебюджетными фондами и о внесении изменений в некоторые акты Правительства Российской Федерации».

Постановление Правительства Российской Федерации от 06.05.2016 № 399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса».

Постановление Правительства РФ от 01.06.2016 № 487 «О первоочередных мерах, направленных на создание государственной информационной системы “Единая информационная среда в сфере систематизации и кодирования информации”».

Постановление Правительства РФ от 09.06.2016 № 516 «Об утверждении Правил осуществления взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти, органами местного самоуправления, с организациями, осу-

ществляющими в соответствии с федеральными законами отдельные публичные полномочия».

Постановление Правительства РФ от 27.06.2016 № 584 «Об особенностях применения профессиональных стандартов в части требований, обязательных для применения государственными внебюджетными фондами Российской Федерации, государственными или муниципальными учреждениями, государственными или муниципальными унитарными предприятиями, а также государственными корпорациями, государственными компаниями и хозяйственными обществами, более пятидесяти процентов акций (долей) в уставном капитале которых находится в государственной собственности или муниципальной собственности».

Постановление Правительства Российской Федерации от 16.09.2016 № 925 «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами».

Постановление Правительства РФ от 30.12.2016 № 1559 «Об утверждении Правил общественного обсуждения проектов документов стратегического планирования по вопросам, находящимся в ведении Правительства Российской Федерации, с использованием федеральной информационной системы стратегического планирования».

2017

Постановление Правительства РФ от 14.02.2017 № 181 «О Единой государственной информационной системе социального обеспечения» (вместе с «Положением о Единой государственной информационной системе социального обеспечения», «Порядком предоставления информации в Единую государственную информационную систему социального обеспечения»).

Постановление Правительства РФ от 03.03.2017 № 256 «О федеральной государственной информационной системе «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации».

Постановление Правительства РФ от 23.03.2017 г. № 325 «Об утверждении дополнительных требований к программам для электронных вычислительных машин и баз данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных».

Постановление Правительства РФ от 30.05.2017 № 667 «Об установлении особенностей оформления виз в форме электронного документа и въезда в Российскую Федерацию на основании виз в форме электронного документа граждан иностранных государств, прибывающих

в Российскую Федерацию через пункты пропуска через государственную границу Российской Федерации, расположенные на территории свободного порта Владивосток, через воздушные пункты пропуска через государственную границу Российской Федерации, расположенные на территории Дальневосточного федерального округа, и о внесении изменений в Положение о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность».

Постановление Правительства РФ от 14.07.2017 № 839 «О федеральной государственной информационной системе “Федеральный ситуационный центр электронного правительства” и внесении изменений в Положение о единой системе межведомственного электронного взаимодействия».

Постановление Правительства РФ от 30.12.2017 № 1710 «Об утверждении государственной программы Российской Федерации “Обеспечение доступным и комфортным жильем и коммунальными услугами граждан Российской Федерации”».

2018

Постановление Правительства РФ от 17.01.2018 № 16 «Об утверждении Положения о создании и функционировании советов по приоритетным направлениям научно-технологического развития Российской Федерации».

Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Постановление Правительства РФ от 12.04.2018 № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями».

Постановление Правительства РФ от 21.04.2018 № 482 «О государственной информационной системе “Типовое облачное решение по автоматизации контрольной (надзорной) деятельности”» (вместе с «Положением о государственной информационной системе “Типовое облачное решение по автоматизации контрольной (надзорной) деятельности”»).

Постановление Правительства РФ от 05.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения» (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения»).

Постановление Правительства Российской Федерации от 08.06.2018 № 656 «О требованиях к операторам электронных площадок, операторам специализированных электронных площадок, электронным площадкам, специализированным электронным площадкам и функционированию электронных площадок, специализированных электронных площадок, подтверждении соответствия таким требованиям, об утрате юридическим лицом статуса оператора электронной площадки, оператора специализированной электронной площадки».

Постановление Правительства РФ от 08.06.2018 № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности» (вместе с «Правилами взаимодействия Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации с федеральными органами исполнительной власти, руководство деятельностью которых осуществляет Правительство Российской Федерации, при планировании и осуществлении централизованных закупок офисного программного обеспечения и программного обеспечения в сфере информационной безопасности, а также взаимодействия Федерального казначейства с федеральными органами исполнительной власти, руководство деятельностью которых осуществляет Правительство Российской Федерации, и подведомственными им федеральными казенными учреждениями при планировании и осуществлении централизованных закупок программного обеспечения для ведения бюджетного учета»).

Постановление Правительства РФ от 26.06.2018 № 728 «Об утверждении Правил хранения организатором распространения информации в информационно-телекоммуникационной сети “Интернет” текстовых сообщений пользователей информационно-телекоммуникационной сети “Интернет”, голосовой информации, изображений, звуков, видео-, иных электронных сообщений пользователей информационно-телекоммуникационной сети “Интернет”».

Постановление Правительства РФ от 29.06.2018 № 747 «Об установлении требований к фиксированию действий при размещении в электронной форме в единой системе идентификации и аутентификации сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, и иных сведений, предусмотренных федеральными законами, а также при размещении биометрических персональных данных гражданина Российской Федерации в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных

данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации».

Постановление Правительства РФ от 29.06.2018 № 748 «О требованиях к банкам (включая требования к их финансовой устойчивости), в которых участниками закупок открываются специальные счета, на которые вносятся денежные средства, предназначенные для обеспечения заявок на участие в закупках товаров, работ, услуг, и признании утратившими силу некоторых актов Правительства Российской Федерации».

Постановление Правительства РФ от 30.06.2018 № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации».

Постановление Правительства РФ от 14.07.2018 № 820 «Об установлении требований к проведению идентификации гражданина Российской Федерации государственными органами и организациями, осуществляющими размещение в электронной форме в единой системе идентификации и аутентификации сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, и иных сведений, предусмотренных федеральными законами, а также размещающими сведения в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации».

Постановление Правительства РФ от 28.07.2018 № 881 «Об установлении требований к эксплуатации государственной информационной системы, указанной в части 13 статьи 4 Федерального закона “О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд”, порядку формирования, хранения и использования содержащейся в ней информации».

Постановление Правительства РФ от 28.07.2018 № 882 «Об утверждении Правил мониторинга доступности (работоспособности) единой информационной системы в сфере закупок, электронной площадки».

Постановление Правительства РФ от 28.07.2018 № 883 «Об утверждении Правил фиксации, включая видеофиксацию, в режиме реального времени действий, бездействия участников контрактной системы в сфере закупок в единой информационной системе в сфере закупок, на электронной площадке».

Постановление Правительства РФ от 23.08.2018 № 984 «Об утверждении Правил подтверждения степени секретности сведений, с которыми предприятия, учреждения и организации предполагают проводить работы, связанные с использованием сведений, составляющих государственную тайну, и о внесении изменения в пункт 5 Положения о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».

Постановление Правительства РФ от 07.09.2018 № 1065 «О Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности» (вместе с «Положением о Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности»).

Постановление Правительства РФ от 31.10.2018 № 1288 «Об организации проектной деятельности в Правительстве Российской Федерации» (вместе с «Положением об организации проектной деятельности в Правительстве Российской Федерации»).

Постановление Правительства РФ от 08.11.2018 № 1335 «Об утверждении Правил осуществления федеральными органами исполнительной власти, осуществляющими функции и полномочия учредителя в отношении федеральных государственных учреждений, права собственника имущества федеральных государственных унитарных предприятий, ведомственного контроля за соблюдением требований Федерального закона “О закупках товаров, работ, услуг отдельными видами юридических лиц” и иных принятых в соответствии с ним нормативных правовых актов Российской Федерации».

2019

Постановление Правительства РФ от 13.02.2019 № 136 «О Центре мониторинга и управления сетью связи общего пользования».

Постановление Правительства РФ от 19.02.2019 № 162 «Об утверждении Правил разработки, утверждения, реализации, корректировки и завершения комплексных научно-технических программ полного инновационного цикла и комплексных научно-технических проектов полного инновационного цикла в целях обеспечения реализации приоритетов научно-технологического развития Российской Федерации».

Постановление Правительства РФ от 02.03.2019 № 234 «О системе управления реализацией национальной программы “Цифровая экономика Российской Федерации”» (вместе с «Положением о системе

управления реализацией национальной программы “Цифровая экономика Российской Федерации”»).

Постановление Правительства РФ от 29.03.2019 № 377 «Об утверждении государственной программы Российской Федерации “Научно-технологическое развитие Российской Федерации”».

Постановление Правительства РФ от 26.04.2019 № 518 «Об определении федерального органа исполнительной власти, уполномоченного на обеспечение эксплуатации и развития государственной информационной системы, указанной в части 13 статьи 4 Федерального закона “О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд”, а также на предоставление информации, содержащейся в ней».

Постановление Правительства РФ от 30.04.2019 № 528 «Об утверждении Правил предоставления из федерального бюджета субсидии на создание и функционирование Центра мониторинга и управления сетью связи общего пользования, а также создание, эксплуатацию и развитие информационной системы мониторинга и управления сетью связи общего пользования».

Постановление Правительства РФ от 30.04.2019 № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции».

Постановление Правительства РФ от 30.04.2019 № 542 «О внесении изменений в Положение о Правительственной комиссии по импортозамещению»¹.

Постановление Правительства РФ от 03.05.2019 № 550 «Об утверждении Правил предоставления субсидий из федерального бюджета на поддержку проектов по преобразованию приоритетных отраслей экономики и социальной сферы на основе внедрения отечественных продуктов, сервисов и платформенных решений, созданных на базе “сквозных” цифровых технологий».

Постановление Правительства РФ от 03.05.2019 № 551 «О государственной поддержке программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных “сквозных” цифровых технологий».

Постановление Правительства РФ от 03.05.2019 № 553 «Об утверждении Правил предоставления субсидии из федерального бюджета федеральному государственному бюджетному учреждению “Фонд со-

¹ Положение о Правительственной комиссии по импортозамещению, утверждено постановлением Правительства Российской Федерации от 4 августа 2015 г. № 785 «О Правительственной комиссии по импортозамещению».

действия развитию малых форм предприятий в научно-технической сфере” на предоставление грантов физическим лицам на реализацию проектов в области цифровой экономики».

Постановление Правительства РФ от 03.05.2019 № 554 «Об утверждении Правил предоставления субсидии из федерального бюджета некоммерческой организации на предоставление грантов юридическим лицам на финансовое обеспечение проектов в целях реализации национальной программы “Цифровая экономика Российской Федерации”».

Постановление Правительства РФ от 03.05.2019 № 555 «Об утверждении Правил предоставления субсидии в рамках поддержки проектов по преобразованию приоритетных отраслей экономики и социальной сферы на основе внедрения отечественных продуктов, сервисов и платформенных решений, созданных на базе “сквозных” цифровых технологий».

Постановление Правительства РФ от 10.07.2019 № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, о внесении изменений в постановление Правительства Российской Федерации от 16 сентября 2016 г. № 925 и признании утратившими силу некоторых актов Правительства Российской Федерации» (вместе с «Правилами формирования и ведения единого реестра Российской радиоэлектронной продукции», «Порядком подготовки обоснования невозможности соблюдения ограничения на допуск радиоэлектронной продукции, происходящей из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»).

Постановление Правительства РФ от 17.07.2019 № 903 «Об утверждении Правил формирования сводного годового доклада о ходе реализации и оценке эффективности государственных программ Российской Федерации, внесении изменений в некоторые акты Правительства Российской Федерации и признании утратившими силу отдельных положений некоторых актов Правительства Российской Федерации».

Постановление Правительства РФ от 11.09.2019 № 1185 «Об утверждении Правил предоставления субсидии из федерального бюджета российскому юридическому лицу в целях реализации отдельных мероприятий федерального проекта “Информационная безопасность” национальной программы “Цифровая экономика Российской Федерации”».

Постановление Правительства РФ от 21.09.2019 № 1234 «О внесении изменений в Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

Постановление Правительства РФ от 07.10.2019 № 1285 «Об утверждении Правил предоставления субсидий из федерального бюд-

жета на создание отраслевого центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах».

Постановление Правительства РФ от 11.10.2019 № 1311 «Об утверждении Правил ведения реестра точек обмена трафиком».

Постановление Правительства РФ от 12.10.2019 № 1316 «Об утверждении Положения о проведении учений по обеспечению устойчивого, безопасного и целостного функционирования на территории Российской Федерации информационно-телекоммуникационной сети “Интернет” и сети связи общего пользования».

Постановление Правительства РФ от 12.10.2019 № 1320 «Об утверждении Правил предоставления субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности».

Постановление Правительства РФ от 26.10.2019 № 1375 «О порядке контроля за выполнением лицами, участвующими в централизованном управлении сетью связи общего пользования, обязанностей по размещению на территории Российской Федерации средств связи, с использованием которых выполняются указания в рамках централизованного управления сетью связи общего пользования».

Постановление Правительства РФ от 29.10.2019 № 1382 «Об утверждении Правил предоставления субсидий из федерального бюджета на достижение отдельных результатов федерального проекта “Информационная безопасность” национальной программы “Цифровая экономика Российской Федерации”».

Постановление Правительства РФ от 29.10.2019 № 1385 «Об утверждении Правил взаимодействия собственников или иных владельцев технологических сетей связи, имеющих уникальный идентификатор совокупности средств связи и иных технических средств в информационно-телекоммуникационной сети “Интернет”, с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации».

Постановление Правительства РФ от 31.10.2019 № 1395 «О внесении изменений в Правила предоставления грантов в форме субсидий из федерального бюджета, выделяемых для государственной поддержки научных исследований, проводимых под руководством ведущих ученых в российских образовательных организациях высшего образования, научных учреждениях и государственных научных центрах Российской Федерации».

Постановление Правительства РФ от 05.11.2019 № 1401 «О типовых формах заявок на участие в электронных процедурах, закрытых

электронных процедурах, требованиях к содержанию, составу, порядку разработки типовой документации о закупке и внесении изменения в дополнительные требования к операторам электронных площадок, операторам специализированных электронных площадок и функционированию электронных площадок, специализированных электронных площадок».

Постановление Правительства РФ от 09.11.2019 № 1438 «Об утверждении Правил предоставления в 2019 году иных межбюджетных трансфертов из федерального бюджета бюджетам субъектов Российской Федерации в целях софинансирования расходных обязательств субъектов Российской Федерации, возникающих при реализации региональных проектов, обеспечивающих достижение целей, показателей и результата федерального проекта «Информационная инфраструктура» национальной программы «Цифровая экономика Российской Федерации»».

Постановление Правительства РФ от 05.12.2019 № 1598 «Об утверждении Правил предоставления из федерального бюджета субсидий в рамках поддержки проектов по преобразованию приоритетных отраслей экономики и социальной сферы на основе внедрения отечественных продуктов, сервисов и платформенных решений, созданных на базе «сквозных» цифровых технологий, с применением льготного кредитования».

Постановление Правительства РФ от 21.12.2019 № 1746 «Об установлении запрета на допуск отдельных видов товаров, происходящих из иностранных государств, и внесении изменений в некоторые акты Правительства Российской Федерации».

Постановление Правительства РФ от 21.12.2019 № 1752 «Об утверждении Правил предоставления субсидий из федерального бюджета на реализацию мероприятий по разработке цифровых учебно-методических комплексов, учебных симуляторов, тренажеров, виртуальных лабораторий для реализации основных общеобразовательных программ, дополнительных общеобразовательных программ и образовательных программ среднего профессионального образования по предметным областям «Математика», «Информатика» и «Технология» федерального проекта «Кадры для цифровой экономики» национальной программы «Цифровая экономика Российской Федерации» государственной программы Российской Федерации «Развитие образования»».

8. Распоряжения Правительства Российской Федерации

Распоряжение Правительства РФ от 24.07.1992 № 1344-р «О создании информационной системы по внешнеполитическим вопросам».

Распоряжение Правительства РФ от 27.09.2004 № 1244-р «О Концепции использования информационных технологий в деятельности

федеральных органов государственной власти до 2010 года и плане мероприятий по ее реализации».

Распоряжение Правительства РФ от 02.10.2009 № 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти».

Распоряжение Правительства РФ от 11.11.2010 № 1950-р «Об утверждении перечня государственных программ Российской Федерации».

Распоряжение Правительства РФ от 20.07.2011 № 1275-р «О Концепции создания и развития государственной интегрированной информационной системы управления общественными финансами “Электронный бюджет”».

Распоряжение Правительства РФ от 08.12.2011 № 2227-р «Об утверждении Стратегии инновационного развития Российской Федерации на период до 2020 года».

Распоряжение Правительства РФ от 01.11.2013 № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года».

Распоряжение Правительства РФ от 25.12.2013 № 2516-р «Об утверждении Концепции развития механизмов предоставления государственных и муниципальных услуг в электронном виде».

Распоряжение Правительства РФ от 30 декабря 2013 года № 2602-р «Об утверждении плана мероприятий (“дорожной карты”) “Развитие отрасли информационных технологий”».

Распоряжение Правительства РФ от 10.05.2014 № 793-р «Об утверждении Концепции методологии систематизации и кодирования информации, а также совершенствования и актуализации общероссийских классификаторов, реестров и информационных ресурсов».

Распоряжение Правительства РФ от 29.12.2014 № 2769-р «Об утверждении Концепции региональной информатизации».

Распоряжение Правительства РФ от 02.04.2015 № 583-р «Об утверждении Перечня видов документов, предусмотренного Правилами обмена документами в электронном виде при организации информационного взаимодействия, утв. постановлением Правительства РФ от 25.12.2014 № 1494».

Распоряжение Правительства РФ от 20.08.2015 № 1616-р «Об утверждении Концепции оптимизации механизмов проектирования и реализации межведомственного информационного взаимодействия, оптимизации порядка разработки и утверждения административных регламентов в целях создания системы управления изменениями».

Распоряжение Правительства РФ от 07.10.2015 № 1995-р «Об утверждении Концепции перевода обработки и хранения государствен-

ных информационных ресурсов, не содержащих сведения, составляющие государственную тайну, в систему федеральных и региональных центров обработки данных».

Распоряжение Правительства РФ от 19.04.2016 № 724-р «Об утверждении перечня документов и (или) информации, запрашиваемых и получаемых в рамках межведомственного информационного взаимодействия органами государственного контроля (надзора), органами муниципального контроля при организации и проведении проверок от иных государственных органов, органов местного самоуправления либо подведомственных государственным органам или органам местного самоуправления организаций, в распоряжении которых находятся эти документы и (или) информация».

Распоряжение Правительства РФ от 26.07.2016 № 1588-р «Об утверждении плана перехода в 2016–2018 годах федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения».

Распоряжение Правительства РФ от 04.07.2017 № 1418-р «Об утверждении Концепции формирования и ведения единого федерального информационного ресурса, содержащего сведения о населении Российской Федерации» (вместе с «Планом мероприятий (“дорожной картой”) по формированию и ведению единого федерального информационного ресурса, содержащего сведения о населении Российской Федерации”»).

Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы “Цифровая экономика Российской Федерации”».

Распоряжение Правительства РФ от 09.03.2018 № 403-р «О выделении Минэкономразвития России из резервного фонда Правительства Российской Федерации в 2018 году бюджетных ассигнований на реализацию плана мероприятий по направлению “Нормативное регулирование” программы “Цифровая экономика Российской Федерации”».

Распоряжение Правительства РФ от 12.07.2018 № 1447-р «Об утверждении перечней операторов электронных площадок и специализированных электронных площадок, предусмотренных Федеральными законами от 05.04.2013 № 44-ФЗ, от 18.07.2011 № 223-ФЗ».

Распоряжение Правительства РФ от 30.09.2018 № 2101-р «Об утверждении комплексного плана модернизации и расширения магистральной инфраструктуры на период до 2024 года».

Распоряжение Правительства РФ от 14.08.2019 № 1797-р «Об утверждении Стратегии развития экспорта услуг до 2025 года» (вместе с «Планом мероприятий по реализации Стратегии развития экспорта услуг до 2025 года»).

Распоряжение Правительства РФ от 28.08.2019 № 1911-р «Об утверждении Концепции создания государственной единой облачной платформы».

Распоряжение Правительства РФ от 17.12.2019 № 3074-р «Концепция создания цифровой аналитической платформы».

9. Основные направления деятельности Правительства Российской Федерации

Основные направления деятельности Правительства Российской Федерации на период до 2024 года — утверждены 29 сентября 2018 г.

10. Руководящие документы ФОИВ

10.1. Документы ФСБ России

Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных — утверждены ФСБ РФ 21.02.2008 № 149/6/6-622.

Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (вместе с «Положением о Национальном координационном центре по компьютерным инцидентам»).

Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъ-

ектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».

Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации».

Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».

10.2. Документы ФСО России

Приказ ФСО России от 07.09.2016 № 443 «Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети “Интернет”».

10.3. Документы ФСТЭК России¹/Государственной технической комиссии при Президенте Российской Федерации / Федерального агентства правительственной связи и информации при Президенте Российской Федерации

Положение о государственном лицензировании деятельности в области защиты информации Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10 (с изменениями и дополнениями от 24 июня 1997 г. № 60).

Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено Приказом пред-

¹ Полный перечень документов ФСТЭК России представлен на сайте этого ведомства в разделе «Документы».

седателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199.

Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.

Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.

Руководящий документ Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Руководящий документ Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Руководящий документ Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.

Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114),

Методический документ. Профиль защиты средств антивирусной защиты типа «А» четвертого класса защиты. ИТ.САВЗАУ.ПЗ. Утверждены ФСТЭК России 14.06.2012 г.

Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».

Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов кри-

тической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Приказ ФСТЭК России от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

Информационное сообщение ФСТЭК России от 24.08.2018 № 240/25/3752 «По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

Приказ ФСТЭК России от 09.11.2018 № 201 «Об утверждении Правил осуществления контроля за выполнением государственного задания на выполнение государственных работ федеральным автономным учреждением “Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю”».

Приказ ФСТЭК России от 21.02.2019 № 40 «Об утверждении Программы профилактики нарушений обязательных требований, соблюдение которых оценивается при проведении ФСТЭК России мероприятий по контролю в рамках федерального государственного контроля за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации и деятельности по разработке и производству средств защиты конфиденциальной информации, на 2019 год».

Приказ ФСТЭК России от 28.05.2019 № 106 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17».

Приказ ФСТЭК России от 16.07.2019 № 135 «Перечень нормативных правовых актов или их отдельных частей, оценка соблюдения которых является предметом государственного контроля (надзора) в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

10.4. Документы Счетной палаты Российской Федерации

СГА 305. Стандарт внешнего государственного аудита (контроля). Аудит федеральных информационных систем и проектов» (утв. постановлением Коллегии Счетной палаты РФ от 23.12.2016 № 11ПК).

11. Приказы Мининформсвязи¹ / Минкомсвязи России

Приказ Мининформсвязи России от 09.01.2008 № 1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации».

Приказ Минкомсвязи России от 02.09.2011 № 221 «Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения».

Приказ Минкомсвязи России от 19.01.2015 № 7 «Об утверждении Положения о федеральной государственной информационной системе “Единая система нормативной справочной информации”, а также Перечня нормативной справочной информации, подлежащей размещению в федеральной государственной информационной системе “Единая система нормативной справочной информации”».

Приказ Минкомсвязи России от 01.04.2015 № 96 «Об утверждении плана импортозамещения программного обеспечения».

Приказ Минкомсвязи России от 23.06.2015 № 210 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия».

Приказ Минкомсвязи России от 31.12.2015 № 621 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных».

Приказ Минкомсвязи России от 11.02.2016 № 44 «Об утверждении правил размещения информации в федеральной государственной информационной системе координации информатизации».

Приказ Минкомсвязи России от 11.08.2016 № 375 «Об утверждении порядка внесения сведений о выполнении требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, а также состава сведений, которые подлежат внесению, и срока их представления».

Приказ Минкомсвязи России от 30.12.2016 № 745 «Об утверждении рекомендаций по согласованию с Министерством связи и массо-

¹ С 13 мая 2008 г. в соответствии с пунктом 5 Указа Президента РФ от 12 мая 2008 г. № 724 «Вопросы системы и структуры федеральных органов исполнительной власти» Мининформсвязи России преобразовано в Министерство связи и массовых коммуникаций Российской Федерации (Минкомсвязь России). Согласно Указу Президента РФ от 15 мая 2018 г. № 215 «О структуре федеральных органов исполнительной власти» Министерство связи и массовых коммуникаций Российской Федерации переименовано в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

вых коммуникаций Российской Федерации предлагаемых главными распорядителями средств федерального бюджета изменений в сводную бюджетную роспись федерального бюджета и лимиты бюджетных обязательств по бюджетным ассигнованиям, предусмотренным на закупку товаров, работ, услуг в сфере информационно-коммуникационных технологий».

Приказ Минкомсвязи России от 29.06.2017 № 334 «Об утверждении методических рекомендаций по переходу федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения».

Приказ Минкомсвязи России от 29.09.2017 № 520 «Об утверждении Плана-графика перехода Министерства связи и массовых коммуникаций Российской Федерации на использование отечественного офисного программного обеспечения на период 2017–2018 годов и на плановый период до 2020 года».

Приказ Минкомсвязи России от 14.02.2018 № 64 «Об утверждении плана информатизации Министерства связи и массовых коммуникаций Российской Федерации на 2018 год и плановый период 2019 и 2020 годов» (вместе с «Планом информатизации на очередной финансовый 2018 год и плановый период 2019–2020 годов»).

Приказ Минкомсвязи России от 21.06.2018 № 307 «Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданами Российской Федерации, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»».

Приказ Минкомсвязи России от 25.06.2018 № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации».

Приказ Минкомсвязи России от 25.06.2018 № 322 «Об определении размера платы, взимаемой оператором единой информационной

системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, за предоставление банкам, соответствующим критериям, установленным абзацами вторым — четвертым пункта 5.7 статьи 7 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», информации о степени соответствия предоставленных биометрических персональных данных биометрическим персональным данным клиента-физического лица, содержащимся в указанной системе».

Приказ Минкомсвязи России от 25.06.2018 № 323 «Об утверждении форм подтверждения соответствия информационных технологий и технических средств, предназначенных для обработки биометрических персональных данных в целях проведения идентификации, требованиям к информационным технологиям и техническим средствам, предназначенным для указанных целей».

Приказ Минкомсвязи России от 04.07.2018 № 335 «Об утверждении методических рекомендаций по переходу органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления муниципальных образований Российской Федерации на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения».

Приказ Минкомсвязи России от 05.07.2018 № 346 «Об отказе во включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных».

Приказ Минкомсвязи России от 05.07.2018 № 347 «О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных».

Приказ Минкомсвязи России от 13.08.2018 № 397 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей».

Приказ Минкомсвязи России от 21.08.2018 № 415 «О внесении изменений в приказ Министерства связи и массовых коммуникаций Российской Федерации от 14.02.2018 № 64 «Об утверждении плана информатизации Министерства связи и массовых коммуникаций Российской Федерации на 2018 год и плановый период 2019 и 2020 годов»».

Приказ Минкомсвязи России от 18.09.2018 № 475 «О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных».

Приказ Минкомсвязи России от 20.09.2018 № 486 «Об утверждении методических рекомендаций по переходу государственных компаний

на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения».

Приказ Минкомсвязи России от 19.12.2018 № 722 «Об утверждении порядка и методики подтверждения соответствия программ для электронных вычислительных машин и баз данных, сведения о которых включены в реестр российского программного обеспечения, дополнительным требованиям, установленным к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, утвержденным постановлением Правительства Российской Федерации от 23 марта 2017 г. № 325, и о внесении изменений в Положение об Экспертном совете по российскому программному обеспечению при Министерстве связи и массовых коммуникаций Российской Федерации, утвержденное приказом Министерства связи и массовых коммуникаций Российской Федерации от 20 июня 2016 г. № 269».

Приказ Минкомсвязи России от 21.01.2019 № 10 «Об утверждении Программы профилактики нарушений обязательных требований, которые установлены Федеральным законом “Об электронной подписи”, на 2019 год».

Приказ Минкомсвязи России от 30.01.2019 № 22 «Об утверждении плана деятельности Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации на период 2019–2024 годов»¹.

Приказ Минкомсвязи России от 05.03.2019 № 84 «Об утверждении Положения об Экспертном совете по программному обеспечению при Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации».

Приказ Минкомсвязи России от 03.06.2019 № 252 «Об утверждении Единых функционально-технических требований по автоматизации приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода».

Приказ Минкомсвязи России от 13.08.2019 № 454 «О внесении изменения в методику подтверждения соответствия программ для электронных вычислительных машин и баз данных, сведения о которых включены в реестр российского программного обеспечения, дополнительным требованиям, установленным к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, утвержденным Постановлением Правительства Российской Федерации от 23 марта

¹ Направление 5.3. Обеспечение защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности в условиях цифровой экономики.

2017 г. № 325, утвержденную Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 19 декабря 2018 г. № 722».

Приказ Минкомсвязи России от 16.09.2019 № 510 «Об утверждении требований к функционированию технических и программных средств (в том числе средств связи), используемых в целях выявления в информационно-телекоммуникационной сети “Интернет” сетевых адресов, соответствующих доменным именам».

Приказ Минкомсвязи России от 08.10.2019 № 576 «Об утверждении порядка отбора получателей грантов в рамках конкурсных отборов, инициированных в 2019 году, во исполнение постановления Правительства Российской Федерации от 3 мая 2019 г. № 550 “Об утверждении Правил предоставления субсидии из федерального бюджета на государственную поддержку проектов по внедрению отечественных продуктов, сервисов и платформенных решений, созданных на базе “сквозных” цифровых технологий, в субъектах Российской Федерации в рамках реализации дорожных карт по направлениям развития “сквозных” цифровых технологий” и максимального размера гранта, предоставляемого одному получателю гранта».

Приказ Минкомсвязи России от 08.10.2019 № 577 «Об утверждении формы соглашения о предоставлении гранта на государственную поддержку проектов по внедрению отечественных продуктов, сервисов и платформенных решений, созданных на базе “сквозных” цифровых технологий, в субъектах Российской Федерации в рамках реализации дорожных карт по направлениям развития “сквозных” цифровых технологий».

Приказ Минкомсвязи России от 09.10.2019 № 579 «Об утверждении требований к обеспечению устойчивого функционирования средств связи, обеспечивающих взаимодействие со средствами связи других операторов связи, собственников или иных владельцев технологических сетей связи, в том числе находящихся за пределами территории Российской Федерации».

Приказ Минкомсвязи России от 09.10.2019 № 580 «Об утверждении Требований к комплексам мероприятий, имеющих высокую социально-экономическую значимость для субъекта Российской Федерации, направленных на разработку и (или) внедрение отечественных продуктов, сервисов и платформенных решений, созданных на базе “сквозных” цифровых технологий, во взаимосвязи с приоритетами, технологиями и субтехнологиями, определенными дорожными картами по направлениям развития “сквозных” цифровых технологий (региональным проектам)».

Приказ Минкомсвязи России от 10.10.2019 № 582 «Об утверждении требований к функционированию систем управления сетями связи

при возникновении угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети “Интернет” и сети связи общего пользования».

Приказ Минкомсвязи России от 30.10.2019 № 634 «О комиссии по отбору получателей грантов на реализацию проектов по разработке отечественного программного обеспечения и увеличению его доли в условиях цифровой экономики, а также по разработке технологических решений по созданию федеральных и региональных государственных информационных ресурсов с использованием технологии распределенных реестров, внедрением методов и технологий обработки и хранения информации».

Приказ Минкомсвязи России от 30.10.2019 № 635 «Об утверждении порядка конкурсного отбора получателей грантов на реализацию проектов по разработке отечественного программного обеспечения и увеличению его доли в условиях цифровой экономики, а также по разработке технологических решений по созданию федеральных и региональных государственных информационных ресурсов с использованием технологии распределенных реестров, внедрением методов и технологий обработки и хранения информации».

Приказ Минкомсвязи России от 11.11.2019 № 707 «О внесении изменений в приказ “Об утверждении Единых функционально-технических требований по автоматизации приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода”».

(вместе с «Положением о конкурсной комиссии Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по проведению конкурсного отбора на предоставление Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации субсидий из федерального бюджета на достижение отдельных результатов федерального проекта “Информационная безопасность” национальной программы “Цифровая экономика Российской Федерации”, «Порядком рассмотрения конкурсной комиссией Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по проведению конкурсного отбора на предоставление Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации субсидий из федерального бюджета на достижение отдельных результатов федерального проекта “Информационная безопасность” национальной программы “Цифровая экономика Российской Федерации” поданных на конкурсный отбор заявок»).

Приказ Минкомсвязи России от 10.12.2019 № 827 «Об утверждении рекомендуемых форм сублицензионного договора на предоставление права использования (неисключительных лицензий) офисного программного обеспечения и программного обеспечения в сфере

информационной безопасности федеральным органам исполнительной власти и направления информации о выявленных недостатках поставленного офисного программного обеспечения и программного обеспечения в сфере информационной безопасности или с предложением по совершенствованию используемого офисного программного обеспечения и программного обеспечения в сфере информационной безопасности при осуществлении централизованных закупок офисного программного обеспечения и программного обеспечения в сфере информационной безопасности».

11.1. Приказы Роскомнадзора

Приказ Роскомнадзора от 29.07.2019 № 216 «Об определении перечня групп доменных имен, составляющих российскую национальную доменную зону».

Приказ Роскомнадзора от 31.07.2019 № 219 «Об утверждении Порядка контроля за соблюдением собственниками или иными владельцами точек обмена трафиком запрета на подключение к точкам обмена трафиком сетей связи, владельцы которых не соблюдают установленные законодательством Российской Федерации требования».

Приказ Роскомнадзора от 31.07.2019 № 220 «Об утверждении порядка предоставления операторам связи, собственникам или иным владельцам технологических сетей связи, имеющим уникальный идентификатор совокупности средств связи и иных технических средств в информационно-телекоммуникационной сети “Интернет”, технических средств контроля за соблюдением указанными лицами требований Федерального закона “Об информации, информационных технологиях и о защите информации” и Федерального закона “О связи”, предусматривающих ограничение доступа к информации, а также требований к таким техническим средствам, их установке и эксплуатации».

Приказ Роскомнадзора от 31.07.2019 № 221 «Об утверждении сроков, порядка, состава и формата представления операторами связи, собственниками или иными владельцами технологических сетей связи, организаторами распространения информации в информационно-телекоммуникационной сети “Интернет”, а также иными лицами, имеющими уникальный идентификатор совокупности средств связи и иных технических средств в информационно-телекоммуникационной сети “Интернет”, в электронной форме информации, предусмотренной подпунктом 4 пункта 8 статьи 56.2 Федерального закона от 7 июля 2003 г. № 126-ФЗ “О связи”».

Приказ Роскомнадзора от 31.07.2019 № 222 «Об утверждении сроков, порядка, состава и формата представления операторами связи, собственниками или иными владельцами технологических сетей связи, иными лицами при использовании линий связи, пересекающих Государственную границу Российской Федерации, информации

в электронной форме о средствах связи, обеспечивающих взаимодействие с такими линиями связи, в том числе через иные линии связи».

Приказ Роскомнадзора от 31.07.2019 № 223 «Об утверждении сроков, порядка, состава и формата представления собственниками или иными владельцами линий связи, пересекающих Государственную границу Российской Федерации, в электронной форме информации о цели использования линии связи, а также о средствах связи, установленных на указанной линии связи».

Приказ Роскомнадзора от 31.07.2019 № 224 «Об утверждении Правил маршрутизации сообщений электросвязи в случае осуществления централизованного управления сетью связи общего пользования».

Приказ Роскомнадзора от 31.07.2019 № 226 «Об утверждении Порядка контроля за соблюдением операторами связи, собственниками или иными владельцами технологических сетей связи, организаторами распространения информации в информационно-телекоммуникационной сети “Интернет”, имеющими уникальный идентификатор совокупности средств связи и иных технических средств в информационно-телекоммуникационной сети “Интернет”, обязанности использования точек обмена трафиком, сведения о которых содержатся в реестре точек обмена трафиком, для взаимодействия с имеющими уникальный идентификатор совокупности средств связи и иных технических средств в информационно-телекоммуникационной сети “Интернет” операторами связи, собственниками или иными владельцами технологических сетей связи, иными лицами для передачи сообщений электросвязи».

Приказ Роскомнадзора от 31.07.2019 № 227 «Об утверждении Порядка контроля за достоверностью и полнотой информации о цели использования пересекающей Государственную границу Российской Федерации линии связи, а также о средствах связи, установленных на указанной линии связи, представляемой собственниками или иными владельцами линии связи».

Приказ Роскомнадзора от 31.07.2019 № 228 «Об утверждении технических условий установки технических средств противодействия угрозам, а также требований к сетям связи при использовании технических средств противодействия угрозам».

Приказ Роскомнадзора от 31.07.2019 № 229 «Об утверждении Положения о национальной системе доменных имен, требований к ней, порядка ее создания, в том числе формирования информации, содержащейся в ней, а также правил ее использования, включая условия и порядок предоставления доступа к информации».

12. Приказы МИД России

Приказ МИД России от 30.03.2012 № 4236 «Об утверждении Административного регламента Министерства иностранных дел Российской Федерации».

ской Федерации по предоставлению государственной услуги по даче разъяснений по вопросам международного права в связи с запросами физических и юридических лиц».

Приказ МИД России от 14.05.2012 № 7063 «Об утверждении Административного регламента Министерства иностранных дел Российской Федерации по предоставлению государственной услуги по оказанию государственных информационно-консультационных услуг».

Приказ МИД России от 19.09.2013 № 17502 «Об утверждении Порядка проведения антикоррупционной экспертизы нормативных правовых актов и проектов нормативных правовых актов Министерства иностранных дел Российской Федерации».

Приказ МИД России от 16.01.2018 № 418 «Об утверждении плана-графика перехода на период 2017–2018 годов и на плановый период до 2020 года Министерства иностранных дел Российской Федерации на использование отечественного офисного программного обеспечения».

Приказ МИД России от 20.12.2018 № 24605 (в ред. Приказа МИД России от 20.03.2019 № 4335) «Об утверждении плана информатизации Министерства иностранных дел Российской Федерации на 2019–2021 годы» (вместе с «Планом информатизации на очередной финансовый 2019 год и плановый период 2020–2021 годов»).

13. Приказы, распоряжения и письма Минэкономразвития России

13.1. Приказы Минэкономразвития России

Приказ Минэкономразвития России от 16.11.2009 № 470 «О Требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти».

Приказ Минэкономразвития России от 04.05.2018 N 235 «Об утверждении Плана информатизации Министерства экономического развития Российской Федерации на 2018 год и плановый период 2019 и 2020 годов».

Приказ Минэкономразвития России от 19.09.2018 № 505 «Об утверждении Методики расчета показателей (индикаторов) государственной программы Российской Федерации “Экономическое развитие и инновационная экономика” и о признании утратившими силу приказа Минэкономразвития России от 9 июня 2017 г. № 285».

13.2. Распоряжения Минэкономразвития России

Распоряжение Минэкономразвития России от 11.08.2016 № 219Р-АУ «Об утверждении Методических рекомендаций по подготовке корпоративных планов импортозамещения государственными корпорациями, государственными компаниями, акционерными обществами, в уставном капитале которых доля участия Российской Федерации превыша-

ет 50 процентов, организациями, реализующими инвестиционные проекты, включенные в реестр инвестиционных проектов в соответствии с решением Правительственной комиссии по импортозамещению».

13.3. Письма Минэкономразвития России

Письмо Минэкономразвития России от 29.12.2018 № 39283-СГ/Д01и «О направлении методических материалов» (вместе с «Методическими материалами (требованиями) к разработке положений о порядке и правилах применения (внедрения) товаров, работ, услуг, удовлетворяющих критериям отнесения к инновационной продукции, высокотехнологичной продукции», «Рекомендациями по стимулированию спроса на инновационную продукцию на основе анализа практик, применяемых в субъектах Российской Федерации»).

13.4. Приказы Росстата

Приказ Росстата от 28.02.2019 № 106 «Об утверждении методик расчета показателей для мониторинга целевых показателей национального проекта “Цифровая экономика”» (вместе с «Методикой расчета показателя “Доля домохозяйств, имеющих широкополосный доступ к сети “Интернет”», «Методикой расчета показателя “Стоимостная доля закупаемого и (или) арендуемого федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации и иными органами государственной власти отечественного программного обеспечения”», «Методикой расчета показателя “Стоимостная доля закупаемого и (или) арендуемого государственными корпорациями, компаниями с государственным участием отечественного программного обеспечения”»).

14. Приказы Минфина России

Приказ Минфина России от 03.11.2016 № 202н «О перечне единых справочников, реестров и классификаторов, используемых в государственной интегрированной информационной системе управления общественными финансами “Электронный бюджет”».

Приказ Минфина России от 08.06.2018 № 132н «О Порядке формирования и применения кодов бюджетной классификации Российской Федерации, их структуре и принципах назначения»¹.

¹ Код 60322 «Обеспечение защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности в условиях цифровой экономики». По данному направлению расходов отражаются расходы федерального бюджета в рамках федерального проекта «Информационная безопасность» подпрограммы «Безопасность в информационном обществе» государственной программы Российской Федерации «Информационное общество» (233 D400000) по обеспечению защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности в условиях цифровой экономики.

Приказ Минфина России от 03.07.2018 № 1590 «О создании Комиссии по подтверждению соответствия электронной площадки, специализированной электронной площадки, оператора электронной площадки, оператора специализированной электронной площадки единым требованиям к операторам электронных площадок, операторам специализированных электронных площадок, электронным площадкам, специализированным электронным площадкам и функционированию электронных площадок, специализированных электронных площадок и дополнительным требованиям к операторам электронных площадок, операторам специализированных электронных площадок и функционированию электронных площадок, специализированных электронных площадок».

Приказ Минфина России от 06.06.2019 № 86н «Об утверждении кодов (перечней кодов) бюджетной классификации Российской Федерации, относящихся к федеральному бюджету и бюджетам государственных внебюджетных фондов Российской Федерации»¹.

14.1. Приказы Казначейства России

Приказ Казначейства России от 10.10.2018 № 36н «Об утверждении графика перехода федеральных органов исполнительной власти, руководство деятельностью которых осуществляет Правительство Российской Федерации, а также подведомственных федеральных казенных учреждений на ведение бюджетного учета с использованием программного обеспечения для ведения бюджетного учета, предоставляемого им Федеральным казначейством по результатам закупок, предусмотренных пунктом 1 постановления Правительства Российской Федерации от 8 июня 2018 г. № 658».

Приказ Казначейства России от 10.10.2018 № 37н «Об утверждении формы и порядка представления информации о потребности в осуществлении централизованных закупок программного обеспечения для ведения бюджетного учета и формирования потребности для осуществления централизованных закупок программного обеспечения для ведения бюджетного учета».

15. Приказы Минтруда России

Приказ Минтруда России от 29.04.2013 № 170н «Об утверждении методических рекомендаций по разработке профессионального стандарта».

¹ Код 12300 «Обеспечение защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности в условиях цифровой экономики». По данному направлению расходов отражаются расходы федерального бюджета в рамках подпрограммы «Безопасность в информационном обществе» государственной программы Российской Федерации «Информационное общество» (233 D400000) по обеспечению защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности в условиях цифровой экономики.

16. Приказы Минпромторга России

Приказ Минпромторга России от 15.08.2018 № 3223 «Об утверждении регламента электронного взаимодействия российских организаций и Министерства промышленности и торговли Российской Федерации в государственной информационной системе промышленности при проведении конкурсных процедур на право предоставления субсидий из федерального бюджета российским организациям на компенсацию части затрат на проведение научно-исследовательских и опытно-конструкторских работ по приоритетным направлениям гражданского промышленного в рамках реализации такими организациями комплексных инвестиционных проектов и при подаче заявлений о предоставлении субсидий».

Приказ Минпромторга России от 17.07.2019 № 2555 «Об утверждении формы отчета о расходах, на возмещение которых предоставляется субсидия российским организациям на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции».

Приказ Минпромторга России от 12.09.2019 № 3418 «Об утверждении формы заявления о присвоении статуса телекоммуникационного оборудования российского происхождения и включении телекоммуникационного оборудования в единый реестр российской радиоэлектронной продукции и формы заявления о подтверждении статуса телекоммуникационного оборудования российского происхождения».

16.1. Приказы Федерального агентства по техническому регулированию и метрологии (Росстандарт)

Приказ Росстандарта от 29.12.2018 № 1190-ст «О принятии и введении в действие Изменения 33/2018 ОКПД2 к Общероссийскому классификатору продукции по видам экономической деятельности ОК 034-2014 (КПЕС 2008)».

17. Приказы Минсельхоза России

Приказ Минсельхоза России от 23.04.2018 № 180 «Об утверждении Положения о Департаменте цифрового развития и управления государственными информационными ресурсами АПК».

18. Приказы Минобрнауки и Минпросвещения России

18.1. Приказы Минобрнауки России

Приказ Минобрнауки России от 09.08.2019 № 590 «О Международном совете по реализации отдельных мероприятий федерального проекта “Кадры для цифровой экономики” национальной программы “Цифровая экономика Российской Федерации”».

18.2. Приказы Минпросвещения России

Приказ Минпросвещения России от 02.12.2019 № 649 «Об утверждении Целевой модели цифровой образовательной среды».

19. Приказы Ростехнадзора

Приказ Ростехнадзора от 15.12.2017 № 543 «Об утверждении планов-графиков перехода Федеральной службы по экологическому, технологическому и атомному надзору и подведомственных организаций на использование отечественного офисного программного обеспечения на период 2017–2020 годов».

20. Совместные приказы ФОИВ

20.1. Приказы Минкомсвязи России/ФСО России

Приказ Минкомсвязи России/Приказ ФСО России от 27.05.2015 № 186/258 «Об утверждении Требований к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде».

20.2. Приказы МИД России/МВД России/ФСБ России

Приказ МИД России № 3663, МВД России № 135, ФСБ России № 110 от 15.03.2018 «Об утверждении Положения о порядке информационного взаимодействия Министерства иностранных дел Российской Федерации с Министерством внутренних дел Российской Федерации и Федеральной службой безопасности Российской Федерации с целью проверки наличия оснований, которые могут повлечь временное ограничение права гражданина Российской Федерации на выезд из Российской Федерации и отказ в оформлении (выдаче) основных документов, удостоверяющих личность гражданина Российской Федерации за пределами территории Российской Федерации».

20.3. Приказы МИД России/МО России, Минприроды России, Минфина России, МВД России, ФСБ России и других ФОИВ

Приказ МИД РФ № 19176, ФСБ РФ № 552, МВД РФ № 1076, Министра обороны РФ № 1861, Минприроды РФ № 840, Минфина РФ № 371, Росрыболовства № 1006, ФТС РФ № 2116, ФССП РФ № 417, Росимущества № 344, Росфинмониторинга № 340 от 13.10.2011 «Об утверждении Положения о взаимодействии федеральных органов исполнительной власти в сфере охраны морских биологических ресурсов и контроля за внешнеэкономическими операциями с морскими биологическими ресурсами и продуктами их переработки».

21. Приказы МВД России

Приказ МВД России от 10 мая 2018 г. № 284 «Об утверждении плана-графика перехода Министерства внутренних дел Российской Федерации на использование отечественного офисного программного обеспечения на 2018 год и на плановый период до 2020 года».

22. Приказы Генпрокуратуры России

Приказ Генпрокуратуры России от 26.08.2019 № 596 «Об утверждении Инструкции о порядке рассмотрения уведомлений о распространяемой с нарушением закона информации в информационно-телекоммуникационных сетях, в том числе в сети “Интернет”».

23. Приказы Минюста России

Приказ Минюста России от 21.11.2019 № 264 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, являющихся подсистемами федеральной государственной информационной системы “Автоматизированная информационная система Федеральной службы судебных приставов”, и информационных системах персональных данных, не являющихся подсистемами федеральной государственной информационной системы “Автоматизированная информационная система Федеральной службы судебных приставов”».

24. Приказы Минэнерго России

Приказ Минэнерго России от 11.07.2019 № 697 «Об утверждении форм предоставления в обязательном порядке юридическими лицами информации для включения в сегмент в области энергосбережения и повышения энергетической эффективности государственной информационной системы топливно-энергетического комплекса и требований к заполнению этих форм».

Приказ Минэнерго России от 02.08.2019 № 819 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении Минэнерго России функций, определенных законодательством Российской Федерации».

25. ГОСТы, межгосударственные и национальные стандарты

ГОСТ 25866-83. «Государственный стандарт Союза ССР. Эксплуатация техники. Термины и определения» (утв. Постановлением Госстандарта СССР от 13.07.1983 № 3105).

ГОСТ 27201-87. «Государственный стандарт Союза ССР. Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования» (утв. и введен в действие Постановлением Госстандарта СССР от 28.01.1987 № 124).

ГОСТ 28397-89 (ИСО 2382-15-85). «Межгосударственный стандарт. Языки программирования. Термины и определения» (утв. и введен в действие Постановлением Госстандарта СССР от 21.12.1989 № 3961).

ГОСТ 34.201-89. «Государственный стандарт Союза ССР. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (утв. Постановлением Госстандарта СССР от 24.03.1989 № 664).

ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (утв. Постановлением Госстандарта СССР от 24.03.1989 № 661).

ГОСТ 34.003-90. «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие Постановлением Госстандарта СССР от 27.12.1990 № 3399)¹.

ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания» (утв. Постановлением Госстандарта СССР от 29.12.1990 № 3469).

ГОСТ 15971-90. «Системы обработки информации. Термины и определения» (утв. Постановлением Госстандарта СССР от 26.10.1990 № 2698).

ГОСТ 34.603-92. «Информационная технология. Виды испытаний автоматизированных систем» (утв. Постановлением Госстандарта СССР от 17.02.1992 № 161).

ГОСТ Р 22.0.02-94 (в ред. Изменения № 1, принятого Постановлением Госстандарта РФ от 31.05.2000 № 148-ст) «Безопасность в чрезвычайных ситуациях. Определения основных понятий». Принят и введен в действие Постановлением Госстандарта РФ от 22.12.1994 № 327 (Группа Т 00, ОКСТУ 0022).

ГОСТ 7.0-99. Межгосударственный стандарт. «Система стандартов по информации, библиотечному и издательскому делу. Информационно-библиотечная деятельность, библиография. Термины и определения» (введен в действие Постановлением Госстандарта России от 07.10.1999 № 334-ст).

¹ Настоящий стандарт должен применяться совместно с ГОСТом 15971 и ГОСТом 16504.

ГОСТ Р 50.1.056-2005. «Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения».

ГОСТ Р 50922-2006. «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 373-ст).

ГОСТ Р 51275-2006. «Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 374-ст).

ГОСТ Р ИСО/МЭК 13335-1-2006. «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (утв. и введен в действие Приказом Ростехрегулирования от 19.12.2006 № 317-ст).

ГОСТ Р ИСО/МЭК 27001-2006. «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 375-ст).

ГОСТ Р ИСО 15489-1-2007. «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования» (утв. Приказом Ростехрегулирования от 12.03.2007 № 28-ст).

ГОСТ Р ИСО/МЭК ТО 19791-2008. «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 N 525-ст).

ГОСТ Р 54471-2011/ISO/TR 15801:2009. «Национальный стандарт Российской Федерации. Системы электронного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности» (утв. и введен в действие Приказом Росстандарта от 18.10.2011 № 466-ст).

ГОСТ Р ИСО/МЭК 29794-1-2012 «Информационные технологии. Биометрия. Качество биометрических образцов. Часть 1. Структура», утвержденном приказом Федерального агентства по техническому регулированию и метрологии от 18 сентября 2012 года № 351-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2013).

ГОСТ Р 53898-2013. «Национальный стандарт Российской Федерации. Системы электронного документооборота. Взаимодействие систем управления документами. Технические требования к электрон-

ному сообщению» (утв. и введен в действие Приказом Росстандарта от 08.11.2013 № 1465-ст).

ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица», утвержденном приказом Федерального агентства по техническому регулированию и метрологии от 06.09.2013 № 987-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2015).

ГОСТ Р 51583-2014. «Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (утв. и введен в действие Приказом Росстандарта от 28.01.2014 № 3-ст).

ГОСТ Р 56545-2015. «Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» (утв. и введен в действие Приказом Росстандарта от 19.08.2015 № 1180-ст)», пункт 3 — извлечение.

ГОСТ ISO/IEC 19794-1-2015 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура», утвержденном приказом Федерального агентства по техническому регулированию и метрологии от 20.11.2015 № 1928-ст «О введении в действие межгосударственного стандарта» (М.: ФГУП «Стандартинформ», 2016).

ГОСТ Р 57193-2016. «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем» (утв. и введен в действие Приказом Росстандарта от 31.10.2016 № 1538-ст).

ГОСТ Р 7.0.97-2016. «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов». (утв. Приказом Росстандарта от 08.12.2016 № 2004-ст).

ГОСТ ISO/IEC 2382-37-2016 «Информационные технологии (ИТ). Словарь. Часть 37. Биометрия», введенном в действие приказом Федерального агентства по техническому регулированию и метрологии от 28.02.2017 № 71-ст (М.: ФГУП «Стандартинформ», 2017).

ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 № 882-ст «Об утверждении национального стандарта» (М.: ФГУП «Стандартинформ», 2017).

ГОСТ Р ИСО 15489-1-2019 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и из-

дательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утв. Приказом Росстандарта от 26.03.2019 № 101-ст).

25.1. Рабочие документы (Методические указания)

РД 50-680-88. «Методические указания. Автоматизированные системы. Общие положения» (утв. Постановлением Госстандарта СССР от 28.12.1988 № 4622).

РД 50-682-89 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения». (утв. Постановлением Госстандарта СССР от 17.02.1989 № 254) (вместе с «Положениями по созданию единого комплекса стандартов автоматизированных систем»).

РД 50-34.698-90. «Методические указания. Информационная технология. Автоматизированные системы. Требования к содержанию документов» (утв. Постановлением Госстандарта СССР от 27.12.1990 № 3380).

26. Решения Высшего Евразийского экономического совета

Решение Высшего Евразийского экономического совета от 11.10.2017 № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года».

27. Постановления правительства Москвы

Постановление Правительства Москвы от 05.04.2011 № 105-ПП (ред. от 25.09.2018)

«Об утверждении Положения о Департаменте информационных технологий города Москвы».

Постановление Правительства Москвы от 21.12.2011 № 604-ПП (ред. от 02.10.2018)

«Об утверждении Положения об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие органов исполнительной власти города Москвы и организаций при предоставлении государственных услуг и исполнении государственных функций в городе Москве».

Постановление Правительства Москвы от 07.02.2012 № 26-ПП (ред. от 19.12.2017) «Об утверждении Положения об эксплуатации автоматизированных информационных систем и ресурсов города Москвы».

Постановление Правительства Москвы от 25.12.2018 № 1691-ПП «Об информационной системе обеспечения деятельности Московской административной дорожной инспекции» (вместе с «Положением об информационной системе обеспечения деятельности Московской административной дорожной инспекции»).

Постановление Правительства Москвы от 06.02.2019 № 59-ПП «Об информационной системе “Единая система мониторинга и администрирования телекоммуникационных услуг”» (вместе с «Положением об информационной системе “Единая система мониторинга и администрирования телекоммуникационных услуг”»).

28. Постановления правительства Московской области

Постановление Правительства Московской области от 17.10.2017 № 854/38 (ред. от 19.08.2019) «Об утверждении государственной программы Московской области “Цифровое Подмосковье” на 2018–2024 годы».

Постановление Правительства МО от 07.10.2019 № 692/33 «О государственной информационной системе Московской области “Единый центр управления регионом”».

29. Положения Банка России

Положение Банка России от 09.01.2019 № 672-П «Положение о требованиях к защите информации в платежной системе Банка России» (вместе с «Правилами материально-технического обеспечения формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП, а также правила материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ»).

30. Паспорта федеральных проектов в рамках национальной программы «Цифровая экономика Российской Федерации»¹

Нормативное регулирование цифровой среды².

Информационная инфраструктура³.

¹ Национальная программа «Цифровая экономика Российской Федерации» утверждена президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16. Паспорт национального проекта «Национальная программа “Цифровая экономика Российской Федерации”» утвержден президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7.

² Приложение № 2 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

³ Приложение № 3 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

Кадры для цифровой экономики¹.
Информационная безопасность².
Цифровые технологии³.
Цифровое государственное управление⁴.

31. Дорожные карты развития «сквозной» цифровой технологии

Квантовые технологии (утв. Минкомсвязью России).
Компоненты робототехники и сенсорики (утв. Минкомсвязью России).
Новые производственные технологии.
Нейротехнологии и искусственный интеллект (утв. Минкомсвязью России).
Системы распределенного реестра (утв. Минкомсвязью России).
Технологии беспроводной связи (утв. Минкомсвязью России).
Технологии виртуальной и дополненной реальности.

32. Регистрация доменных имен

Правила регистрации доменных имен в доменах .RU и .РФ (утв. решением Координационного центра национального домена сети Интернет от 05.10.2011 № 2011-18/81).

¹ Приложение № 4 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

² Приложение № 5 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

³ Приложение № 6 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

⁴ Приложение № 7 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9.

Алфавитный указатель терминов и определений основных понятий законодательства о цифровой экономике и информационной безопасности

А

- Абонент — 84
- Автоматизированная обработка персональных данных — 84
- Автоматизированная система (Operational system) — 84
- Автоматизированная система управления — 85
- Автоматизированное рабочее место — 85
- Автоматизированный производственный комплекс — 85
- Автоматизированный процесс — 85
- Автоматический процесс — 85
- Авторизация — 85
- Агент (Agent) — 85
- Адаптивность автоматизированной системы — 86
- Административные данные — 86
- Административный регламент — 86
- Администратор — 86
- Администратор защиты (Security administrator) — 86
- Администрирование — 86
- Адрес — 87
- Аккредитация удостоверяющего центра — 87
- Активы (Asset) — 87
- Актуализация информационного ресурса — 87
- Акты общего регулирования — 87
- Алгоритм — 87
- Алгоритм проектирования в САПР — 87
- Алгоритм функционирования автоматизированной системы — 87
- Алиби — 88
- Анализ риска (Risk analysis) — 88
- Анализ рисков (Risk analysis) — 88
- Аннулирование регистрации — 88

- Апелляционная инстанция — 88
- Архитектура (системы) (Architecture) — 88
- Архитектура вычислительной машины — 89
- Архитектурное представление (Architecture view) — 89
- Аттестация (Validation) — 89
- Аттестация объекта в защищенном исполнении — 89
- Аудит (Audit) — 89
- Аудит информационной безопасности в организации (Аудиторская проверка информационной безопасности в организации) — 89
- Аудиторская проверка информационной безопасности в организации (Аудит информационной безопасности в организации) — 90
- Аутентификационные данные — 90
- Аутентификация (Authentication) — 90
- Аутентификация, идентификация лица — 90
- Аффилированные лица — 91
- Аффилированные лица физического лица, осуществляющего предпринимательскую деятельность — 91
- Аффилированные лица юридического лица — 91

Б

- База данных перенесенных абонентских номеров — 92
- Базовая линия (Baseline) — 92
- Базовая организация — 92
- Базовый образ виртуальной машины — 92
- Байт — 92
- Банк — 93
- Банковский платежный агент — 93
- Банковский платежный субагент — 93
- Банкомат — 93
- Безопасность — 93
- Безопасность информации (Information security) — 93
- Безопасность информации — 94
- Безопасность критической информационной инфраструктуры — 94
- Безопасность продукции и связанных с ней процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации (далее — безопасность) — 94
- Безопасные программное обеспечение и сервис — 94
- Безотзывность перевода денежных средств — 94
- Безусловность перевода денежных средств — 95
- Бит — 95
- Бизнес-процесс — 95
- Большие данные — 95
- Бортовая ЭВМ — 96
- Близкие лица — 96

- Близкие родственники — 96
- Блокирование персональных данных — 96
- Быстроразвивающиеся опасные природные явления и техногенные процессы — 96

В

- Валидатор — 96
- Валидация, аттестация (Validation) — 96
- Валидация цифровой записи — 96
- Ввод в эксплуатацию — 97
- Ввод данных — 97
- Веб-сбор — 97
- Ведомственная отчетность — 97
- Ведомственный проект — 97
- Вердикт — 97
- Верификация (Verification) — 97
- Ветеринарно-санитарные и фитосанитарные меры — 98
- Вежа — 98
- Вещатель — 99
- Взаимодействие автоматизированных систем — 99
- Взаимодействие информационных систем электронного документооборота — 99
- Вид профессиональной деятельности — 99
- Виртуальный — 99
- Владелец сайта в сети «Интернет» — 100
- Владелец сертификата ключа проверки электронной подписи — 100
- Внемашинная информационная база автоматизированной системы — 100
- Внедрение инновационного решения — 100
- Внедряемый компонент — 100
- Внешняя автоматизированная система (External operational system) — 101
- Внешняя память — 101
- Военная техника — 101
- Военные объекты — 101
- Войска — 101
- Вооружение — 101
- Впервые выпускаемая в обращение продукция — 101
- Вредоносная программа — 102
- Вспомогательная функция автоматизированной системы управления технологическим процессом — 102
- Вспомогательный информационный ресурс — 102
- Входная информация автоматизированной системы — 102
- Вывод данных — 102
- Выделение полосы радиочастот — 103

- Высокопроизводительные рабочие места — 103
- Высокотехнологичная промышленная продукция — 103
- Высоочастотные устройства — 103
- Выходная информация автоматизированной системы — 103
- Выход, выходной результат процесса (Process outcome) — 103
- Вычислительная машина — 103

Г

- Гарантия качества (Quality assurance) — 104
- Гармонизация информации — 104
- Главный редактор — 104
- Головная организация интегрированной структуры оборонно-промышленного комплекса — 104
- Государственная информационная система промышленности — 104
- Государственная пошлина — 104
- Государственная тайна — 104
- Государственная услуга, предоставляемая федеральным органом исполнительной власти, органом государственного внебюджетного фонда, исполнительным органом государственной власти субъекта Российской Федерации, а также органом местного самоуправления при осуществлении отдельных государственных полномочий, переданных федеральными законами и законами субъектов Российской Федерации — 105
- Государственно-частное партнерство, муниципально-частное партнерство — 105
- Государственные органы — 105
- Государственный адресный реестр — 106
- Государственный заказчик — 106
- Государственный контракт, муниципальный контракт — 106
- Государственный обвинитель — 106
- Гриф секретности — 106
- Группа реагирования на инциденты защиты информации — 107

Д

- Данные — 107
- Действие процессуальное — 107
- Декларация о соответствии — 107
- Декларирование соответствия — 107
- Делегирование домена — 107
- Деятельность, действие (Activity) — 108
- Диалоговый режим — 108
- Диалоговый режим выполнения функции автоматизированной системы — 108
- Динамический анализ исходных текстов программ — 108

- Дискретно выполняемая функция автоматизированной системы управления технологическим процессом — 108
- Дискреционное управление доступом (Discretionary access control) — 109
- Дислокация объекта — 109
- Диспетчер доступа (ядро защиты) (Security kernel) — 109
- Доверенная третья сторона — 109
- Доверенный источник — 109
- Дознаватель — 109
- Дознание — 109
- Доказательство (Evidence) — 109
- Документация на автоматизированную систему — 110
- Документированная информация — 110
- Документная система (Records system) — 110
- Документы (Records) — 111
- Должностное лицо — 111
- Домен — 111
- Домен безопасности (Security domain) — 111
- Домен .РФ — 111
- Домен .RU — 111
- Доменное имя — 111
- Допуск к государственной тайне — 111
- Доступ (Access) — 112
- Доступ к информации (Access to information) — 112
- Доступ к информации — 112
- Доступ к информации, составляющей коммерческую тайну — 112
- Доступ к сведениям, составляющим государственную тайну — 112
- Доступность (Availability) — 112
- Досудебное производство — 112
- Досудебное соглашение о сотрудничестве — 113

Е

- Единая информационная система в сфере закупок (единая информационная система) — 113
- Единая система идентификации и аутентификации — 113

Ж

- Жалоба — 113
- Жалоба на нарушение порядка предоставления государственной или муниципальной услуги — 113
- Живучесть автоматизированной системы — 114
- Жизненно важные интересы — 114
- Жизненный цикл (Life cycle) — 114
- Жизненный цикл информационной системы — 114
- Жилище — 115

3

- Загрузка в память — 115
- Задание на проектирование в САПР — 115
- Задача (Task) — 115
- Задача автоматизированной системы — 116
- Задача, требующая инновационного (высокотехнологичного) решения (Задача) — 116
- Задержание подозреваемого — 116
- Заинтересованная сторона, правообладатель (Stakeholder) — 116
- Заказчик (Customer) — 116
- Закладочное средство (устройство) — 117
- Заключение суда — 118
- Законные представители — 118
- Закупка товара, работы, услуги для обеспечения государственных или муниципальных нужд — 118
- Закупки офисного программного обеспечения, программного обеспечения в сфере информационной безопасности, программного обеспечения для ведения бюджетного учета — 118
- Замысел защиты информации — 119
- Запоминающее устройство — 119
- Запрос — 119
- Защита информации — 119
- Защита информации от иностранной разведки — 120
- Защита информации от непреднамеренного воздействия — 120
- Защита информации от несанкционированного воздействия — 120
- Защита информации от несанкционированного доступа — 120
- Защита информации от преднамеренного воздействия — 120
- Защита информации от разглашения — 120
- Защита информации от утечки — 121
- Защита от вредоносного кода на уровне гипервизора — 121
- Защита от несанкционированного доступа (Protection from unauthorized access) — 121
- Защитные контрмеры — 121
- Защищаемая информационная система — 122
- Защищаемая информация — 122
- Защищаемый объект информатизации — 122
- Защищенное средство вычислительной техники (защищенная автоматизированная система) (Trusted computer system) — 122
- Заявитель — 122
- Заявка — 123
- Заявление — 123
- Знак обращения на рынке — 124

- Знак соответствия — 124
- Значимая платежная система — 124
- Значимый объект критической информационной инфраструктуры — 124
- Зона чрезвычайной ситуации — 124
- Зона экстренного оповещения населения — 124

И

- Идентификатор доступа (Access identifier) — 124
- Идентификатор — 124
- Идентификация (Identification) — 125
- Идентификация, аутентификация лица — 125
- Идентификация продукции — 125
- Избрание меры пресечения — 126
- Издатель — 126
- Импортозамещение — 126
- Индустриальный интернет — 126
- Индустриальный (промышленный) парк — 126
- Инжиниринговый центр — 126
- Инициативное предложение — 126
- Инициатор — 127
- Инициатор комплексного проекта — 127
- Инициатор комплексной программы — 127
- Инновационная продукция — 127
- Инновационный цикл — 127
- Инновационное решение — 127
- Иностранная платежная система — 128
- Иностранная продукция — 128
- Интеграционные подсистемы — 128
- Интегрированная автоматизированная система — 128
- Интегрированная структура оборонно-промышленного комплекса — 129
- Интерактивный режим — 129
- Интернет вещей — 129
- Интерес (системы) (Concern) — 129
- Интерфейс — 129
- Информатизация — 129
- Информатика — 130
- Информационная база автоматизированной системы — 130
- Информационная безопасность (Information security) — 130
- Информационная безопасность Российской Федерации — 130
- Информационная инфраструктура Российской Федерации — 130
- Информационная модель — 130
- Информационная модель объекта капитального строительства — 131
- Информационная система — 131

- Информационная система общего пользования — 131
- Информационная система персональных данных — 131
- Информационная совместимость автоматизированных систем — 131
- Информационная технология (технология обработки (передачи) информации в информационной системе) — 132
- Информационная угроза — 132
- Информационная функция автоматизированной системы управления технологическим процессом — 132
- Информационно-коммуникационные технологии — 132
- Информационное изделие в автоматизированной системе — 132
- Информационное обеспечение автоматизированной системы — 133
- Информационное общество — 133
- Информационное пространство — 133
- Информационное средство — 133
- Информационно-телекоммуникационная сеть — 133
- Информационные технологии — 133
- Информационный обмен между виртуальными машинами — 134
- Информационный объект — 134
- Информационный ресурс — 134
- Информация — 134
- Информация конфиденциального характера — 134
- Информация о деятельности государственных органов и органов местного самоуправления — 134
- Информация, составляющая коммерческую тайну (секрет производства) — 135
- Информирование населения о чрезвычайных ситуациях — 135
- Инфраструктура взаимодействия — 135
- Инфраструктура поддержки деятельности в сфере промышленности — 136
- Инфраструктура цифрового профиля — 136
- Инфраструктура экономики Российской Федерации — 136
- Инфраструктура электронного правительства — 136
- Инцидент (Incident) — 136
- Инцидент информационной безопасности (Information security incident) — 136
- Искусственный интеллект — 137
- Использование по назначению — 137
- Использование радиочастотного спектра — 137
- Источник угрозы безопасности информации — 137
- Итоговое судебное решение — 137

К

- Канал ввода-вывода — 138
- Кассационная инстанция — 138

- Качество эксплуатации продукции — 138
- Квалификация (Qualification) — 138
- Квалификация работника — 138
- Квалифицированный сертификат ключа проверки электронной подписи — 138
- Класс защищенности средств вычислительной техники (автоматизированной системы) (Protection class of computer systems) — 138
- Классификация (Classification) — 139
- Ключ электронной подписи — 139
- Ключ проверки электронной подписи — 139
- Код «AuthInfo-код» — 139
- Коммерческая тайна — 139
- Комплекс программ «Почтовая служба» — 139
- Комплекс средств автоматизации автоматизированной системы — 139
- Комплекс средств защиты (Trusted computing base) — 140
- Комплексная программа — 140
- Комплексная система экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций — 140
- Комплексный план научных исследований — 140
- Комплексный проект — 141
- Комплектуемое изделие в автоматизированной системе — 141
- Компонент (Component) — 142
- Компонент автоматизированной системы — 142
- Компонент информационной системы — 142
- Компоненты информационно-телекоммуникационной инфраструктуры — 142
- Компрометация аутентификационных данных — 142
- Компромисс (Trade-off) — 143
- Компьютеризация — 143
- Компьютерная атака — 143
- Компьютерная информация — 143
- Компьютерный вирус — 143
- Компьютерный инцидент — 143
- Конверсия радиочастотного спектра — 144
- Конвертирование (Conversion) — 144
- Конец эксплуатации — 144
- Контентные услуги — 144
- Контрагент — 144
- Контракт — 144
- Контракт жизненного цикла — 145
- Контрактная система в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд (контрактная система в сфере закупок) — 145
- Контроль телефонных и иных переговоров — 146
- Контрольный орган в сфере закупок — 146

- Контур безопасности — 146
- Конфигурация информационной системы — 146
- Конфигурация системы обработки информации — 147
- Конфиденциальная информация (Sensitive information) — 147
- Конфиденциальность (Confidentiality) — 147
- Конфиденциальность информации — 147
- Концепция диспетчера доступа (Reference monitor concept) — 147
- Концепция функционирования, эксплуатации (Concept of operations) — 147
- Координатор — 148
- Координационный орган — 148
- Корпоративная информационная система — 148
- Кредитная организация — 148
- Криптовалюта — 148
- Криптографическая защита информации — 149
- Критическая информационная инфраструктура — 149
- Криптографическое средство защиты информации — 149
- Критерий эффективности деятельности — 149
- Критическая информационная инфраструктура Российской Федерации
(далее — критическая информационная инфраструктура) — 149
- Критически важный объект — 149
- Критический маршрут выполнения функциональных объектов — 150
- Кросс-отраслевые процессы — 150
- Крупный ущерб — 150

Л

- Легальный субъект доступа — 150
- Лидерная эксплуатация — 150
- Лидирующий исследовательский центр — 150
- Ликвидация чрезвычайных ситуаций — 151
- Лимит бюджетных обязательств — 151
- Лингвистическая совместимость автоматизированных систем — 151
- Лингвистическое обеспечение автоматизированной системы — 151
- Линейно-кабельные сооружения связи — 152
- Линии связи — 152
- Лицензиат — 152
- Лицензиат в области защиты информации — 152
- Лицензионные требования — 152
- Лицензирование — 152
- Лицензирование в области защиты информации — 152
- Лицензируемый вид деятельности — 153
- Лицензирующие органы — 153
- Лицензия — 153
- Лицензия в области защиты информации — 153
- Логический доступ к ресурсу доступа (логический доступ) — 154

М

- Майнинг — 154
- Мандатное управление доступом (Mandatory access control) — 154
- Массовая информация — 154
- Массовые беспорядки — 154
- Массовый трансфер — 155
- Математическое обеспечение автоматизированной системы — 155
- Матрица доступа (Access matrix) — 155
- Машинная информационная база автоматизированной системы — 155
- Машинное моделирование — 155
- Межведомственное информационное взаимодействие — 155
- Межведомственный запрос — 156
- Межведомственный электронный документооборот — 156
- Международно-правовая защита присвоения (назначения) радиочастот или радиочастотных каналов — 156
- Международный стандарт — 156
- Менеджмент качества (Quality management) — 157
- Менеджмент риска (Risk management) — 157
- Менеджмент рисков (Risk management) — 157
- Мероприятия по импортозамещению — 157
- Мероприятия по информатизации — 158
- Меры безопасности — 158
- Меры обеспечения безопасности (Security controls) — 158
- Меры стимулирования деятельности в сфере промышленности — 158
- Место осуществления лицензируемого вида деятельности — 159
- Место осуществления отдельного вида деятельности, подлежащего лицензированию — 159
- Метаданные документов (Metadata for records) — 159
- Метка доверенного времени — 159
- Метка конфиденциальности (Sensitivity label) — 160
- Методическое обеспечение автоматизированной системы — 160
- Метрологическая совместимость автоматизированных систем — 160
- Миграция (Migration) — 160
- Микроданные — 160
- Микро-ЭВМ — 160
- Мини-ЭВМ — 160
- Многоуровневая защита (Multilevel secure) — 161
- Многофакторная аутентификация — 161
- Многофункциональный центр предоставления государственных и муниципальных услуг (многофункциональный центр) — 161
- Модель жизненного цикла (Life cycle model) — 161
- Модель защиты (Protection model) — 161
- Модель нарушителя правил разграничения доступа (Security policy violator's model) — 161

- Модель угроз безопасности информации — 162
- Модернизация высокопроизводительных рабочих мест — 162
- Момент фактического задержания — 162
- Мониторинг безопасности информации — 162
- Мониторинг экспериментального режима — 162
- Монтированная емкость — 162
- Мультипрограммирование — 163
- Муниципальная отчетность — 163
- Муниципальная услуга, предоставляемая органом местного самоуправления (муниципальная услуга) — 163
- Муниципальный заказчик — 163
- Муниципальный контракт — 164

Н

- Наведенный в токопроводящих линейных элементах технических средств сигнал; наводка — 164
- Надежность автоматизированной системы — 164
- Надзорная инстанция — 164
- Налог — 164
- Нарушитель правил разграничения доступа (Security policy violator) — 165
- Научно-технический уровень автоматизированной системы — 165
- Национальная безопасность — 165
- Национальная безопасность Российской Федерации (национальная безопасность) — 165
- Национальная платежная система — 166
- Национальная электронная библиотека — 166
- Национальные интересы Российской Федерации — 166
- Национальные интересы Российской Федерации в информационной сфере (национальные интересы в информационной сфере) — 166
- Национальные счета — 166
- Национальный проект — 167
- Начало эксплуатации — 167
- Начальник органа дознания — 167
- Начальник подразделения дознания — 167
- Неавтоматизированный режим выполнения функции автоматизированной системы — 167
- Недекларированные возможности — 168
- Недекларированные возможности программного обеспечения — 168
- Некапитальные строения, сооружения — 168
- Неопределенность — 168
- Неотложные следственные действия — 168
- Непрерывно выполняемая функция автоматизированной системы управления технологическим процессом — 168

- Непричастность — 169
- Несанкционированное воздействие на информацию — 169
- Несанкционированный доступ к информации (Unauthorized access to information) — 169
- Норма эффективности защиты информации — 169
- Нормальная эксплуатация — 169
- Нормативно-справочная информация автоматизированной системы — 170
- Нормативный правовой акт — 170
- Носители сведений, составляющих государственную тайну — 170
- Носитель данных — 170
- Носитель защищенной информации — 170
- Ночное время — 170
- Нумерация — 170

О

- Обвинение — 171
- Обезличивание персональных данных — 171
- Обеспечение информационной безопасности — 171
- Обеспечение национальной безопасности — 171
- Обеспечивающая система (Enabling system) — 172
- Обладатель информации — 172
- Обладатель информации, составляющей коммерческую тайну — 172
- Облачные вычисления — 172
- Обмен электронными сообщениями — 172
- Обобщенная трудовая функция — 173
- Обоснование бюджетных ассигнований — 173
- Обработка больших объемов данных — 173
- Обработка информации — 173
- Обработка персональных данных — 173
- Обработка риска (Risk treatment) — 173
- Обработка рисков (Risk treatment) — 174
- Обработка текстов — 174
- Обращение гражданина — 174
- Общее регулирование — 174
- Общее программное обеспечение автоматизированной системы — 174
- Общество знаний — 175
- Объект адресации — 175
- Объект деятельности — 175
- Объект доступа (Access object) — 175
- Объект защиты информации — 176
- Объект информатизации — 176
- Объект информатизации финансовой организации (объект информатизации) — 176

- Объект капитального строительства — 176
- Объект народного хозяйства — 176
- Объекты административного управления — 176
- Объекты инженерной инфраструктуры — 176
- Объекты критической информационной инфраструктуры — 177
- Объекты режимные — 177
- Объекты систематизации — 177
- Объекты ядерного комплекса — 177
- Однофакторная аутентификация — 178
- Ожидание использования по назначению — 178
- Оконечное оборудование — 178
- Окончателность перевода денежных средств — 178
- Оперативная информация автоматизированной системы — 178
- Оперативная память — 178
- Оператор — 178
- Оператор, занимающий существенное положение в сети связи общего пользования — 179
- Оператор информационной системы — 179
- Оператор обмена цифровых финансовых активов — 179
- Оператор обязательных общедоступных телеканалов и (или) радиоканалов — 180
- Оператор платежной системы — 180
- Оператор по переводу денежных средств — 180
- Оператор связи — 180
- Оператор специализированной электронной площадки — 180
- Оператор универсального обслуживания — 181
- Оператор услуг платежной инфраструктуры — 181
- Оператор электронной площадки — 181
- Оператор электронных денежных средств — 181
- Операционная концепция (Operational concept) — 181
- Операционная система — 182
- Операционные услуги — 182
- Операционный центр — 182
- Операция записи данных — 182
- Операция устройства вычислительной машины — 182
- Операция чтения данных — 182
- Оповещение населения о чрезвычайных ситуациях — 182
- Определение поставщика (подрядчика, исполнителя) — 183
- Орган исполнительной власти субъекта Российской Федерации по регулированию контрактной системы в сфере закупок — 183
- Орган по сертификации — 183
- Организационная мера защиты информации — 183
- Организационная совместимость автоматизированных систем — 184
- Организационное обеспечение автоматизированной системы — 184
- Организационные меры безопасности (Operational controls) — 184

- Организация (Organization) — 184
- Организация предпринимательского сообщества — 185
- Организация связи — 185
- Органы дознания — 185
- Органы управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций — 185
- Отбор и передача на хранение или уничтожение (Disposition) — 186
- Ответственный исполнитель — 186
- Отрасль промышленности — 186
- Освоение производства промышленной продукции — 186
- Основная память — 187
- Основные средства (Facility) — 187
- Особо опасные, технически сложные сооружения связи — 187
- Остаточный риск (Residual risk) — 187
- Остаточный риск (Residual risk) — 187
- Отечественная продукция — 187
- Офисное программное обеспечение — 188
- Официальная статистическая информация — 188
- Официальный сайт государственного органа или органа местного самоуправления (далее — официальный сайт) — 189
- Официальный статистический учет — 189
- Охраняемые сведения — 189
- Оценивание риска (Risk evaluation) — 189
- Оценка информационного риска — 189
- Оценка риска (Risk assessment) — 190
- Оценка рисков (Risk assessment) — 190
- Оценка соответствия — 190
- Оценка соответствия требованиям по защите информации — 190
- Очередной финансовый год — 190
- Очередь автоматизированной системы — 190

П

- Пакет прикладных программ — 190
- Память данных — 191
- Паразитное электромагнитное излучение — 191
- Пароль (Password) — 191
- Паспорт Программы — 191
- Паспорт федерального проекта Программы — 191
- Педагог — 192
- Передача информации, составляющей коммерческую тайну — 192
- Перечень задач — 192
- Перечень инновационной, высокотехнологичной продукции — 192
- Перечень сведений, составляющих государственную тайну — 192
- Первичные статистические данные — 192

- Передача информации, составляющей коммерческую тайну — 192
- Перечень сведений, составляющих государственную тайну — 192
- Периодическое печатное издание — 193
- Перевод денежных средств — 193
- Персональная ЭВМ — 193
- Персональные данные — 193
- Плановый период — 193
- Платежная система — 193
- Платежная система иностранная — 194
- Платежная услуга — 194
- Платежные клиринговые позиции — 194
- Платежный клиринговый центр — 194
- Побочное электромагнитное излучение — 194
- Подведомственная государственному органу или органу местного самоуправления организация — 194
- Подготовка населения в области защиты от чрезвычайных ситуаций — 194
- Поддержка сведений о доменном имени — 195
- Подсистема (Subsystem) — 195
- Подтверждение соответствия — 195
- Поисковая система — 195
- Показатель защищенности средств вычислительной техники (Protection criterion of computer systems) — 196
- Показатель эффективности автоматизированной системы — 196
- Поколение ЭВМ — 196
- Положение — 196
- Положение о применимости (Statement of applicability) — 196
- Получатель государственной поддержки — 197
- Получатель гранта — 197
- Получение информации о соединениях между абонентами и (или) абонентскими устройствами — 197
- Пользователи официальной статистической информацией — 198
- Пользователь (User) — 198
- Пользователь автоматизированной системы — 198
- Пользователь информацией — 198
- Пользователь радиочастотным спектром — 198
- Пользователь системы обработки информации — 199
- Пользователь услугами связи — 199
- Пользовательское оборудование — 199
- Помехоустойчивость автоматизированной системы — 199
- Портал государственных и муниципальных услуг — 199
- Портфель проектов (Project portfolio) — 199
- Поставщик (Supplier) — 199
- Поставщик инновационного решения — 200
- Постановление — 200

- Потенциально опасный объект — 200
- «Почтовая служба» (комплекс программ) — 200
- Права логического доступа — 200
- Правила отбора и передачи (Disposition authority) — 201
- Правила платежной системы — 201
- Правила разграничения доступа (Security policy) — 201
- Правовая защита информации — 201
- Правовое обеспечение автоматизированной системы — 201
- Предварительный национальный стандарт — 201
- Преднамеренное силовое электромагнитное воздействие на информацию — 202
- Предложение — 202
- Предоплаченная карта — 202
- Предоставление государственных и муниципальных услуг в электронной форме — 202
- Предоставление информации — 202
- Предоставление информации, составляющей коммерческую тайну — 203
- Предоставление персональных данных — 203
- Председательствующий — 203
- Представление — 203
- Предупреждение чрезвычайных ситуаций — 203
- Прерывание — 203
- Претендент — 203
- Приговор — 203
- Приемочная документация на автоматизированную систему — 204
- Признак классификации уязвимостей — 204
- Применение меры пресечения — 204
- Принятие риска (Risk acceptance) — 204
- Приобретающая сторона (Acquirer) — 204
- Приобретение (Acquisition) — 204
- Присвоение (назначение) радиочастоты или радиочастотного канала — 204
- Присяжный заседатель — 205
- Проблема, задача (Problem) — 205
- Провайдер хостинга — 205
- Программа деятельности лидирующего исследовательского центра — 205
- Программа экспериментального режима — 205
- Программная закладка — 205
- Программная совместимость автоматизированных систем — 206
- Программное воздействие — 206
- Программное изделие в автоматизированной системе — 206
- Программное обеспечение в сфере информационной безопасности — 206

- Программное обеспечение автоматизированной системы — 206
- Программное обеспечение для ведения бюджетного учета — 207
- Программное обеспечение несанкционированного доступа в компьютерные сети — 207
- Программное обеспечение офисное — 207
- Программно-методический комплекс системы автоматизированного проектирования — 207
- Программно-технический комплекс автоматизированной системы — 208
- Программные закладки — 208
- Программный продукт — 208
- Продукт, продукция (Product) — 209
- Продукция — 209
- Продукция средства массовой информации — 209
- Продление регистрации доменного имени — 209
- Проект (Project) — 209
- Проект государственно-частного партнерства, проект муниципально-частного партнерства — 210
- Проектирование (Design, noun) — 210
- Проектировать (Design, verb) — 211
- Проектная деятельность — 211
- Проектное решение в САПР — 211
- Проектно-сметная документация на АС — 211
- Проектный документ в САПР — 211
- Производственно-технологический процесс — 211
- Прокурор — 212
- Промежуточное судебное решение — 212
- Промышленная инфраструктура — 212
- Промышленная политика — 212
- Промышленная продукция — 212
- Промышленная продукция, не имеющая произведенных в Российской Федерации аналогов — 212
- Промышленное производство — 212
- Промышленность — 212
- Промышленный кластер — 213
- Промышленный (индустриальный) парк — 213
- Промышленный технопарк — 213
- Простая функция автоматизированной системы управления технологическим процессом — 213
- Профессиональный стандарт — 213
- Процесс (Process) — 214
- Процесс создания автоматизированной системы — 214
- Процессор — 214
- Процессор ввода-вывода — 214
- Процессуальное действие — 214

- Процессуальное решение — 214
- Прямое соглашение — 214
- Публичный партнер — 214

Р

- Рабочая документация на автоматизированную систему — 215
- Рабочий процесс (Work process) — 215
- Радиоканал, телеканал — 215
- Радиопомеха — 216
- Радиочастота — 216
- Радиочастотный спектр — 216
- Радиоэлектронные средства — 216
- Развитие автоматизированной системы — 216
- Разглашение информации, составляющей коммерческую тайну — 216
- Разрабатываемый компонент — 217
- Распределение полос радиочастот — 217
- Распределенный реестр цифровых транзакций — 217
- Распространение информации — 217
- Распространение персональных данных — 217
- Распространение продукции средства массовой информации — 217
- Распространитель — 218
- Рассматриваемая система (System-of-interest) — 218
- Расчетные услуги — 218
- Расчетный центр — 218
- Реабилитация — 218
- Реабилитированный — 218
- Реальная эксплуатация — 218
- Региональная организация по стандартизации — 219
- Региональная отчетность — 219
- Региональный проект — 219
- Региональный проект Программы — 220
- Региональный свод правил — 220
- Региональный стандарт — 220
- Регистратор — 220
- Регистратор-донор — 220
- Регистратор-реципиент — 220
- Регистрация доменного имени — 220
- Регистрация событий защиты информации (регистрация) — 220
- Регламентирующие документы Координатора — 220
- Регламентный информационный ресурс — 221
- Регулирующий орган — 221
- Регулятивная песочница — 221
- Редакция средства массовой информации — 221
- Реестр — 222

- Реестр обращений — 222
- Реестр цифровых транзакций — 222
- Режим пакетной обработки — 222
- Режим разделения времени — 222
- Режим реального времени — 222
- Режим функционирования органов управления и сил единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций — 222
- Режимные объекты — 223
- Результат проектирования в САПР — 223
- Результаты оперативно-розыскной деятельности — 223
- Реквизиты документа — 223
- Ремонт — 223
- Реплика — 223
- Ресурс (Resource) — 223
- Ресурс доступа — 224
- Ресурс нумерации — 224
- Ресурс персональных данных — 224
- Решение процессуальное — 224
- Риск (Risk) — 225
- Родственники — 225
- Розыскные меры — 225
- Роль защиты информации — 225
- Роль логического доступа (роль) — 226
- Российская организация — 226
- Руководитель следственного органа — 226

С

- Сайт в сети «Интернет» — 226
- Сайт Координатора — 226
- Санкционированный доступ к информации (Authorized access to information) — 227
- Сбор — 227
- Свидетельский иммунитет — 227
- Свод правил — 227
- Свод правил иностранного государства — 227
- Сводная бюджетная роспись — 227
- Секрет производства (информация, составляющая коммерческую тайну) — 228
- Семейство ЭВМ — 228
- Сервер DNS — 228
- Серверные компоненты виртуализации — 228
- Сервисные подсистемы — 228
- Сертификат защиты (Protection certificate) — 230

- Сертификат ключа проверки электронной подписи — 230
- Сертификат соответствия — 230
- Сертификат квалифицированный ключа проверки электронной подписи (квалифицированный сертификат) — 230
- Сертификация — 231
- Сертификация уровня защиты (Protection level certification) — 231
- Сетевая атака — 231
- Сетевое издание — 231
- Сетевой адрес — 231
- Сети связи нового поколения — 231
- Сеть связи — 231
- Силы обеспечения информационной безопасности — 231
- Силы обеспечения национальной безопасности — 232
- Система (System) — 232
- Система государственной статистики — 233
- Система защиты государственной тайны — 233
- Система защиты информации — 233
- Система защиты информации от несанкционированного доступа (System of protection from unauthorized access to information) — 234
- Система защиты секретной информации (Secret information security system) — 234
- Система как объект оценки (System target of evaluation) — 234
- Система локальной автоматики — 234
- Система межведомственного электронного документооборота — 235
- Система менеджмента информационной безопасности (Information security management system) — 235
- Система обеспечения информационной безопасности — 235
- Система обеспечения национальной безопасности — 235
- Система обработки информации — 236
- Система организации и управления защитой информации — 236
- Система разграничения доступа (Security policy realization) — 236
- Система сертификации — 236
- Система хранения данных виртуализации (система хранения данных) — 236
- Система эксплуатации — 237
- Система электронного документооборота — 237
- Систематизация информации — 237
- Системная инженерия (Systems engineering) — 237
- Системный элемент (System element) — 237
- «Сквозная» цифровая технология — 238
- Сквозные технологии — 238
- Смарт-контракт — 238
- Следователь — 238
- Следователь-криминалист — 239
- Снятие с эксплуатации — 239

- Снятие с эксплуатации (выведение из эксплуатации), списание (Retirement) — 239
- Событие информационной безопасности (Information security event) — 239
- Совместимость автоматизированных систем — 239
- Совместный конкурс — 240
- Совокупный годовой объем закупок — 240
- Современный функциональный эквивалент сети связи — 240
- Согласие — 240
- Соглашение (Agreement) — 240
- Соглашение о государственно-частном партнерстве, соглашение о муниципально-частном партнерстве — 240
- Содержание под стражей — 241
- Соискатель лицензии — 241
- Соисполнитель — 241
- Сообщение автоматизированной системы — 241
- Сообщение о преступлении — 241
- Сооружения связи — 241
- Сопровождение автоматизированной системы — 241
- Составная функция автоматизированной системы управления технологическим процессом — 242
- Специализированная организация — 242
- Специализированная ЭВМ — 242
- Специализированная электронная площадка — 242
- Специализированное средство массовой информации — 243
- Специализированное учреждение для несовершеннолетних — 243
- Специализированные технические средства оповещения и информирования населения в местах массового пребывания людей — 243
- Специальная проверка — 243
- Специальное исследование объекта защиты информации — 243
- Специальное программное обеспечение автоматизированной системы — 243
- Специальное регулирование — 243
- Сравнительное преимущество — 244
- Средства доверенной третьей стороны — 244
- Средства защиты информации — 244
- Средства контроля — 244
- Средства обеспечения информационной безопасности — 245
- Средства обеспечения национальной безопасности — 245
- Средства связи — 245
- Средства удостоверяющего центра — 245
- Средства эксплуатации — 245
- Средства электронной подписи — 245
- Средство защиты информации — 246
- Средство защиты от несанкционированного доступа (Protection facility) — 246

- Средство контроля эффективности защиты информации — 246
- Средство коллективного доступа — 246
- Средство криптографической защиты информации (Cryptographic information protection facility) — 246
- Средство массовой информации — 246
- Средство физической защиты информации — 247
- Стадия (Stage) — 247
- Стадия создания автоматизированной системы — 247
- Стандарт иностранного государства — 247
- Стандартизация — 247
- Статический анализ исходных текстов программ — 247
- Степень опасности уязвимости — 248
- Стоп-лист — 248
- Сторона (Party) — 248
- Стороны — 248
- Сторона защиты — 248
- Сторона обвинения — 248
- Страница сайта в сети «Интернет» (далее также — интернет-страница) — 248
- Стратегические национальные приоритеты — 248
- Стратегические национальные приоритеты Российской Федерации — 249
- Структура архитектуры (Architecture framework) — 249
- Структура информационного ресурса — 249
- Субъект доступа (Access subject) — 249
- Субъект экспериментального режима — 250
- Субъекты деятельности в сфере промышленности — 250
- Субъекты критической информационной инфраструктуры — 250
- Субъекты официального статистического учета — 251
- Суд — 251
- Суд первой инстанции — 251
- Суд второй инстанции — 251
- Судебная экспертиза — 251
- Судебное заседание — 251
- Судебное разбирательство — 251
- Судебное решение — 251
- Судебное решение итоговое — 252
- Судебное решение промежуточное — 252
- Судья — 252
- Супер-ЭВМ — 252
- Существующие компоненты — 252
- Схема классификации деловых операций (Business classification scheme) — 252
- Схема метаданных (Schema) — 252
- Схема подтверждения соответствия — 252

Т

- Техника защиты информации — 253
- Текущий образ виртуальной машины — 253
- Текущий финансовый год — 253
- Телеканал, радиоканал — 253
- Территория, подверженная риску возникновения быстроразвивающихся опасных природных явлений и техногенных процессов —
- Технический центр — 254
- Технологически независимое программное обеспечение и сервис — 254
- Техническая защита информации — 254
- Техническая мера защиты информации — 254
- Техническая совместимость автоматизированных систем — 254
- Техническая учетная запись — 255
- Технические меры безопасности (Technical controls) — 255
- Технические средства системы обработки информации — 255
- Технический проект автоматизированной системы — 255
- Технический регламент — 255
- Техническое задание на автоматизированную систему — 256
- Техническое обеспечение автоматизированной системы — 256
- Техническое обслуживание объекта соглашения — 256
- Техническое регулирование — 257
- Техническое средство обработки информации (ТСОИ) — 257
- Технологическая инфраструктура — 257
- Технологическая структура организации — 257
- Технологический объект управления — 258
- Технологический процесс финансовой организации (технологический процесс) — 258
- Технология обработки (передачи) информации в информационной системе (информационная технология) — 258
- Технопарк промышленный — 258
- Технорабочий проект автоматизированной системы — 259
- Типовое проектное решение в САПР — 259
- Токен — 259
- Точка доступа — 259
- Точка зрения на архитектуру (Architecture viewpoint) — 259
- Точка обмена трафиком — 259
- Транзакция (Transaction) — 260
- Трансграничная передача персональных данных — 260
- Трансграничный перевод денежных средств — 260
- Трансляция телеканалов и (или) радиоканалов — 260
- Транспортирование при эксплуатации — 260
- Трафик — 260
- Требование (Requirement) — 261
- Требование по защите информации — 261

- Трудовая функция — 261
- Трудовое действие — 261
- Туманные вычисления — 261

У

- Уголовное преследование — 261
- Уголовное судопроизводство — 261
- Уголовный закон — 262
- Угроза безопасности информации — 262
- Угроза информационной безопасности Российской Федерации (информационная угроза) — 262
- Угроза национальной безопасности — 262
- Удаленный доступ работника финансовой организации (удаленный доступ) — 262
- Удостоверяющий центр — 262
- Универсальные услуги связи — 263
- Унифицированная процедура в автоматизированной системе — 263
- Уничтожение (Destruction) — 263
- Уничтожение персональных данных — 263
- Уполномоченное учреждение — 263
- Уполномоченные органы — 263
- Уполномоченный орган — 264
- Управление — 264
- Управление документами (Records management) — 264
- Управление инцидентами защиты информации — 264
- Управление сетью связи — 265
- Управленческие меры безопасности (Management controls) — 265
- Управляющая функция автоматизированной системы управления технологическим процессом — 265
- Уровень защиты информации — 265
- Уровень полномочий субъекта доступа (Subject privilege) — 266
- Уровень реагирования на чрезвычайную ситуацию (далее — уровень реагирования) — 266
- Услуга (Service) — 266
- Услуги платежного клиринга — 266
- Услуга по пропуску трафика — 266
- Услуга присоединения — 266
- Услуга связи — 266
- Услуги контентные — 267
- Устройство управления системы обработки информации — 267
- Устройство связи с объектом — 267
- Условия эксплуатации — 267
- Устойчивость автоматизированной системы управления военного назначения — 267

- Участник закупки — 267
- Участник экспериментального режима — 268
- Участники комплексной программы — 268
- Участники комплексного проекта — 268
- Участники консорциума — 268
- Участники платежной системы — 269
- Участники реестра цифровых транзакций — 269
- Участники уголовного судопроизводства — 269
- Участники электронного взаимодействия — 269
- Учетная запись — 269
- Уязвимость (Vulnerability) — 269
- Уязвимость архитектуры — 270
- Уязвимость информационной системы — 270
- Уязвимость кода — 270
- Уязвимость конфигурации — 270
- Уязвимость организационная — 270
- Уязвимость многофакторная — 270

Ф

- Фактический маршрут выполнения функциональных объектов — 270
- Фактор, воздействующий на защищаемую информацию — 271
- Федеральная информационная адресная система — 271
- Федеральная государственная информационная система «Единая система нормативной справочной информации» (ФГИС ЕИСИ) — 271
- Федеральное статистическое наблюдение —
- Федеральный орган исполнительной власти по регулированию контрактной системы в сфере закупок — 271
- Федеральный проект — 272
- Федеральный проект Программы — 272
- Физическая защита информации — 272
- Физический доступ к объекту доступа (физический доступ) — 272
- Финансирующее лицо — 273
- Форма подтверждения соответствия — 273
- Функциональный объект — 273
- Функциональное устройство системы обработки информации — 273
- Функция (Function) — 273
- Функция автоматизированной системы — 274

Х

- Характеристика проекта (Design characteristic) — 274
- Хранение при эксплуатации — 274

Ц

- Целостность (Integrity) — 274
- Целостность информации (Information integrity) — 274
- Цель деятельности — 274
- Цель защиты информации — 274
- Цель процесса (Process purpose) — 275
- Централизованное управление техническими мерами защиты информации — 275
- Центральный платежный клиринговый контрагент — 276
- Центральный процессор — 276
- Цифровая запись — 276
- Цифровая инновация — 276
- Цифровая платформа — 276
- Цифровая повестка — 277
- Цифровая транзакция — 277
- Цифровая трансформация — 277
- Цифровая экономика — 277
- Цифровая экосистема — 278
- Цифровое преобразование — 278
- Цифровое пространство — 278
- Цифровой актив — 278
- Цифровой кошелек — 278
- Цифровой профиль — 278
- Цифровой финансовый актив — 278
- Цифровые инновации — 279
- Цифровые права — 279

Ч

- Частный обвинитель — 279
- Частный партнер — 279
- Чрезвычайная ситуация — 279

Ш

- Шифровальные средства — 280
- Штатная эксплуатация — 280

Э

- ЭВМ общего назначения — 280
- Экосистема цифровой экономики — 280
- Экспериментальный правовой режим — 281
- Эксперт, экспертная организация — 281
- Экспертиза судебная — 281
- Экспертная площадка — 281

-
- Экспертное учреждение — 282
 - Эксплуатационная документация на автоматизированную систему — 282
 - Эксплуатация — 282
 - Эксплуатация объекта соглашения — 282
 - Электронная вычислительная машина — 282
 - Электронная площадка — 283
 - Электронная подпись — 283
 - Электронное сообщение — 283
 - Электронное средство платежа — 283
 - Электронные денежные средства — 283
 - Электронный документ — 284
 - Электромагнитная совместимость — 284
 - Электросвязь — 284
 - Эмуляция — 284
 - Эргономическое обеспечение автоматизированной системы — 284
 - Этап создания автоматизированной системы — 285
 - Эффективность автоматизированной системы — 285
 - Эффективность защиты информации — 285

Я

- Ядро защиты (диспетчер доступа) (Security kernel) — 285
- Язык программирования — 285
- Язык проектирования в САПР — 286
- Ячейка памяти — 286

Ответственность за правонарушения в сфере защиты информации и информационных технологий

Ответственность за правонарушения в сфере защиты информации и информационных технологий предусмотрена статьей 17¹ Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее Федеральный закон № 149-ФЗ), действующего по состоянию на текущую дату в редакции от 29.06.2018 г.

В соответствии с частью 1 этой статьи нарушение требований Федерального закона № 149-ФЗ влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации. При этом в части 1.1. этого Федерального закона отмечается, что лица, виновные в нарушении требований его статьи 14.1², введенной в действие Федеральным законом от 31.12.2017 № 482-ФЗ, в части обработки, включая сбор и хранение, биометрических персональных данных, несут административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Согласно части 2 статьи 17 Федерального закона № 149-ФЗ лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. При этом отмечается, что требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установлен-

¹ Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

² Статья 14.1. Применение информационных технологий в целях идентификации граждан Российской Федерации.

ные законодательством РФ требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

Приложение 3.1

Административная ответственность

Административная ответственность в сфере связи и информации предусмотрена Главой 13 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 года № 195-ФЗ.

В свете темы настоящего издания особый интерес из этой Главы представляют ряд статей, в частности, статьи: 13.6¹; 13.12² и 13.13³.

В интересах исключения неоднозначных трактовок положений этих статей их содержание приведено в виде извлечения.

Статья 13.6. Использование средств связи или несертифицированных средств кодирования (шифрования), не прошедших процедуру подтверждения их соответствия установленным требованиям

1. Использование в сетях связи несертифицированных средств связи или несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети «Интернет», если законодательством предусмотрена их обязательная сертификация, —

влечет наложение административного штрафа
на граждан в размере от 3 000 до 5 000 рублей с конфискацией несертифицированных средств связи либо без таковой;

на должностных лиц — от 15 000 до 30 000 рублей с конфискацией несертифицированных средств связи либо без таковой;

на юридических лиц — от 60 000 до 300 000 рублей с конфискацией несертифицированных средств связи либо без таковой.

2. Использование в сетях связи средств связи без декларации о соответствии, если законодательством не предусмотрена их обязательная сертификация, —

влечет наложение административного штрафа
на должностных лиц в размере от 15 000 до 30 000 рублей с конфискацией незадекларированных средств связи либо без таковой;

на юридических лиц — от 60 000 до 150 000 рублей с конфискацией незадекларированных средств связи либо без таковой.

¹ Статья 13.6. Использование несертифицированных средств связи либо предоставление несертифицированных услуг связи.

² Статья 13.12. Нарушение правил защиты информации.

³ Статья 13.13. Незаконная деятельность в области защиты информации.

Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), —

влечет наложение административного штрафа
на граждан в размере от 1 000 до 1 500 рублей;
на должностных лиц — от 1 500 до 2 500 рублей;
на юридических лиц — от 15 000 до 20 000 рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), —

влечет наложение административного штрафа
на граждан в размере от 1 500 до 2 500 рублей с конфискацией несертифицированных средств защиты информации или без таковой;
на должностных лиц — от 2 500 до 3 000 рублей;
на юридических лиц — от 20 000 до 25 000 рублей с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, —

влечет наложение административного штрафа
на должностных лиц в размере от 2 000 до 3 000 рублей;
на юридических лиц — от 20 000 до 25 000 рублей.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, —

влечет наложение административного штрафа
на должностных лиц в размере от 3 000 до 4 000 рублей;
на юридических лиц — от 20 000 до 30 000 рублей с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

5. Грубое нарушение¹ условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), —

влечет наложение административного штрафа
на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица², в размере от 2 000 до 3 000 рублей или административное приостановление деятельности на срок до 90 суток;

¹ Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности.

² Лиц, осуществляющих индивидуальную предпринимательскую деятельность.

на должностных лиц — от 2 000 до 3 000 рублей;

на юридических лиц — от 20 000 до 25 000 тысяч рублей или административное приостановление деятельности на срок до 90 суток.

6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, за исключением случаев, предусмотренных частями 1, 2 и 5 настоящей статьи, —

влечет наложение административного штрафа

на граждан в размере от 500 до 1 000 рублей;

на должностных лиц — от 1 000 до 2 000 рублей;

на юридических лиц — от 10 000 до 15 000 рублей.

7. Нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, за исключением случаев, предусмотренных частями 3 и 4 настоящей статьи, если такие действия (бездействие) не содержат уголовно наказуемого деяния, —

влечет наложение административного штрафа

на граждан в размере от 1 000 до 2 000 рублей;

на должностных лиц — от 3 000 до 4 000 рублей;

на юридических лиц — от 15 000 до 20 000 рублей.

Статья 13.13. Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), —

влечет наложение административного штрафа

на граждан в размере от 500 до 1 000 рублей с конфискацией средств защиты информации или без таковой;

на должностных лиц — от 2 000 до 3 000 рублей с конфискацией средств защиты информации или без таковой;

на юридических лиц — от 10 000 до 20 000 рублей с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии —

влечет наложение административного штрафа

на должностных лиц в размере от 4 000 до 5 000 рублей;

на юридических лиц — от 30 000 до 40 000 рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.40. Неисполнение обязанностей оператором поисковой системы

1. Неисполнение оператором поисковой системы обязанности по подключению к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен на территории Российской Федерации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, —

влечет наложение административного штрафа

на граждан в размере от 3 000 до 5 000 рублей;

на должностных лиц — от 30 000 до 50 000 рублей;

на юридических лиц — от 500 000 до 700 000 рублей.

2. Неисполнение оператором поисковой системы обязанности по прекращению на территории Российской Федерации выдачи по запросам пользователей указанной поисковой системы сведений об информационных ресурсах, информационно-телекоммуникационных сетях, доступ к которым ограничен на территории Российской Федерации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, —

влечет наложение административного штрафа

на граждан в размере от 3 000 до 5 000 рублей;

на должностных лиц — от 30 000 до 50 000 рублей;

на юридических лиц — от 500 000 до 700 000 рублей.

3. Неисполнение оператором поисковой системы обязанности по прекращению на территории Российской Федерации выдачи по запросам пользователей указанной поисковой системы сведений из доменном имени и об указателях страниц сайтов в сети «Интернет», доступ к которым ограничен на основании соответствующего решения Московского городского суда, или копий заблокированных сайтов —

влечет наложение административного штрафа

на граждан в размере от 3 000 до 5 000 рублей;

на должностных лиц — от 30 000 до 50 000 рублей;

на юридических лиц — от 500 000 до 700 000 рублей.

Статья 19.7.10. Непредставление сведений или представление заведомо недостоверных сведений в орган, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций

1. Непредставление или несвоевременное представление в орган, осуществляющий функции по контролю и надзору в сфере связи, ин-

формационных технологий и массовых коммуникаций, провайдером хостинга или иным лицом, обеспечивающим размещение сайта или страницы сайта в сети «Интернет», данных, позволяющих идентифицировать владельца новостного агрегатора или владельца аудио-визуального сервиса, либо представление в указанный орган заведомо недостоверных сведений —

влечет наложение административного штрафа
на граждан в размере от 10 000 до 30 000 рублей;
на юридических лиц — от 50 000 до 300 000 рублей.

1.1. Непредставление или несвоевременное представление в орган, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций, провайдером хостинга или иным лицом, обеспечивающим размещение в сети «Интернет» программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, данных, позволяющих идентифицировать владельца программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, или сведений об уведомлении владельца программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, о необходимости размещения данных, позволяющих идентифицировать такого владельца, —

влечет наложение административного штрафа
на граждан в размере от 10 000 до 30 000 рублей;
на юридических лиц — от 50 000 до 300 000 рублей.

2. Повторное в течение года совершение административного правонарушения, предусмотренного частями 1 и 1.1 настоящей статьи, —

влечет наложение административного штрафа
на граждан в размере от 30 000 до 50 000 рублей;
на юридических лиц — от 300 000 до 500 000 рублей или административное приостановление деятельности на срок до 30 суток.

В свете обсуждения вопроса об административной ответственности следует отметить положения статей 23.44, 23.45 и 23.46 Главы 23 КоАП, которая называется «Судьи, органы, должностные лица, уполномоченные рассматривать дела об административных правонарушениях».

Статья 23.44. Органы, осуществляющие функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций

1. Органы, осуществляющие функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций, рассматривают дела об административных правонарушениях, предусмотренных

статьями 13.2–13.4, 13.6–13.9, частью 1 статьи 13.18, статьями 13.27.1, 13.29, 13.30, частью 1 статьи 13.31, статьями 13.32, 13.35, 13.36, 13.37, 13.40 частями 2, 3 и 5 статьи 14.3.1, частями 1–3 статьи 15.27 (в пределах своих полномочий), статьями 19.7.10, 19.7.10–1, 19.7.10–2 настоящего Кодекса.

2. Рассматривать дела об административных правонарушениях от имени органов, указанных в части 1 настоящей статьи, вправе:

1) главный государственный инспектор Российской Федерации по надзору в сфере связи, информационных технологий и массовых коммуникаций, его заместители;

2) старшие государственные инспектора Российской Федерации по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Статья 23.45. Федеральные органы исполнительной власти, осуществляющие контроль за обеспечением защиты государственной тайны

1. ФОИВ, осуществляющие контроль за обеспечением защиты государственной тайны, рассматривают дела об административных правонарушениях, предусмотренных частями 3, 4 и 7 статьи 13.12, частью 2 статьи 13.13 настоящего Кодекса.

2. Рассматривать дела об административных правонарушениях от имени органов, указанных в части 1 настоящей статьи, вправе:

1) руководитель ФОИВ, уполномоченного в области обеспечения безопасности РФ, его заместители, руководители территориальных органов указанного ФОИВ, их заместители, начальники структурных подразделений территориальных органов указанного ФОИВ;

2) руководитель ФОИВ, уполномоченного в области обороны, его заместители;

4) руководитель ФОИВ, уполномоченного в области внешней разведки, его заместители;

5) руководитель ФОИВ, уполномоченного в области противодействия техническим разведкам и технической защиты информации, его заместители, руководители территориальных органов указанного ФОИВ, их заместители;

6) руководители подразделений ФОИВ, уполномоченных в области обеспечения безопасности РФ, обороны РФ, внешней разведки, противодействия техническим разведкам и технической защиты информации, осуществляющих лицензирование видов деятельности, которые связаны с использованием и защитой сведений, составляющих государственную тайну, их заместители.

Статья 23.46. Федеральные органы исполнительной власти, осуществляющие государственный контроль в области обращения и защиты информации

1. ФОИВ осуществляющие государственный контроль в области обращения и защиты информации, рассматривают дела об административных

правонарушениях, предусмотренных частями 3 и 4 статьи 13.5, статьей 13.6, частями 1, 2 и 6 статьи 13.12, частью 1 статьи 13.13, статьями 13.17, 13.22, 20.23, 20.24 настоящего Кодекса.

2. Рассматривать дела об административных правонарушениях от имени органов, указанных в части 1 настоящей статьи, вправе:

1.1) руководитель **ФОИВ** в области государственной охраны, его заместители, руководители подразделений указанного **ФОИВ**, их заместители — об административных правонарушениях, предусмотренных частями 3 и 4 статьи 13.5 настоящего Кодекса;

2) руководитель **ФОИВ**, уполномоченного в области противодействия техническим разведкам и технической защиты информации, его заместители, руководители территориальных органов указанного **ФОИВ**, их заместители — об административных правонарушениях, предусмотренных частями 1, 2 и 6 статьи 13.12, частью 1 статьи 13.13 настоящего Кодекса;

3) руководитель **ФОИВ**, уполномоченного в области безопасности РФ, его заместители, руководители территориальных органов указанного **ФОИВ**, их заместители, руководители структурных подразделений указанного **ФОИВ**, их заместители, руководители территориальных органов указанного **ФОИВ**, их заместители, начальники структурных подразделений территориальных органов указанного **ФОИВ** — об административных правонарушениях, предусмотренных частями 3 и 4 статьи 13.5, статьей 13.6, частями 1, 2 и 6 статьи 13.12, частью 1 статьи 13.13, статьями 13.17, 20.23, 20.24 настоящего Кодекса;

4) руководитель **ФОИВ**, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций, его заместители, руководители территориальных органов указанного **ФОИВ**, их заместители — об административных правонарушениях, предусмотренных статьями 13.17, 13.22 настоящего Кодекса.

Приложение 3.2

Уголовная ответственность

Что касается уголовной ответственности, то следует, в первую очередь, руководствоваться положениями статей 272–274 и 274.1 Главы 28¹ Уголовного кодекса РФ от 13 июня 1996 г. № 63-ФЗ.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, —

наказывается штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо исправительными работами на срок до 1 года, либо огра-

¹ Глава 28. Преступления в сфере компьютерной информации.

ничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, —

наказывается штрафом в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо исправительными работами на срок от 1 года до 2 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 4 лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, —

наказываются штрафом в размере до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 5 лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, —

наказываются лишением свободы на срок до 7 лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, —

наказываются ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 4 лет, либо лишением свободы на тот же срок со штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, —

наказываются ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо лишением свободы на срок до 5 лет со штрафом в размере от 100 000 до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период от 2 до 3 лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, —

наказываются лишением свободы на срок до 7 лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и окончного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, —

наказывается штрафом в размере до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, — наказывается принудительными работами на срок до 5 лет либо лишением свободы на тот же срок.

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру РФ

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, —

наказываются принудительными работами на срок до 5 лет с ограничением свободы на срок до 2 лет или без такового либо лишением свободы на срок от 2 до 5 лет со штрафом в размере от 500 000 до 1 000 000 рублей

или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет.

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру РФ, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре РФ, —

наказывается принудительными работами на срок до 5 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет и с ограничением свободы на срок до 2 лет или без такового либо лишением свободы на срок от 2 до 6 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 3 лет.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре РФ, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре РФ, —

наказывается принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового либо лишением свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.

4. Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, —

наказываются лишением свободы на срок от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.

5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия, —

наказываются лишением свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. М.: Проспект, 2020. 640 с.
2. Финансовое право в условиях развития цифровой экономики: монография / К. Т. Анисина, Б. Г. Бадмаев, И. В. Бит-Шабо и др.; под ред. И. А. Цинделиани. М.: Проспект, 2019. 320 с.
3. Проблемы гармонизации экономических отношений и права в цифровой экономике: монография / колл. авторов; МГУ имени М. В. Ломоносова, Университет имени О. Е. Кутафина (МГЮА), Московское отделение ассоциации юристов России, Международный союз юристов и экономистов (Франция); отв. ред. В. А. Вайпан, М. А. Егорова. М.: Юстицинформ, 2020. 280 с.
4. Антимонопольное регулирование в цифровую эпоху: как защитить конкуренцию в условиях глобализации и четвертой промышленной революции: монография / нац. исслед. ун-т «Высшая школа экономики» ФАС России: «Антимонопольное регулирование в цифровую эпоху: как защитить конкуренцию в условиях глобализации и четвертой промышленной революции»; под ред. А. Ю. Цариковского, А. Ю. Иванова и Е. А. Войниканис. 2-е изд., испр. и доп. М.: Изд. дом Высшей школы экономики, 2019. 391 с.
5. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: «Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: монография» / колл. авторов / Московское отделение Ассоциации юристов России, МГУ имени М. В. Ломоносова, Ассоциация российских дипломатов / отв. ред. В. А. Вайпан, М. А. Егорова. М.: Юстицинформ, 2019. 376 с.
6. *Вайпан В. А.* Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11. С. 5–18.
7. *Городов О. А., Егорова М. А.* Основные направления совершенствования правового регулирования в сфере цифровой экономики в России // Право и цифровая экономика. 2018. № 1. С. 6–12.
8. *Зорькин В. Д.* Право в цифровом мире // РГ. 2018. № 115 (7578). 30 мая. С. 1, 4.

9. *Ландабасо А. И.* Европейская модель цифровизации экономики: опыт для России // *Право и цифровая экономика*. 2018. № 2. С. 5–14.
10. *Санникова Л. В., Харитоновна Ю. С.* Цифровые активы и технологии: некоторые правовые проблемы выработки понятийного аппарата // *Право и цифровая экономика*. 2018. № 1. С. 25–30.
11. *Ступаченко Е. В.* О некоторых вопросах возможности использования технологии блокчейн в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд // *Журнал предпринимательского и корпоративного права*. 2018. № 4. С. 18–21.
12. *Гринев В. П.* О возможностях использования проектных методов в закупочной деятельности в условиях ее цифровой трансформации // *Шаг в будущее: искусственный интеллект и цифровая экономика. Революция в управлении: новая цифровая экономика или новый мир машин: материалы II Международного научного форума*. Вып. 3. М.: Издательский дом ГУУ, 2018. С. 27–36.
13. *Гринев В. П.* Государственное регулирование цифровой экономики // *Право и цифровая экономика*. 2018. № 2. С. 15–22.
14. *Гринев В. П.* Проектное управление развитием и использованием информационно-коммуникационных технологий в цифровой экономике // *E-MANAGEMENT*. 2018. Т. 1. № 2. С. 67–79.
15. *Гринев В. П.* К вопросу о новых возможностях обеспечения государственных нужд в условиях цифровой экономики и проблемах правоприменения при переводе закупок в электронную форму // *Публичные закупки: проблемы правоприменения. Материалы VI Международной научно-практической конференции (8 июня 2018 г., МГУ имени М. В. Ломоносова)*. М.: Юстицинформ, 2018. С. 50–62.
16. *Гринев В. П.* К вопросу о переводе публичных закупок в электронную форму // *Публичные закупки: проблемы правоприменения. Материалы VI Международной научно-практической конференции (8 июня 2018 г., МГУ имени М. В. Ломоносова)*. М.: Юстицинформ, 2018. С. 32–49.
17. *Гринев В. П.* Особенности закупочной деятельности в сфере обеспечения информационной безопасности: правовые аспекты // *Публичные закупки: проблемы правоприменения. Материалы VII Международной научно-практической конференции (13–14 июня 2019 г., МГУ имени М. В. Ломоносова)*. М.: Юстицинформ, 2019. С. 55–68.
18. *Гринев В. П.* Жилищное и градостроительное законодательство. Словарь-справочник. М.: ГроссМедиа, 2006.
19. *Гринев В. П.* Законодательство о пожарной безопасности и чрезвычайных ситуациях. Словарь-справочник. М.: ОАО ЦПП, 2009.
20. *Гринев В. П.* Контрактная система как механизм нормоконтроля расходования бюджетных средств // *Право и экономика*. 2015. № 7. С. 37–44.

21. *Гринеv В. П.* Возможности цифровой сети с интеграцией обслуживания и эргатические системы управления // Информационная безопасность России: Информационно-аналитический бюллетень. Специальный выпуск. М.: Клуб «Реалисты», 1998. С. 97–101.
22. *Лобовский И. М., Гринеv В. П.* Цифровая наложенная сеть КОМСТАР — инфраструктурный модуль телекоммуникационных систем поддержки принятия решений с интеграцией услуг // Анализ систем на пороге XXI века: теория и практика. Материалы Международной конференции. В 4-х т. Т. 3. М.: Интеллект, 1996.
23. *Заморин А. П., Марков А. С.* Толковый словарь по вычислительной технике и программированию: Основные термины. М.: Русский язык, 1988.
24. *Анисина К. Т.* Взаимодействие государственных органов власти с другими участниками финансовых правоотношений посредством цифровой экономики // Финансовое право. 2018. № 9. С. 5–9.
25. *Лопатин В. Н.* Информационная безопасность в электронном государстве // Информационное право. 2018. № 2. С. 14–19.
26. *Шарандина Н. Л.* Цифровая экономика как приоритетная национальная цель развития Российской Федерации: правовой аспект // Финансовое право. 2018. № 9. С. 17–21.
27. *Шарандина Н. Л.* Цифровая экономика и формирование налоговой культуры: правовой аспект // Финансовое право. 2019. № 10. С. 25–32.
28. *Дремлюга Р. И.* Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // Уголовное право. 2018. № 4. С. 52–57.
29. *Дремлюга Р. И.* Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 6. С. 129–133.
30. *Соловых Н. Н.* Цифровая экономика диктует необходимость квалифицированных кадров с новыми компетенциями // Российский следователь. 2018. № 5. С. 64–68.
31. *Алиев В. М.* Политико-правовые аспекты перехода к цифровой экономике в России // Российский следователь. 2018. № 9. С. 48–52.
32. *Лопатин В. Н.* Информационная безопасность в электронном государстве // Информационное право. 2018. № 2. С. 14–19.
33. *Лопатин В. Н.* Проблемы информационной безопасности и риски интеллектуальной собственности в цифровой экономике // Информационное право. 2017. № 2. С. 8–16.
34. *Танимов О. В.* Влияние цифровых технологий на появление новых структурных элементов системы права // Российская юстиция. 2019. № 7. С. 2–5.
35. *Валеев Д. Х., Нуриев А. Г.* Российское правосудие в реалиях цифровой экономики // Арбитражный и гражданский процесс. 2019. № 5. С. 3–8.

36. *Тютюнник И. Г., Толкачев С. А.* Нормативно-правовое обеспечение конкурентоспособности социально-экономических систем в условиях цифровой экономики // *Безопасность бизнеса.* 2019. № 3. С. 10–15.
37. *Веремева О. В.* Совершенствование бюджетного законодательства в условиях построения цифровой экономики в Российской Федерации // *Финансовое право.* 2019. № 1. С. 26–30.
38. *Шестакова Е., Жиркова А.* Цифровые права и электронные сделки. Какое будущее у цифровизации юридического сопровождения бизнеса // *Финансовая газета.* 2019. № 28. С. 10–11.
39. *Алиев В. М., Соловых Н. Н.* Цифровая экономика поставила нас перед необходимостью решения проблемы обеспечения цифрового суверенитета // *Безопасность бизнеса.* 2018. № 3. С. 18–22.
40. *Тропская С. С.* Финансовый рынок в условиях развития цифровой экономики (финансово-правовой аспект) // *Финансовое право.* 2018. № 8. С. 28–33.
41. *Белицкая А. В.* Перспективы разработки новых правовых конструкций инвестирования для цифровой экономики // *Юрист.* 2019. № 3. С. 28–33.
42. *Абрамян Т. А.* Актуальные проблемы привлечения к ответственности лиц за преступления в сфере информационных технологий // *Юрист.* 2018. № 5. С. 68–72.
43. *Филимонов С. А.* Проблемы борьбы с компьютерным мошенничеством как потенциальной угрозой информационному сообществу // *Современное право.* 2014. № 9. С. 123–127.

ОГЛАВЛЕНИЕ

Принятые сокращения.....	3
Введение.....	7
1. Цифровая экономика: настоящее и будущее.....	12
2. Правовые аспекты правового регулирования закупочной деятельности в сфере обеспечения информационной безопасности цифровой экономики	41
3. Профессиональные стандарты в сфере обеспечения информационной безопасности цифровой экономики	59
3.1. Общие положения	59
3.2. Порядок применения профессиональных стандартов.....	80
4. Термины, нормы и определения основных понятий законодательства о цифровой экономике и обеспечения ее информационной безопасности.....	84
А.....	84
Б.....	92
В.....	96
Г.....	104
Д.....	107
Е.....	113
Ж.....	113
З.....	115
И.....	124
К.....	138
Л.....	150
М.....	154
Н.....	164
О.....	171
П.....	191
Р.....	215

С.....	227
Т.....	253
У.....	262
Ф.....	271
Х.....	275
Ц.....	275
Ч.....	280
Ш.....	280
Э.....	281
Я.....	286

Приложение 1

Перечень основных нормативных правовых актов по вопросам регулирования цифровой экономики и информационной безопасности	287
---	-----

Приложение 2

Алфавитный указатель терминов и определений основных понятий законодательства о цифровой экономике и информационной безопасности	340
--	-----

Приложение 3

Ответственность за правонарушения в сфере защиты информации и информационных технологий	368
Список использованной литературы	379

95.9000

