МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ
ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ НИЗАМИ

И.У. НАЗАРОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УЧЕБНОЕ ПОСОБИЕ ДЛЯ СТУДЕНТОВ ВЫСШИХ ПЕДАГОГИЧЕСКИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

Ташкент - 2019

Назаров И.У. «Информационная безопасность». Учебное пособие предназначено для студентов высших педагогических учебных заведений, обучающихся по специальности 5110700 - *«Методика преподавания информатики»*

ANNOTATSIYA

Ushbu o‘quv qo‘llanmani yozishdan asosiy maqsad talabalarni axborot xavfsizligi asoslari, axborot xavfsizligi muammolari va ularni hal yetishga yondashuvlar bilan tanishtirishdan iborat.

O‘quv qo‘llanmada axborot xavsizligining asosiy tushunchalari, axborot xavfsizligi sohasiga tegishli chora va tadbirlar, foydalanuvchining identifikatsiya va autentifikatsiya masalalari, kriptografik himoya va axborot yaxlitligini nazorat qilish, asosiy tizimlarni tashkil yetish, yerkin foydalanishni farqlash masalalari, xavfsizlik siyosati modellari va axborot xavfsizligi standartlari haqida umumiy fikrlar keltirilgan.

Har bir bo‘limda o‘z-o‘zini nazorat uchun savollar mavjud.

АННОТАЦИЯ

Целью данного учебного пособия является ознакомление студентов с основами информационной безопасности, проблемами защиты информации и подходами к их решению.

Рассматриваются основные понятия информационной безопасности, структура мер в области ИБ, вопросы идентификации и аутентификации пользователей, криптографической защиты и контроля целостности информации, организации ключевых систем, вопросы разграничения доступа, модели политик безопасности, обзор стандартов информационной безопасности.

В каждом разделе имеются вопросы для самоконтроля.

ANNOTATION

The purpose of data educational the grant is acquaintance of students with bases of information safety of computer systems, problems of protection of the information and approaches to their decision.

The basic concepts of information safety, structure of measures in the field of Information Security, questions of identification and authentication users, cryptographic protection and the control of integrity of the information, the organization of key systems, questions of differentiation of access, model the politician of safety, the review of standards of information safety are considered.

Рецензенты:

д.п.н., профессор А.А. Абдукадыров,

д.э.н., профессор Р.Х. Аюпов.

ПРЕДИСЛОВИЕ

Информационная безопасность (ИБ) - сравнительно молодая, быстроразвивающаяся область информационных технологий *(ИТ*), для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими *ветвями ИТ*. Быстро развивающиеся компьютерные информационные технологии вносят заметные изменения в нашу жизнь. Все чаще понятие "информация" используется как обозначение специального товара, который можно приобрести, продать, обменять на что-то другое и т. п. При этом стоимость информации часто превосходит в сотни и тысячи раз стоимость компьютерной системы, в которой она находится. Поэтому вполне естественно возникает необходимость в защите информации от *несанкционированного доступа, умышленного изменения, кражи, уничтожения* и других преступных действий.

Проблемы защиты информации привлекают все большее внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей современных компьютерных средств. В то же время эта актуальная проблематика компьютерной науки и практики пока недостаточно освещена в отечественной научно-технической и учебной литературе.

В книге подробно излагаются классические методы шифрования и современные криптографические методы, алгоритмы, протоколы и системы. Описаны методы и средства защиты локальных и корпоративных сетей от удаленных атак через сеть *Internet*, а также рассмотрена защита информации в электронных платежных системах. Приводятся подробные данные об эффективных аппаратно-программных средствах криптографической защиты компьютерной информации.

В основу книги положены материалы лекций, читаемым автором на кафедре *"Методика преподавания информатики"* Ташкентского государственного педагогического университета имени Низами.

Автор понимает, что книга со временем может быть улучшена за счет корректировок, и заранее благодарит читателей, которые поспособствуют изменению и дополнению материала данного учебного пособия.

ВВЕДЕНИЕ

Актуальной проблемой в условиях информатизации для всех организаций и учреждений *(любых форм собственности)* становится проблема информационной безопасности. Проблемы защиты информации волновали человечество с незапамятных времен. Необходимость защиты информации возникла из потребностей тайной передачи, как военных, так и дипломатических сообщений. Например, античные спартанцы шифровали свои военные сообщения. У китайцев простая запись сообщения с помощью иероглифов делала его тайным для чужестранцев.

Для обозначения всей области тайной *(секретной)* связи используется термин "криптология", который происходит от греческих корней "*cryptos*"- тайный и "*logos*"- сообщение. Криптология довольно четко может быть разделена на два направления: криптографию и криптоанализ.

Задача криптографа - обеспечить конфиденциальность *(секретность)* и аутентичность *(подлинность)* передаваемых сообщений.

Задача криптоаналитика - «взломать» систему защиты, разработанную криптографами. Он пытается раскрыть зашифрованный текст или выдать поддельное сообщение за настоящее.

Первые каналы связи были очень простыми. Их организовывали, используя надежных курьеров. Безопасность таких систем связи зависела как от надежности курьера, так и от его способности не попадать в ситуации, при которых могло иметь место раскрытие сообщения.

Создание современных компьютерных систем и появление глобальных компьютерных сетей радикально изменило характер и диапазон проблем защиты информации. В широко компьютеризированном и информатизированном современном обществе обладание реальными ценностями, управление ими, передача ценностей или доступ к ним часто основаны на неовеществленной информации, т.е. на информации, существование которой не обязательно связывается с какой-либо записью на физическом носителе. Поэтому весьма важно создавать и применять

эффективные средства для реализации всех необходимых функций, связанных с обеспечением конфиденциальности и целостности информации.

Поскольку информация может быть очень ценной или особо важной, возможны разнообразные злонамеренные действия по отношению к компьютерным системам, хранящим, обрабатывающим или передающим такую информацию. Например, нарушитель может попытаться выдать себя за другого пользователя системы, подслушать канал связи или перехватить и изменить информацию, которой обмениваются пользователи системы. Нарушителем может быть и пользователь системы, который отказывается от сообщения, в действительности сформированного им, или который пытается утверждать, что им получено сообщение, которое в действительности не передавалось. Он может попытаться расширить свои полномочия, чтобы получить доступ к информации, к которой ему предоставлен только частичный доступ, или попытаться разрушить систему, не санкционированно изменяя права других пользователей.

Для решения указанных и других подобных проблем не существует какого-то одного технического приема или средства. Однако общим в решении многих из них является использование криптографии и криптоподобных преобразований информации.

На протяжении более чем тысячелетней истории криптографии она представляла собой постоянно обновляющийся и совершенствующийся набор технических приемов шифрования и расшифрования, которые сохранялись в строгом секрете.

Период развития криптологии с древних времен до 1949 г. принято называть эрой донаучной криптологии, поскольку достижения тех времен были основаны на интуиции и не подкреплялись доказательствами. Криптологией занимались тогда почти исключительно как искусством, а не как наукой. Конечно, это не означает, что история криптологии тех времен не представляет для нас никакого интереса. Более 2000 лет назад Юлий Цезарь

писал Цицерону и друзьям в Риме, используя шифр, теперь названный его именем.

Публикация статьи К. Шеннона "Теория связи в секретных системах" *(1949)* стала началом новой эры научной криптологии с секретными ключами. В этой работе Шеннон связал криптографию с теорией информации.

С середины семидесятых годов *(в связи с изобретением систем с открытым ключом)* криптография не только перестала быть секретным сводом приемов шифрования-расшифрования, но и начала оформляться в новую математическую теорию. На последние двадцать лет пришлось значительное повышение активности в области развития криптографии и ее применения для решения проблем защиты информации. Это вызвано широким признанием крайней необходимости в средствах обеспечения защиты информации во всех областях деятельности широко информатизированного человеческого сообщества и обусловлено появлением таких новых фундаментальных идей, как асимметричная *(с открытым ключом)* криптография, доказательно стойкие протоколы, надежность которых основана на гарантированной сложности решения математических задач, и т.д.

В криптографической системе преобразование шифрования может быть симметричным или асимметричным относительно преобразования рас шифрования. Соответственно различают два класса криптосистем:

- *симметричные* одно ключевые криптосистемы *(с секретным ключом)*;
- *асимметричные* двух ключевые криптосистемы *(с открытым ключом)*.

Современные симметричные одно ключевые крипто алгоритмы базируются на принципах, изложенных в упомянутой работе Шеннона. К ним относятся зарубежные крипто алгоритмы **DES** и **IDEA**. Схемы реализации этих крипто алгоритмов открыто опубликованы и тщательно проанализированы многими исследователями. В этих криптосистемах

секретным является только ключ, с помощью которого осуществляется шифрование и расшифрование информации. Данные криптосистемы могут использоваться не только для шифрования, но и для проверки подлинности *(аутентификации)* сообщений.

Появлению нового направления в криптологии-асимметричной криптографии с открытым ключом-способствовали две проблемы, которые не удавалось решить в рамках классической симметричной одноключевой криптографии.

Первая из этих проблем связана с распространением секретных ключей. Наличие секретного ключа, известного только получателю сообщения и его отправителю, столетиями считалось непременным условием безопасной передачи информации. Но при использовании симметричных криптосистем с секретными ключами требуют решения следующие вопросы. Как передать участникам обмена информацией сменяемые секретные ключи, которые требуются им для выполнения этого обмена? Как участники обмена смогут убедиться в целостности того, что они получили?

Вторая из этих проблем связана с формированием электронной цифровой подписи. В конце письма или другого авторизованного документа отправитель обычно ставит свою подпись. Подобное действие преследует две цели: во-первых, получатель может убедиться в подлинности письма, сличив подпись с имеющимся у него образцом; во-вторых, личная подпись является юридическим гарантом авторства документа.

Обе эти проблемы казались трудноразрешимыми. Однако они были успешно решены с помощью криптографии с открытыми ключами в опубликованной статье *"Новые направления в криптографии" (1976).* У. Диффи и М. Хеллман впервые показали, что секретная связь возможна без передачи секретного ключа между отправителем и получателем. В основе этого криптографического метода лежат так называемые однонаправленные *(односторонние)* функции: при заданном значении *x* относительно просто

вычислить значение ***f(x)***, однако, зная ***y = f(x)***, определить по ***y*** значения ***x*** чрезвычайно трудно.

В *асимметричных криптосистемах* с открытым ключом используются два ключа, по крайней мере, один из которых невозможно вычислить из другого. Один ключ используется отправителем для шифрования информации; другой - получателем для рас шифрования получаемых шифр текстов. Обычно в приложениях один ключ должен быть несекретным, а другой-секретным.

Если ключ расшифрования невозможно получить из ключа зашифрования с помощью вычислений, то секретность информации, зашифрованной на несекретном *(открытом)* ключе, будет обеспечена. Однако этот ключ должен быть защищен от подмены или модификации, иначе отправитель может быть обманут и будет выполнять зашифрование на поддельном ключе, соответствующий ключ расшифрования которого известен противнику. Для того чтобы обеспечить закрытие информации, ключ расшифрования получателя должен быть секретным и физически защищенным от подмены. Так работает канал обеспечения конфиденциальности *(секретности)* информации.

Если же, наоборот, вычислительно невозможно получить ключ шифрования из ключа расшифрования, то ключ расшифрования может быть несекретным, а секретный ключ шифрования можно использовать для формирования электронной цифровой подписи под сообщением. В этом случае, если результат расшифрования цифровой подписи содержит аутентификационную информацию *(заранее согласованную законным отправителем информации с потенциальным получателем)*, эта подпись удостоверяет целостность сообщения, полученного от отправителя. Так работает канал аутентификации сообщения.

Кроме задачи аутентификации сообщения в проблеме аутентификации можно выделить еще две:

• задачу аутентификации пользователя-является ли пользователь, обращающийся к ресурсам компьютерной системы, именно тем, за кого он себя выдает?

• задачу взаимной аутентификации абонентов сети в процессе установления соединения между ними.

Обе эти задачи также успешно решаются с привлечением криптографических методов и средств.

Появление новых информационных технологий и интенсивное развитие компьютерных сетей привлекают все большее внимание пользователей к глобальной сети *Internet*. Подключение к *Internet* дает большие преимущества, однако при этом возникают серьезные проблемы с обеспечением информационной безопасности подключаемой локальной или корпоративной сети. В силу открытости своей идеологии *Internet* предоставляет злоумышленникам много возможностей для вторжения во внутренние сети организаций с целью хищения, искажения или разрушения важной и конфиденциальной информации. Решение задач по защите внутренних сетей от наиболее вероятных атак через *Internet* может быть возложено на межсетевые экраны, иногда называемые брандмауэрами или firewall. Применяются и программные методы защиты, к которым относятся защищенные криптопротоколы SSL и SKIP.

ГЛАВА 1. ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

==========

1-§. Основные понятия безопасности информации

Ключевые слова: *информационная безопасность, угроза, объект, компьютерное мошенничество, подделка, повреждение данных, компьютерный саботаж, несанкционированный доступ, нарушение авторских прав, неавторизованный доступ, авторство, ущерб.*

Проблема обеспечения информационной безопасности в рамках любого государства в последнее время все чаще является предметом обсуждения не только в научных кругах, но и на политическом уровне. Данная проблема также становится объектом внимания международных организаций, в том числе и ООН.

Информационная безопасность – это защищенность информационной среды общества посредством различных *средств* и *методов*.

Под *информационной средой* понимается совокупность информационных ресурсов и наличие соответствующей инфраструктуры их создания и использования. Целью информационной безопасности является предотвращение влияния неблагоприятных событий *(угроз)* или обеспечение минимального ущерба от них информационной среде.

Современный этап развития общества характеризуется возрастающей ролью электронных ресурсов, представляющих собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений.

Стремительный рост компьютерных технологий в различных сферах человеческой деятельности, с одной стороны, позволил обеспечить высокие

достижения в этих сферах, а с другой стороны, стал источником самых непредсказуемых и вредных для человеческого общества последствий. В результате, можно говорить о появлении принципиально нового сегмента международного противоборства, затрагивающего как вопросы безопасности отдельных государств, так и общую систему международной безопасности на всех уровнях.

Становится очевидной необходимость теоретической разработки международно-правовых основ регулирования взаимоотношений субъектов международного права в сфере качественно изменяющихся под воздействием информационной революции условий обеспечения международной и национальной безопасности, в сфере обеспечения информационной безопасности государства.

Новые технологии порождают и новые преступления. Согласно унификации Комитета министров Европейского Совета, определены криминальные направления компьютерной деятельности. К ним относятся [9]:

- компьютерное мошенничество;
- подделка компьютерной информации;
- повреждение данных или программ;
- компьютерный саботаж;
- несанкционированный доступ к информации;
- нарушение авторских прав.

Актуальность проблемы информационной безопасности заключается[1]:

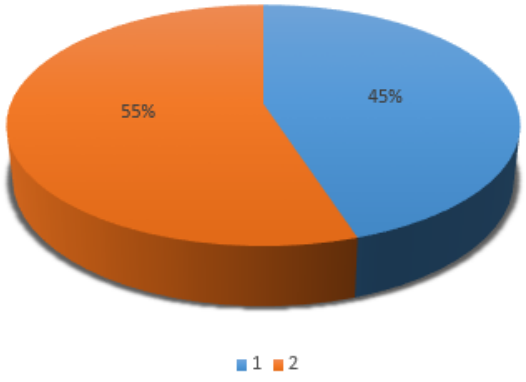
- в особом характере общественной опасности возможных преступлений;
- в наличии тенденции к росту числа преступлений в информационной сфере;

[1] *John R. Vacca. Computer and Information Security Handbook, Third Edition 3rd Edition. Morgan Kaufmann Pub; 3 edition (June 15, 2017). 1280 pages*

- в не разработанности ряда теоретических положений, связанных с информационной безопасностью.

Проблема обеспечения безопасности носит комплексный характер, для ее решения необходимо сочетание законодательных, организационных и программно-технических мер и средств. В курсе Информационной безопасности нас будут интересовать программно-технические средства, реализующиеся программным и аппаратным обеспечением, решающие разные задачи по защите. Они могут быть встроены в операционные системы, либо могут быть реализованы в виде отдельных продуктов. Во многих случаях центр тяжести смещается в сторону защищенности операционных систем [9].

Генеральная Ассамблея ООН приняла резолюцию, в которой выражается озабоченность тем, что распространение и использование современных информационных технологий и средств потенциально может быть использовано в целях, несовместимых с задачами обеспечения международной стабильности и безопасности[2]. *(рис. 1.1.1).*



(рис. 1.1.1). Соотношение различных вилов атак

Специалистам в области информационной безопасности сегодня почти невозможно обойтись без знаний соответствующих стандартов и спецификаций. На то имеется несколько причин.

[2] *John R. Vacca. Computer and Information Security Handbook, Third Edition 3rd Edition. Morgan Kaufmann Pub; 3 edition (June 15, 2017). 1280 pages*

Формальная состоит в том, что необходимость следования некоторым стандартам закреплена законодательно. Однако наиболее убедительны содержательные причины.

Во-первых, стандарты и спецификации - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях информационной безопасности. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами.

Во-вторых, и те, и другие являются основным средством обеспечения взаимной совместимости аппаратно - программных систем и их компонентов.

Среди множества различных стандартов и спецификаций, можно выделить две группы документов, которые будут рассмотрены в данном курсе [12]:

- оценочные стандарты, предназначенные для оценки и классификации информационных систем и средств защиты по требованиям безопасности;
- спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты.

Эти группы, разумеется, дополняют друг друга. Оценочные стандарты описывают важнейшие, с точки зрения информационной безопасности, понятия и аспекты информационных систем *(ИС)*, играя роль организационных и архитектурных спецификаций. Спецификации определяют, как именно строить ИС предписанной архитектуры и выполнять организационные требования.[3]

Из числа оценочных необходимо выделить стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» *(Trusted Computer System Evaluation Criteria-TCSEC)* и его интерпретацию для

[3] *John R. Vacca. Computer and Information Security Handbook, Third Edition 3rd Edition. Morgan Kaufmann Pub; 3 edition (June 15, 2017). 1280 pages*

сетевых конфигураций *(Trusted Network Interpretation)*, «Гармонизированные критерии Европейских стран» *(Information Technology Security Evaluation Criteria (ITSEC)*. Harmonised Criteria of France - Germany- the Netherlands - the United Kingdom, международный стандарт «Критерии оценки безопасности информационных технологий» *(Common Criteria for Information Technology Security Evaluation (CCITSE)*. К этой же группе относятся: Федеральный стандарт США *(Federal Information Processing Standardization, FIPS)* «Требования безопасности для криптографических модулей» *(FIPS 140-2)*, Британский стандарт BS 7799 часть 2. «Управление информационной безопасностью. Практические правила» *(Information Security Management Systems - Specification with guidance for use)*, а также международный стандарт ISO/IEC 17799 «Информационная технология. Практический кодекс по менеджменту информационной безопасности» *(Information Technology – Code of practice for information security management)*, являющийся изложением BS 7799 часть 1.

Технические спецификации, применимые к современным распределенным ИС, создаются, главным образом, «Тематической группой по технологии Интернет» *(Internet Engineering Task Force, IETF)* и ее подразделением – рабочей группой по безопасности. Ядром рассматриваемых технических спецификаций служат документы по безопасности на IP-уровне *(IPsec)*. Кроме этого, анализируется защита на транспортном уровне *(Transport Layer Security, TLS)*, а также на уровне приложений *(спецификации GSS-API, Kerberos)*. Акцентируется внимание на административном и процедурном уровнях безопасности *(«Руководство по информационной безопасности предприятия», «Как выбирать поставщика интернет-услуг», «Как реагировать на нарушения информационной безопасности»)*.

В вопросах сетевой безопасности невозможно разобраться без освоения спецификаций:

X.800 «Архитектура безопасности для взаимодействия открытых систем»;

X.500 «Служба каталогов: обзор концепций, моделей и сервисов»;

X.509 «Служба каталогов: каркасы сертификатов открытых ключей и атрибутов».

Это «стандартный минимум», которым должны активно владеть все действующие специалисты в области информационной безопасности.

По существу, проектирование системы безопасности подразумевает ответы на следующие вопросы [12]:

- какую информацию защищать;
- какого рода атаки на безопасность системы могут быть предприняты;
- какие средства использовать для защиты информации каждого вида.

Поиск ответов на данные вопросы называется формированием политики безопасности, которая помимо чисто технических аспектов включает также и решение организационных проблем. На практике реализация политики безопасности состоит в присвоении субъектам и объектам идентификаторов, фиксации набора правил, позволяющих определить, имеет ли данный субъект авторизацию, достаточную для предоставления к данному объекту указанного типа доступа.

Формируя политику безопасности, необходимо учитывать несколько базовых принципов. Так, Зальтцер и Шредер на основе своего опыта работы сформулировали следующие рекомендации для проектирования системы безопасности операционных систем[4]:

- Проектирование системы должно быть открытым. Нарушитель и так все знает *(криптографические алгоритмы открыты)*.
- Не должно быть доступа по умолчанию. Ошибки с отклонением легитимного доступа будут обнаружены скорее, чем ошибки там, где разрешен неавторизованный доступ.

---

[4] *John R. Vacca. Computer and Information Security Handbook, Third Edition 3rd Edition. Morgan Kaufmann Pub; 3 edition (June 15, 2017). 1280 pages*

- Нужно тщательно проверять текущее авторство. Так, многие системы проверяют привилегии доступа при открытии файла и не делают этого после. В результате пользователь может открыть файл и держать его открытым в течение недели и иметь к нему доступ, хотя владелец уже сменил защиту.
- Давать каждому процессу минимум возможных привилегий.
- Защитные механизмы должны быть просты, постоянны и встроены в нижний слой системы, это не аддитивные добавки *(известно много неудачных попыток «улучшения» защиты слабо приспособленной для этого ОС)*.
- Важна физиологическая приемлемость. Если пользователь видит, что защита требует слишком больших усилий, он от нее откажется.
- Ущерб от атаки и затраты на ее предотвращение должны быть сбалансированы.

Приведенные соображения показывают необходимость продумывания и встраивания защитных механизмов на самых ранних стадиях проектирования системы.

Вопросы для самоконтроля

1. Дайте определение информационной безопасности.
2. Чем определяется информационная безопасность?
3. Какие исторические события можно связать с понятием «нарушение информационной безопасности»?
4. Что относится к субъектам информационных отношений?
5. Перечислите виды компьютерных преступлений.
6. Какие руководящие документы существуют в области информационной безопасности?
7. Какие стандарты и спецификации информационной безопасности вы знаете?
8. Приведите список угроз безопасности информационной системы.

9. Приведите список мер противодействия угрозам информационной безопасности.

2-§. Защита информации и её виды

Ключевые слова: *безопасность, информационная безопасность, защита информации, уровни защиты информации, маркирование документов, закрытое обсуждение, шифрование информации, использование соглашения о конфиденциальности, ограничение доступа к информации*

Изучение любой дисциплины необходимо начинать с освоения понятийного аппарата ее предметной области. Раскрытие значений некоторых ключевых терминов позволяет сформировать начальные представления о целях и задачах защиты информации. Терминология в области защиты информации изложена в законах, указах Президента, постановлениях Правительства, государственных и отраслевых стандартах.

Прежде всего определимся с объектом защиты. *Под информацией понимается:*

1. сообщение, осведомление о положении дел, сведения о чем-либо, передаваемые людьми;
2. *(в теории вероятности)* уменьшаемая, снимаемая неопределенность в результате получения сообщений;
3. *(с точки зрения математических подходов)* сообщение, неразрывно связанное с управлением, сигналы в единстве синтаксических, семантических и прагматических характеристик;
4. передача, отражение разнообразия в любых объектах и процессах *(неживой и живой природы)* [9].

Трудно переоценить роль информации в современном мире. По мнению многих ученых, именно информация является решающим фактором в конкурентной борьбе государств. Так, на Западе пользуется популярностью

классификация, в соответствии с которой все страны делятся по уровню их развития следующим образом:

- страны, способные производить и продавать информационные услуги;
- страны, не производящие информационных услуг на продажу, но создающие и продающие промышленные товары;
- страны, не производящие ни информационных услуг, ни товаров и являющиеся поставщиками сырья и рабочей силы в страны первых двух классов.

Владение информацией необходимого качества в нужное время и в нужном месте является залогом успеха в любом виде хозяйственной деятельности. Монопольное обладание определенной информацией оказывается зачастую решающим преимуществом в конкурентной борьбе, именно поэтому собственнику необходимо ее защищать.

Выделяются два вида собственной информации у предпринимателя: техническая *(технологическая)* и деловая информация. К первому типу относятся, например, методы производства продукции, программное обеспечение и т.п. Ко второму типу относятся, например, бизнес - планы предприятия, списки клиентов, материалы различных заказных исследований.

Уточним, что понимается под безопасностью информации.

Безопасность - это «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Понятие защищенности указывает на способность *(степень, уровень)* противостояния конкретным, четко сформулированным угрозам.

В прикладном аспекте, на более низком уровне, чем государство и общество в целом, безопасность определяется как состояние защищенности жизненно важных интересов человека, общества, государства и субъекта защиты в определенной сфере отношений при соблюдении баланса интересов между ними.

Анализ отечественных и зарубежных источников показывает, что в основном все определения понятия безопасности включают следующие основные положения: наличие внутренних и внешних угроз, наличие жизненно важных интересов и соблюдение баланса интересов. Первичным в определениях безопасности является наличие угроз и опасностей, наличие жизненно важных интересов вторично.

Под безопасностью информации понимается такое ее состояние, при котором исключается возможность ознакомления с этой информацией, ее изменения или уничтожения лицами, не имеющими на это права, а также утечки за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (*уничтожения*) при передаче между объектами вычислительной техники[5].

Информационная безопасность - это один из лучших переводов английского термина ***information security***.

По другому его можно перевести - *"защита информации"*. Информация является одним из наиболее ценных ресурсов, поэтому обеспечение защиты информации является одной из важнейших и приоритетных задач [9].

Защита информации - действия и средства по предотвращению утечки, хищению, искажению или подделки информации.

В общем виде систему защиты информации можно представить, как многоуровневый комплекс, включающий в себя организационные, организационно-технические мероприятия, предусматривающие применение инженерно-технических и программных *(программно-аппаратных)* средств защиты на всех этапах обработки, хранения и транспортировки информации.

[5] *The InfoSec Handbook: An Introduction to Information Security 2014th Edition by Umesh Hodeghatta Rao.*

Первый уровень обеспечивает защиту от угроз, исходящих от внешнего нарушителя. Внешний нарушитель не имеет доступа в здание, следовательно, и к основным носителям информации *(за исключением линий связи)*. Такой нарушитель имеет возможность, находясь за пределами контролируемой зоны, извлекать интересующие его сведения из информативных физических полей *(электромагнитных, акустических, виброакустических и т.д.)* или наводок на проводники, возникающих в результате работы технических средств. При этом используются специальные устройства съёма информации или устройства-закладки, обеспечивающие её трансляцию за пределы контролируемой зоны. В ряде случаев причиной утечки информации могут стать выброшенные расходные материалы *(копирок, красящих лент принтеров, списанных магнитных носителей и т.д.)*. Обеспечение защиты на первом уровне достигается реализацией комплекса организационных и инженерно-технических мероприятий.

Второй уровень обеспечивает ограничение доступа к носителям защищаемой информации внутри здания. В этом случае предполагается, что нарушитель имеет возможность пребывания в здании, но не имеет доступа в защищаемое помещение. Такими нарушителями могут быть посетители, сотрудники сторонних организаций, находящихся в одном здании [11].

Возможность внедрения нарушителя в информационную среду в этом случае увеличивается вследствие расширения спектра доступных носителей информации. Доступ к информации может быть реализован в результате подключения к внутренним линиям связи, установки специальных закладных устройств, путем хищения материальных носителей информации, прослушивания помещений с недостаточной звукоизоляцией, просмотра оставленных без присмотра документов, бесконтрольного проведения ремонтно-профилактических работ на объекте, халатного обращения сотрудников с физическими носителями информации, неконтролируемого доступа в выделенные помещения и т.д.

Защита в этом случае реализуется, как и на первом уровне, проведением организационных и организационно-технических мероприятий, но в качестве охраняемого объекта рассматривается уже не здание, а помещения, обычно называемые «выделенные помещения» для работы с защищаемыми сведениями, и внутренние коммуникации.

Третий уровень обеспечивает защиту от угроз, исходящих от внутреннего нарушителя, имеющего возможность работы со средствами обработки или хранения информации, но не имеющего прав доступа к защищаемым сведениям.

Задача предупреждения и нейтрализации злоумышленных действий такого нарушителя является наиболее сложной и приобретает особую актуальность при работе со средствами вычислительной техники *(при «бумажной технологии» защита осуществляется путем принятия организационно-режимных мер)*.

При работе со средствами вычислительной техники защита реализуется внедрением комплекса программных и программно-аппаратных средств, не позволяющих нарушителю считывать, модифицировать или удалять информацию, к которой он не допущен. Обеспечивается путем применения средств криптозащиты и разграничения доступа к информации, средств регистрации действий операторов технических средств, в том числе пользователей ПК [11].

Четвертый уровень. Для случаев, когда в качестве злоумышленника рассматривается сотрудник, имеющий доступ к работе с защищаемыми сведениями, основной задачей системы защиты информации, как организационно-технического комплекса, является создание условий для его быстрой идентификации и нейтрализации. Эту задачу возможно решить исключительно методами оперативно-розыскной деятельности. Другие методы и средства в этом случае играют вспомогательную роль.

Рассмотренный подход к построению схемы защиты информации позволяет систематизировать проведение мероприятий по защите

информации и объединить их в единый комплекс, учитывающий все основные направления угроз безопасности информации. При этом на каждом уровне защита реализуется путем комплексного внедрения определенных методов и технических средств.

В целом создание системы защиты информации необходимо начинать с построения системы её управления - решения организационных и нормативно-правовых вопросов, определяющих политику информационной безопасности и создающих основу для выбора и развертывания средств защиты и объединения их в единый комплекс[6].

При разработке политики безопасности и её практической реализации важно читывать, что система безопасности должна удовлетворять принципу достаточности, обеспечивающему рациональное использование финансовых и материальных средств, затрачиваемых на защиту информации. Практический опыт показывает, что необоснованное завышение требований к принятию защитных мер приводит не только к избыточным материальным затратам, но и к дискредитации этих мер там, где они действительно необходимы. Такая дискредитация, вероятно, связана с тем, что сотрудники, сознавая необоснованность принимаемых мер, зачастую нарушают устанавливаемые ограничения работы с открытой информацией, вырабатываемая при этом привычка нарушения требований нормативных документов переносится впоследствии и на режимные объекты.

Как показывает практика, значительного ограничения утечки информации из организации можно добиться путем применения шести основных правил.

Основная задача состоит в том, чтобы добиться обязательного соблюдения этих правил всеми сотрудниками организации [11].

---

[6] *John R. Vacca. Computer and Information Security Handbook, Third Edition 3rd Edition. Morgan Kaufmann Pub; 3 edition (June 15, 2017). 1280 pages*

1. *Маркирование документов*. Документы *(бумажные и электронные)*, содержащие конфиденциальную информацию, подлежат обязательному маркированию путем проставления грифа конфиденциальности в правом верхнем углу титульного листа. Маркирование конфиденциальных документов осуществляется ответственным за их подготовку или ответственным за работу с данными документами. Маркирование сообщений электронной почты осуществляется пользователем, выполняющим отправку *(распространение)* данных сообщений[7].

В документах, содержащих конфиденциальную информацию и передаваемых третьей стороне, на обороте титульного листа в обязательном порядке должно быть «заявление о конфиденциальности».

2. *Закрытое обсуждение*. Не следует обсуждать конфиденциальную информацию с посторонними лицами *(или в их присутствии)*, с друзьями, родственниками, сотрудниками организации, не допущенными к работе с данной информацией, и т.п. Не следует обсуждать конфиденциальную информацию в общественных местах в присутствии посторонних *(не допущенных к данной информации)* лиц, включая столовую и места для курения, расположенные на территории структуры.

3. *Шифрование информации при хранении и передаче*. Для обеспечения надлежащего уровня защиты шифрование должно применяться как при хранении, так и при передаче конфиденциальной информации. Электронный обмен конфиденциальной информацией с внешними респондентами должен вестись в зашифрованном виде, при наличии соответствующих технических возможностей.

4. *Использование соглашения о конфиденциальности*. Передача сведений, содержащих конфиденциальную информацию, третьей стороне

---

[7] *Darren Death. The Information Security Handbook. Packt Publishing - ebooks Account (December 8, 2017). Paperback 330 pages, eBook PDF*

должна осуществляться только после заключения с этой стороной «Соглашения о конфиденциальности».

5. *Ограничение доступа к информации*. Не следует хранить электронные документы, содержащие конфиденциальную информацию, в общедоступных местах, включая общие папки файловых серверов, Web, почтовые папки и т.п. Информирование. Необходимо всему персоналу овладеть методами защиты информации, следить за их выполнением каждым сотрудником, вести разъяснительную работу. Обо всех фактах утечки информации следует незамедлительно сообщать своему непосредственному руководителю.

Вопросы для самоконтроля

1. Дайте характеристику основных понятий теории защиты информации.
2. Что является объектами защиты?
3. Каковы цели и задачи системы безопасности?
4. Назовите основные принципы организации и функционирования системы безопасности.
5. Этапы работ по обеспечению режима ИБ в организации.
6. Определение политики безопасности и границ системы ИБ.
7. Методика оценки ситуации по защите информации.

3-§. Обеспечение защиты информации

Ключевые слова: *обеспечение защиты информации, правовая защита информации, административная защита информации, программная защита информации, физико-техническая защита информации, антивирусная профилактика*

В современном обществе в связи с бурной информатизацией всё более актуальной становится проблема защиты информации. Основой для

раскрытия сущности и определения понятия защиты информации должно быть определение понятия защиты в целом, безотносительно к предмету защиты. В толковых словарях термин «защита», интерпретируется: как процесс охраны, сбережения, спасения от враждебного, опасного и как совокупность методов, средств и мер, принимаемых для предотвращения, предупреждения чего-либо.

Обеспечение защиты информации представляет собой принятие правовых, организационных и технических мер, направленных на [11]:

1. *обеспечение защиты информации* от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. *соблюдение конфиденциальности* информации ограниченного доступа;
3. *реализацию* права на доступ к информации

Правовая защита информации

Правовая защита информации предполагает наличие регламентации прав на информацию, контроль за процедурами реализации прав[8].

[8] *Darren Death. The Information Security Handbook. Packt Publishing - ebooks Account (December 8, 2017). Paperback 330 pages, eBook PDF*

(рис.1.3.1.). Типы информации

Административная защита информации

Административная защита информации - это комплекс мер, направленных на создание системы защиты, организацию всех ее остальных форм, повышение их надежности. Меры административной защиты могут приниматься на различных уровнях, имеющих определенную степень иерархии: страны, республики, региона, отрасли и т.д. Административная защита информации предусматривает:

1. Определение стратегии, планирование, координацию и руководство процессами представления информации, обработки, хранений и коммуникации данных;

2. Планирование и организацию системы мероприятий по предотвращению несанкционированного доступа к информации;

3. Планирование аварийных работ по спасению информации в нештатных ситуациях;

4. Организацию защиты авторских и имущественных прав на информацию.

Программная защита данных

Программная защита данных - это комплекс мероприятий по разработке, внедрению и организации функционирования специализированного программно-информационного обеспечения, предназначенного для защиты данных[9].

1. Защита операционной системы:
   1.1. Ограничение доступа к компьютеру и операционной системе,
   1.2. Программная организация доступа.
2. Защита информационных систем:
   2.1. Защита ее содержания и целостности,
   2.2. Защита от несанкционированного доступа и копирования.
3. Система криптографии данных.
4. Защита программ от несанкционированного использования:
   4.1. Жесткая защита информации,
   4.2. Защита дискет от копирования,
   4.3. Программная защита данных при передаче данных.
5. Программная защита интеллектуальной собственности.
6. Защита целостности и точности данных.
7. Создание распределенной дисковой системы.
8. Программное восстановление данных.

[9] *Гафнер. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2017. - 324 с.*

Физико-техническая защита данных

Физико-техническая (физическая) защита данных - это комплекс таких производственных профилактических мероприятий по сохранению информации и средств, предназначенных для хранения и передачи данных. Эти мероприятия не связаны непосредственно с процессами программирования, компьютерной обработки и коммуникации, относятся, в основном, к функциям технико-операторского обслуживания и профилактики, осуществляемый на уровне пользователей и специальных групп людей.

Методы физико-технической защиты информации:

Защита машинных носителей данных (винчестеров, дискет, бумаг и пр.). Защита технического обеспечения компьютерных систем *(процессора, оргтехники)*. Работа на аппаратуре, не удовлетворяющей необходимым требованиям безопасности и качества, может привести к аварийной ситуации, непредсказуемым последствиям, искажению или потере информации.

- ✓ Выбор и защита средств коммуникации.
- ✓ Дополнительные технические средства защиты данных.
- ✓ Профилактические работы по защите данных.
- ✓ Архивация данных.

Антивирусология. Для борьбы с вирусами применяются следующие средства и меры: аппаратные *(специальные платы в процессоре)*, программные *(полифаги, ревизоры, вакцины, сторожа)*. Более подробную информацию о вирусах, их природе и классификации, методах и средствах борьбы с ними можно получить в сети Интернет *(сайты AVP Касперского, Доктор Веб и др.)*.

Антивирусная профилактика. Соблюдение правил, которым желательно следовать в целях защиты от вирусов и программ-вандалов [28].

1. Нельзя загружать в ОП программу, не зная всех последствий ее работы. Опасно приобретать программы контрабандным путем.
2. Убедитесь в чистоте программы от вирусов.

3. Имейте аварийную базу данных.
4. Обновляйте антивирусную систему.

Таким образом, принцип современной защиты информации - это поиск оптимального соотношения между доступностью и безопасностью. К сожалению, абсолютной защиты быть не может, но все же мы можем обеспечить ее.

Перечисленные выше способы и методы для обеспечения защиты информации, профилактические мероприятия позволяют надеяться на относительную защищенность данных в персональном компьютере. Необходимо следовать тем правилам, нормативным актам, использовать необходимые средства защиты, чтобы оградить себя от потери, кражи или изменения необходимой информации. Таким средствами могут быть антивирусы, резервное копирование, шифрование компьютерных данных.

В настоящее время применяемые на практике подходы и средства нередко страдают существенными недостатками и не обладают объявленной надежностью. Поэтому необходимо ориентироваться во всем спектре вопросов обеспечения информационной безопасности, понимая их комплексный и взаимообусловленный характер[10].

Вопросы для самоконтроля

1. Какие меры обеспечения защиты информации Вы знаете?
2. Что включает в себя правовая защита информации?
3. Что такое административная защита информации?
4. Какой комплекс мер включает в себя программная защита информации?
5. Какие средства и меры применяются для борьбы с компьютерными вирусами?

[10] *Гафнер. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2017. - 324 с.*

4-§. Защита информации

Ключевые слова: *информация, принципы защиты информации, конфиденциальность, целостность, достоверность, требования к защите информации, уровни защиты информации, законы о защите информации, защита информации в интернете, защита персональной информации, защита носителей информации, развитие защиты информации*

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информация сегодня стоит дорого и её необходимо охранять.

В последнее время особенно актуальной стала защита информации, под которой подразумевается комплекс мероприятий, направленных на исключение похищения важных данных. Задача заключается в поддержании целостности, доступности и конфиденциальности информации. Существуют определенные принципы защиты и методики для реализации задуманного.

Защита - система мер по обеспечению безопасности с целью сохранения государственных и коммерческих секретов. *Защита обеспечивается* соблюдением режима секретности, применением охранных систем сигнализации и наблюдения, использованием шифров и паролей.

Защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Принципы защиты информации

Для выполнения поставленной задачи нужна правовая, организационная и техническая база, благодаря чему можно исключить неправомерный доступ, соблюдение конфиденциальности и реализации права на разрешение. Организация защиты информации базируется на трех основных принципах, причем нарушение хотя бы одного из них свидетельствует об утечке или искажении [28].

1. *Конфиденциальность.* Лицо, располагающее конкретной информацией, не должно передать ее другим людям без согласия ее обладателя. При этом стоит заметить, что конфиденциальность не является свойством.

2. *Целостность.* Подразумевает исключение каких-либо несанкционированных изменений, причем, это касается как случайных, так и преднамеренных корректировок.

3. *Достоверность*. Эта некая гарантия, что информация была получена из достоверного или надежного источника.

Требования к защите информации

Чтобы реализовать представленные выше принципы, система должна отвечать ряду требований[11]:

1. *Централизованность.* Процесс управления всегда является централизованным, а система, используемая для его реализации, должна подходить под структуру объекта, который нужно оберегать.

2. *Плановость*. Система защиты информации должна базироваться на взаимодействии всех подразделений, направленных на реализацию принятой политики безопасности.

3. *Конкретика и целенаправленность*. Защищаться должны конкретные информационные ресурсы, которые могут быть интересны для конкурентов.

---

[11] *Гафнер. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2017. - 324 с.*

4. *Активность*. Защита информации должна организовываться с настойчивостью, поэтому важны средства прогнозирования, экспертных системы и других инструментов, направленных на реализацию принципа «обнаружить и устранить».

5. *Надежность и универсальность*. Система должна применять разные методы и средства для предотвращения утечки.

6. *Открытость*. В любое время должна быть возможность изменить или дополнить меры обеспечения безопасности.

7. *Экономический эффект*. Важно, чтобы затраты на защиту не были больше размера возможного ущерба.

Уровни защиты информации

Чтобы достичь хороших результатов, необходимо применять комплексный подход, так, рекомендуется сочетать меры законодательного, административного, процедурного и программно-технического характера. Организационные меры защиты информации на каком-либо предприятии можно разделить на три уровня, относящиеся к рабочему месту, подразделению и ко всему предприятию. На каждом этапе применяются более сложные механизмы [28].

Закон о защите информации

Существует специальный государственный закон, направленный на регулирование правовых отношений по защите данных, которые находятся в системе. При этом должны соблюдаться права собственности людей. Правовая защита информации на законодательном уровне имеет большое значение, так, применяются две группы[12]:

1. Способы, помогающие организовать и поддерживать в обществе негативную реакцию в сторону нарушителей закона.

---

[12] *Гафнер. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2017. - 324 с.*

2. Способы, помогающие направлять и координировать меры, направленные на увеличение образованности общества в области информационной безопасности

Защита информации в интернете

Объектами атак хакеров становятся не только госучреждения, банки и популярные сайты, поэтому важно защищать информацию, которая находится на любом компьютере. Существует несколько способов[13]:

1. *Надежные пароли*. Специалисты рекомендуют использовать комбинации из больших и маленьких латинских букв, цифр и символов. Они должны легко запоминаться, но не нести смысловой нагрузки.

2. *Шифрование данных*. В корпоративной и профессиональной версии Windows есть инструмент BitLocker. Этот механизм поможет зашифровать данные на одном или нескольких разделах жесткого диска. Для безопасности отдельных файлов можно использовать зашифрованные архивы.

3. *Антивирусные программы*. Взломщики для получения информации применяют вспомогательное программное обеспечение. Вирусы занимаются перехватом данных. В этом деле нужна для защиты информации антивирусная защита, причем должна быть актуальная версия.

4. *Установка пароля на BIOS*. При помощи этой защиты делается невозможной загрузка ПК с встроенного и внешнего носителя. Полезно будет установить пароль на жесткий диск, который становится бесполезным в руках злоумышленника [57].

[13] *В.Ф. Шаньгин. Информационная безопасность компьютерных систем и сетей. Москва ИД «ФОРУМ» - ИНФРА-М 2011.*

Защита информации на предприятии

Чтобы получить защиту, необходимо пройти несколько этапов: проанализировать и выбрать политику безопасности, внедрить подходящие средства, разработать и применить организационные меры.

1. На предприятии важна не только техническая защита информации, но и нормативно-правовые документы.
2. После следует определить потенциальные угрозы и оценить ущерб по отношению к каждому из них.
3. Когда вся необходимая информация будет собрана, то создается специальное подразделение по безопасности. Оно действует в нескольких направлениях: защищает данные, предотвращает несанкционированное проникновение, обеспечивает целостность информации и так далее.
4. Защита информации предполагает применение таких методов: электронная подпись, криптографический способ шифрования, пароли, система аудита и протоколирования, электронные ключи и так далее.

Защита персональной информации

К личной информации относят паспортные данные, пароли доступа к разным сервисам и электронным кошелькам, номер телефона и другие данные, при помощи которых можно добыть какую-то важную информацию. В интернете человек должен сам решать предоставлять ли свои данные или нет. Защита конфиденциальной информации проводится с учетом таких советов:

1. Не скачивайте и не активируйте программы, которые являются сомнительными.
2. Не записывайте важную информацию в легкодоступных местах.
3. Не вписывайте пароли в необычные форма авторизации.
4. Не игнорируйте предупреждения в браузере о проблемах с сертификатами и регистрацией сайта.
5. Во время работы на чужих компьютерах не сохраняйте свои пароли и всегда выходите из сайтов.

6. Используйте антивирус и проверяйте все скачанные файлы.

Защита носителей информации

В этом случае используется несколько методик, которые можно разделить на три группы: программные, аппаратные и комбинированные. Важно понимать, что абсолютно надежной защиты не существует. К самым популярным способам относят[14]:

1. Для всех съемных носителей допустима физическая защита, например, закрытие в сейфе.

2. Подходящие средства защиты от утечки информации на носителях встроенных в ПК подразумевают воспрепятствование включению питания.

3. Программное закрытие доступа к определенному носители или полностью ко всему ПК. В пример можно привести пароль CMOS.

4. Может использоваться программно-аппаратный метод с применением электронных ключей, которые часто вставляются в COM-порт ПК. Если прибор не получает нужный ответ, то программа не будет запускаться [35].

Развитие защиты информации

Процесс развития способов защиты прошел три этапа и последний начался в 80-х и длится до сегодняшнего дня. Задача заключается в аналитико-синтетической обработке данных и формировании научно-методологического базиса защитной системы. Специалисты работают над тем, чтобы способы защиты информации имели строго научную основу. В настоящее время уже представлены теории, которыми активно пользуются по всему миру. Еще одна характерная особенность развития – более широкое представление проблемы информационной безопасности [57].

Методы обеспечения информационной безопасности

1. *Управление доступом*. Включает следующие функции защиты:

---

[14] *В.Ф. Шаньгин. Информационная безопасность компьютерных систем и сетей. Москва ИД «ФОРУМ» - ИНФРА-М 2011.*

- ✓ идентификация пользователей, персонала и ресурсов системы;
- ✓ аутентификация объектов и субъектов;
- ✓ проверка полномочий субъекта на соответствие регламенту безопасности;
- ✓ разрешение и создание условий работы в пределах регламента;
- ✓ регистрация обращений к защищаемым ресурсам;
- ✓ реагирование при попытках несанкционированных действий *(отказ в запросе, задержка работы, отключение, сигнализация).*

Пример: Управление доступом на секретный объект, включающее в себя процедуры и правила, которые должен выполнять персонал объекта, а также алгоритмы работы механизмов и устройств слежения, фиксации и ограничения доступа.

2. *Препятствие* - метод физического преграждения пути злоумышленнику к ресурсам ИС.

Пример: Блокировки, не позволяющие техническому устройству или программе выйти за опасные границы; создание физических препятствий на пути злоумышленников, экранирование помещений и технических средств и т. п.

3. *Маскировка* - включает в себя методы криптографической и стеганографической защиты.

Пример: Шифрование информации, дезинформация о месте нахождения конфиденциальной информации, создание легенд, намеренное внесение помех.

4. *Регламентация* – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

5. *Принуждение* - метод защиты, при использовании которого пользователи и персонал ИС вынуждены соблюдать правила обработки,

передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

6. *Побуждение* - такой метод защиты, который побуждает пользователей и персонал системы не нарушать сложившиеся моральные нормы.

7. *Нападение* - способ защиты, применяемый в активной фазе информационной угрозы. Цель - заставить противника сосредоточить усилия на защите, ослабив усилия на создание угроз [35].

Содержание способов обеспечения безопасности представлено на (рис.1.4.1).

(рис.1.4.1). Методы защиты информации

Перечисленные методы ИБ реализуются на практике применением различных средств защиты информации.

Вопросы для самоконтроля

1. Что такое информация?
2. Какую деятельность подразумевает под собой защита информации?
3. Перечислите основные принципы организации защиты информации.
4. Расскажите об уровнях защиты информации.
5. На какие две группы подразделяется правовая защита информации?
6. Какие существуют способы защиты информации в интернете?

5-§. Криптографическая защита информации

Ключевые слова: *криптография, шифрование, дешифрование, ключ шифрования, криптоаналитические атаки, криптографические средства, криптоанализ, криптостойкость*

Криптография представляет собой совокупность методов преобразования данных *(шифрования)*, направленных на то, чтобы сделать эти данные бесполезными для противника. Эти преобразования позволяют решить проблему обеспечения конфиденциальности данных. Для ознакомления с зашифрованной информацией применяется обратный процесс-*дешифрование* [10].

Для шифрования обычно используется некоторый алгоритм или устройство, реализующее заданный алгоритм, которые могут быть известны широкому кругу лиц. Управление процессом шифрования осуществляется с помощью периодически меняющегося *ключа шифрования*, обеспечивающего каждый раз оригинальное представление информации при использовании одного и того же алгоритма или устройства. Знание ключа дешифрования позволяет просто и надежно расшифровать текст. Однако, без знания этого ключа процедура дешифрования может быть практически невыполнима даже при известном алгоритме. *Ключ шифрования K* - конкретное состояние некоторого параметра *(параметров)*, обеспечивающее выбор одного преобразования из совокупности возможных для используемого метода шифрования[15].

Будем называть *открытым текстом M* исходное сообщение, которое шифруют для его сокрытия от посторонних лиц. Сообщение, формируемое в результате шифрования открытого текста, будем называть *закрытым текстом (шифротекстом) C*.

---

[15] *Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.*

Обратной стороной криптографии является *криптоанализ*, который пытается решить обратную задачу, характерную для злоумышленника - раскрыть шифр, получив открытый текст, не имея подлинного ключа шифрования.

Существуют несколько основных типов криптоаналитических атак. Реализация каждой из них предполагает, что злоумышленник знает применяемый алгоритм шифрования.

1. *Криптоаналитическая атака* при наличии только известного закрытого текста *C*.

2. *Криптоаналитическая атака* при наличии известного открытого текста *(атака по открытому тексту)*. В этом случае, криптоаналитику известен открытый текст *M* и соответствующий ему закрытый текст *C*. Задача криптоаналитика состоит в нахождении ключа шифрования *K* для возможности прямой расшифровки последующих шифротекстов. Более мощным вариантом данного метода криптоанализа является криптоаналитическая атака при возможности выбора криптоаналитиком открытого текста.

3. *Криптоаналитическая атака* методом полного перебора всех возможных ключей. Данная атака предполагает использование криптоаналитиком известного шифротекста и осуществляется посредством полного перебора всех возможных ключей с проверкой осмысленности получаемого открытого текста. Такой подход требует привлечения предельных вычислительных ресурсов и иногда называется силовой атакой, атакой *«в лоб»*, или brute-forcing.

4. *Криптоаналитическая атака* методом анализа частотности закрытого текста. Реализация данной атаки предполагает использование криптоаналитиком информации о частоте встречаемости символов в закрытом тексте с целью получения информации о символах открытого текста.

Основной характеристикой шифра является его *криптостойкость*, которая определяет его стойкость к раскрытию с помощью методов криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия шифра [10].

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований[16].

1. Зашифрованный текст должен поддаваться чтению только при наличии секретного ключа шифрования.

2. *Закон Керхоффа* – знание алгоритма шифрования не должно влиять на надежность защиты, стойкость шифра должна определяться только секретностью ключа. Иными словами, данное требование предполагает, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника.

3. Единственно возможный метод раскрытия шифротекста должен заключаться в дешифровании его на секретном ключе. Единственно возможный способ нахождения ключа дешифрования должен заключаться в полном их переборе.

4. При знании криптоаналитиком шифротекста *C* и соответствующего ему открытого текста *M*, для нахождения ключа шифрования необходим полный перебор ключей (невозможность криптоаналитической атаки по открытому тексту).

5. Незначительное изменение ключа шифрования или открытого текста должно приводить к существенному изменению вида шифротекста.

6. Избыточность информации, вносимая в шифротекст за счет шифрования, должна быть незначительной.

7. Алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

---

[16] *Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.*

Криптографические средства - это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Техническая защита информации путем ее преобразования, исключающего ее прочтение посторонними лицами, волновала человека с давних времен. Криптография должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями - такими, как транснациональные корпорации и крупные государства. Криптография в прошлом использовалась лишь в военных целях. Однако сейчас, со становлением информационного общества, она становится инструментом для обеспечения конфиденциальности, доверия, авторизации, электронных платежей, корпоративной безопасности и бесчисленного множества других важных вещей. Почему проблема использования криптографических методов стала в настоящий момент особо актуальна? С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц [10].

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем, еще недавно считавшихся практически не раскрываемыми[17].

Проблемой защиты информации путем ее преобразования занимается криптология *(kryptos-тайный, logos-наука)*. Криптология разделяется на два направления - криптографию и криптоанализ. Цели этих направлений прямо

---

[17] *Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.*

противоположны. Криптография занимается поиском и исследованием математических методов преобразования информации].

Сфера интересов криптоанализа - исследование возможности расшифровывания информации без знания ключей.

Современная криптография включает в себя 4 крупных раздела:

- ✓ Симметричные криптосистемы
- ✓ Криптосистемы с открытым ключом
- ✓ Системы электронной подписи
- ✓ Управление ключами

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи *(например, электронная почта)*, установление подлинности передаваемых сообщений, хранение информации *(документов, баз данных)* на носителях в зашифрованном виде [10].

Криптография дает возможность преобразовать информацию таким образом, что ее прочтение *(восстановление*) возможно только при знании ключа. В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите. Под этими терминами понимается следующее.

- *Алфавит* - конечное множество используемых для кодирования информации знаков.
- *Текст* - упорядоченный набор из элементов алфавита.

Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом. Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

- *Ключ* - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство $M\ [M_1, M_2, ..., M_k]$ преобразований открытого текста. Члены этого семейства

индексируются, или обозначаются символом *«k»*; параметр *k* является ключом. Пространство ключей *K* - это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на симметричные и с открытым ключом. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения[18].

Термины распределение ключей и управление ключами относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями [36].

Электронной *(цифровой)* подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения[19].

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа *(т.е. криптоанализу)*.

Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра. Наиболее простой критерий такой эффективности - вероятность раскрытия ключа или мощность множества ключей *(M)*. По сути, это то же самое, что и криптостойкость. Для

---

[18] *Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.*

[19] *М.А. Иванов. Криптографические методы защиты информации в компьютерных системах и сетях. "КУДИЦ-ОБРАЗ" Москва 2001*

ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех ключей[20].

Однако этот критерий не учитывает других важных требований к криптосистемам:

- невозможность раскрытия или осмысленной модификации информации на основе анализа ее структуры;
- совершенство используемых протоколов защиты;
- минимальный объем применяемой ключевой информации;
- минимальная сложность реализации *(в количестве машинных операций)*, ее стоимость;
- высокая оперативность.

Часто более эффективным при выборе и оценке криптографической системы является применение экспертных оценок и имитационное моделирование. В любом случае выбранный комплекс криптографических методов должен сочетать как удобство, гибкость и оперативность использования, так и надежную защиту от злоумышленников циркулирующей в ИС информации [10].

Такое деление средств защиты информации *(техническая защита информации)*, достаточно условно, так как на практике очень часто они взаимодействуют и реализуются в комплексе в виде программно - аппаратных модулей с широким использованием алгоритмов закрытия информации.

Принципы криптографической защиты информации

Проблемы конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, показана на *рис.1.5.1*. Отправитель

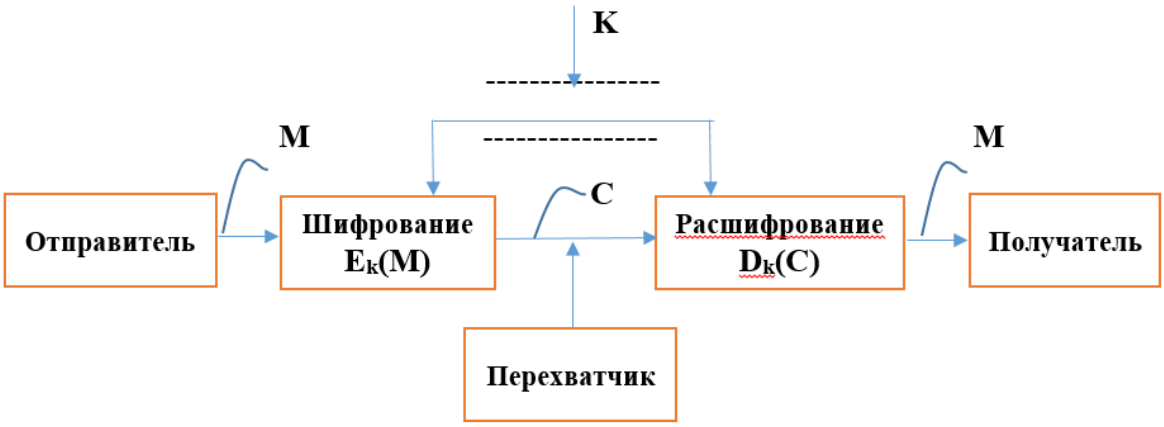
---

[20] Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.

генерирует открытый текст исходного сообщения *M*, которое должно быть передано законному получателю по незащищенному каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы перехватчик не смог узнать содержание сообщения *M*, отправитель шифрует его с помощью обратимого преобразования E_k и получает шифр текст *(или криптограмму)* $C=E_k(M)$, который отправляет получателю [36].

Законный получатель, приняв шифр текст *C*, расшифровывает его с помощью обратного преобра*зования* $D = E_k^{-1}$ и получает исходное сообщение в виде открытого текста *M*:

$$D_k(C)=E_k^{-1}\big(E_k(M)\big) = M$$



(рис.1.5.1) . Обобщенная схема криптосистемы

Преобразование E_k выбирается из семейства криптографических преобразований, называемых криптоалгоритмами. Параметр, с помощью которого выбирается отдельное используемое преобразование, называется криптографическим ключом *K*. Криптосистема имеет разные варианты реализации: набор инструкций, аппаратные средства, комплекс программ компьютера, которые позволяют зашифровать открытый текст и расшифровать шифртекст различными способами, один из которых выбирается с помощью конкретного ключа *K*.

Криптографическая система – это однопараметрическое семейство $(E_k)k\in \bar{k}$ обратимых преобразований

$$E_k:\bar{M}\ \ \bar{C}$$

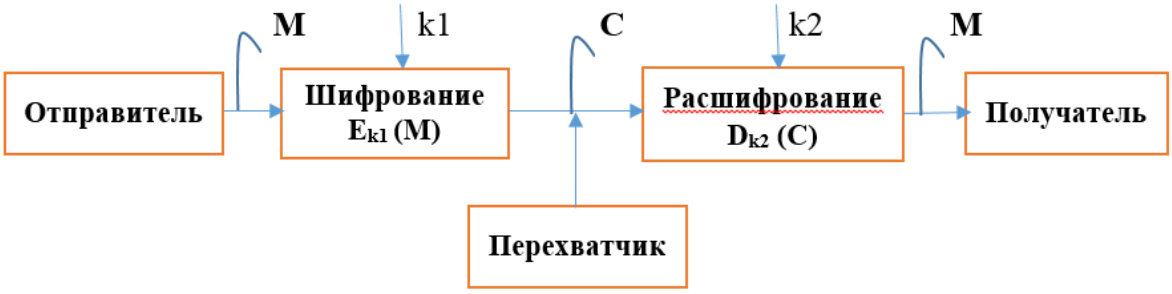
из пространства $\bar{M}$ сообщений открытого текста в пространство $\bar{C}$ шифрованных текстов. Параметр K *(ключ)* выбирается из конечного множества $\bar{K}$, называемого пространством ключей.

Вообще говоря, преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования. Это важное свойство функции преобразования определяет два класса криптосистем:

- симметричные *(одноключевые)* криптосистемы;
- асимметричные *(двухключевые)* криптосистемы *(с открытым ключом)*.

Схема симметричной криптосистемы с одним секретным ключом была показана на рис.3. В ней используются одинаковые секретные ключи в блоке шифрования и блоке расшифрования[21].

Обобщенная схема асимметричной криптосистемы с двумя разными ключами K_1 и K_2 показана на *рис.1.5.2*. В этой криптосистеме один из ключей является открытым, другой-секретным.



(рис.1.5.2). Обобщенная схема асимметричной криптосистемы с открытым ключом

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например такому, как курьерская служба. На рисунке этот канал показан "*экранированной*" линией. В асимметричной криптосистеме

[21] *Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.*

передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют на месте его генерации[10].

На *рис.1.5.3.* показан поток информации в криптосистеме в случае активных действий перехватчика. Активный перехватчик не только считывает все шифртексты, передаваемые по каналу, но может также пытаться изменять их по своему усмотрению.

Любая попытка со стороны перехватчика расшифровать шифртекст *C* для получения открытого текста *M* или зашифровать свой собственный текст *M'* для получения правдоподобного шифртекста *C'*, не имея подлинного ключа, называется криптоаналитической атакой.

Если предпринятые криптоаналитические атаки не достигают поставленной цели и криптоаналитик не может, не имея подлинного ключа, вывести *M* из *C* или *C'* из *M'*, то полагают, что такая криптосистема является криптостойкой.

(рис.1.5.3). Поток информации в криптосистеме при активном перехвате сообщений

Криптоанализ - это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу. Успешный анализ может раскрыть исходный текст или ключ. Он позволяет также обнаружить слабые места в криптосистеме, что, в конечном счете, ведет к тем же результатам[22].

[22] *Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.*

Фундаментальное правило криптоанализа, впервые сформулированное голландцем А. Керкхоффом еще в XIX веке заключается в том, что стойкость шифра *(криптосистемы)* должна определяться только секретностью ключа. Иными словами, правило Керкхоффа состоит в том, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника. Это обусловлено тем, что криптосистема, реализующая семейство криптографических преобразований, обычно рассматривается как открытая система. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации. Обычно криптосистема представляет собой совокупность аппаратных и программных средств, которую можно изменить только при значительных затратах времени и средств, тогда как ключ является легко изменяемым объектом. Именно поэтому стойкость криптосистемы определяется только секретностью ключа.

Другое почти общепринятое допущение в криптоанализе состоит в том, что криптоаналитик имеет в своем распоряжении шифртексты сообщений.

Существует четыре основных типа криптоаналитических атак. Конечно, все они формулируются в предположении, что криптоаналитику известны применяемый алгоритм шифрования и шифртексты сообщений. Перечислим эти криптоаналитические атаки[10].

1. **Криптоаналитическая атака при наличии только известного шифртекста.** Криптоаналитик имеет только шифртексты $C_1, C_2, \ldots, C_i$ нескольких сообщений, причем все они зашифрованы с использованием одного и того же алгоритма шифрования E_k. Работа криптоаналитика заключается в том, чтобы раскрыть исходные тексты $M_1, M_2, \ldots. M_i$ по возможности большинства сообщений или, еще лучше, вычислить ключ K, использованный для шифрования этих сообщений, с тем, чтобы расшифровать и другие сообщения, зашифрованные этим ключом.

2. **Криптоаналитическая атака при наличии известного открытого текста.** Криптоаналитик имеет доступ не только к шифртекстам $C_1, C_2, \ldots, C_i$ нескольких сообщений, но также к открытым текстам $M_1, M_2, \ldots, M_i$, этих сообщений. Его работа заключается в нахождении ключа К, используемого при шифровании этих сообщений, или алгоритма расшифрования D_k любых новых сообщений, зашифрованных тем же самым ключом.

3. **Криптоаналитическая атака при возможности выбора открытого текста.** Криптоаналитик не только имеет доступ к шифртекстам $C_1, C_2, \ldots, C_i$ и связанным с ними открытым текстам $M_1, M_2, \ldots, M_i$ нескольких сообщений, но и может по желанию выбирать открытые тексты, которые затем получает в зашифрованном виде. Такой криптоанализ получается более мощным по сравнению с криптоанализом с известным открытым текстом, потому что криптоаналитик может выбрать для шифрования такие блоки открытого текста, которые дадут больше информации о ключе. Работа криптоаналитика состоит в поиске ключа K, использованного для шифрования сообщений, или алгоритма расшифрования D_k новых сообщений, зашифрованных тем же ключом[23].

4. **Криптоаналитическая атака с адаптивным выбором открытого текста.** Это-особый вариант атаки с выбором открытого текста. Криптоаналитик может не только выбирать открытый текст, который затем шифруется, но и изменять свой выбор в зависимости от результатов предыдущего шифрования. При криптоанализе с простым выбором открытого текста криптоаналитик обычно может выбирать несколько крупных блоков открытого текста для их шифрования; при криптоанализе с адаптивным выбором открытого текста он имеет возможность выбрать сначала более мелкий пробный блок открытого текста, затем выбрать следующий блок в

[23] *Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.*

зависимости от результатов первого выбора, и т.д. Эта атака предоставляет криптоаналитику еще больше возможностей, чем предыдущие типы атак.

Кроме перечисленных основных типов криптоаналитических атак, можно отметить, по крайней мере, еще два типа [10].

5. **Криптоаналитическая атака с использованием выбранного шифртекста.** Криптоаналитик может выбирать для расшифрования различные шифртексты $C_1, C_2, \ldots, C_i$ и имеет доступ к расшифрованным открытым текстам $M_1, M_2, \ldots, M_i$. Например, криптоаналитик получил доступ к защищенному от несанкционированного вскрытия блоку, который выполняет автоматическое расшифрование. Работа криптоаналитика заключается в нахождении ключа. Этот тип криптоанализа представляет особый интерес для раскрытия алгоритмов с открытым ключом[24].

6. **Криптоаналитическая атака методом полного перебора всех возможных ключей.** Эта атака предполагает использование криптоаналитиком известного шифртекста и осуществляется посредством полного перебора всех возможных ключей с проверкой, является ли осмысленным получающийся открытый текст. Такой подход требует привлечения предельных вычислительных ресурсов и иногда называется силовой атакой[10].

Существуют и другие, менее распространенные, криптоаналитические атаки, некоторые из них будут описаны в соответствующих разделах книги.

Проблемы и перспективы развития криптографических методов защиты.

Криптосистема на основе эллиптических уравнений.

Эллиптическая кривая суть математический объект, который может быть определен над любым полем. В криптографии обычно используются

[24] *Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.*

конечные поля. Для точек на эллиптической кривой вводится операция сложения, которая играет ту же роль, что и операция умножения в криптосистемах RSA и эль-Гамаля.

Многочисленные исследования показали, что криптосистемы на основе эллиптических кривых превосходят другие системы с открытым ключом по двум важным параметрам: степени защищенности в расчете на каждый бит ключа и быстродействию при программной и аппаратной реализации[25].

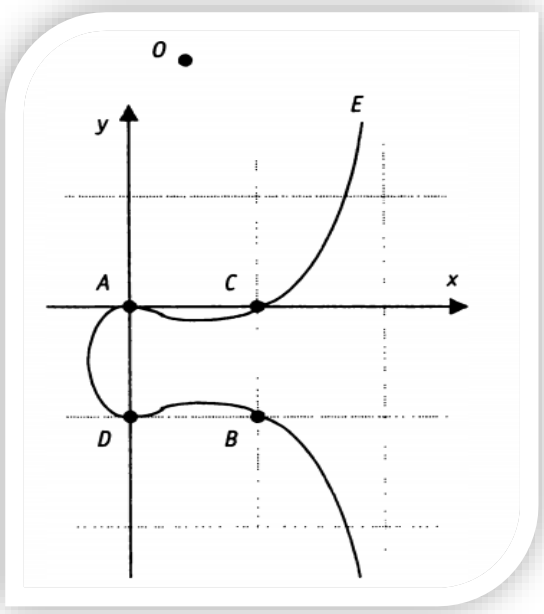
Группа точек эллиптической кривой

Рассмотрим эллиптическую кривую *E*, соответствующую уравнению

$$y^2+y = x^3-x^2 \text{ (рис.1.5.4.)}$$

На этой кривой лежат только четыре точки, координаты которых являются целыми числами. Это точки

A(0,0), B(1,-1), C(1,0) и *D(0,-1).*



(рис.1.5.4). Группа из пяти точек эллиптической кривой E, соответствующей уравнению $y^2+y = x^3-x^2$: 0 - бесконечно удаленная точка)

[25] *Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.*

Вопросы для самоконтроля

1. Что понимают под криптографией?
2. Дайте определение ключа шифрования.
3. Что понимают под криптоанализом?
4. Приведите примеры криптоаналитических атак. Кратко охарактеризуйте их.
5. Какие требования предъявляются к стойким шифрам, используемым для криптографической защиты информации?
6. Сформулируйте закон Керхоффа.
7. Охарактеризуйте подход к криптографической защите, используемый в симметричных криптосистемах.
8. Перечислите недостатки симметричных криптосистем.
9. Какие вы знаете угрозы информационным системам?
10. В чем заключается нарушение конфиденциальности? Приведите пример.
11. Что подразумевается под понятием криптография?
12. Перечислите криптоаналитические атаки и кратко расскажите о них.
13. Что включает в себя криптоаналитическая атака при наличии только известного шифртекста?
14. Что включает в себя криптоаналитическая атака методом полного перебора всех возможных ключей?

6-§. Средства защиты информации

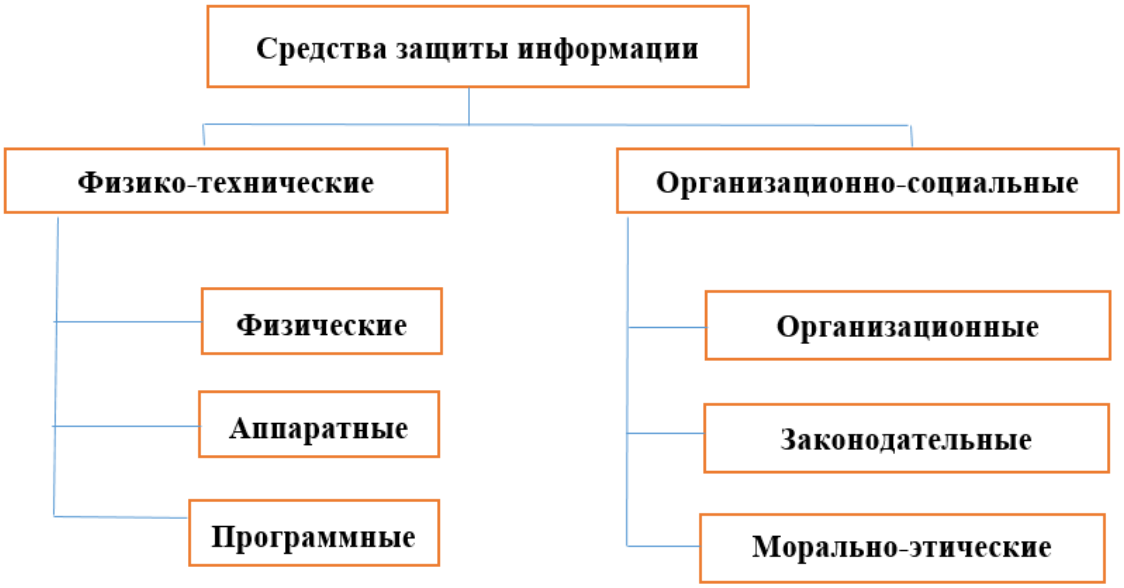
Ключевые слова: *управление доступом, средства защиты информации, технические средства, биометрические средства контроля и доступа, методы защиты от компьютерных вирусов, компьютерные вирусы*

Средства защиты информации - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и

приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации[26].

> *Под средством защиты информации понимается* - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на 6 групп рис.1.6.1.



(рис.1.6.1). Средства защиты информации

1. *Технические (аппаратные) средства*. Это различные по типу устройства *(механические, электромеханические, электронные и др.)*, которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная

[26] *Darren Death. The Information Security Handbook. Packt Publishing - ebooks Account (December 8, 2017). Paperback 330 pages, eBook PDF*

сигнализация и др. Вторую - генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны - недостаточная гибкость, относительно большие объем и масса, высокая стоимость [11].

2. *Программные средства* включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной *(рабочей)* информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств - универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров *(их аппаратных средств)*.

3. *Смешанные аппаратно-программные* средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

4. *Организационные средства* складываются из организационно-технических *(подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.)* и организационно-правовых *(законодательство в сфере ИБ и правила работы, устанавливаемые руководством конкретного предприятия)*. Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки – высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

5. *Законодательные средства* - нормативно-правовые акты, с помощью которых регламентируются права и обязанности всех лиц и подразделений, связанных с защитой информации, а также устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации.

6. *Морально-этические средства* защиты информации предполагают, прежде всего, воспитание сотрудника, допущенного к секретам, то есть проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений *(патриотизма, понимания важности и полезности защиты информации и для него лично)*, обучение сотрудника, осведомленного в сведениях, составляющих охраняемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Биометрические средства контроля и доступа.

Аутентификация по отпечаткам пальцев. В настоящее время существуют два возможных способа использования этого приема для аутентификации пользователя автоматизированной системы [33]:

- непосредственное сравнение изображений отпечатков пальцев, полученных с помощью оптических устройств, с отпечатками из архива;
- сравнение характерных деталей отпечатка в цифровом виде, которые получают в процессе сканирования изображений отпечатка.

При непосредственном сравнении изображений отпечатков устройство аутентификации определяет оптическое соотношение двух изображений и вырабатывает сигнал, определяющий степень совпадения отпечатков. Сравнение отпечатков обычно выполняется непосредственно на месте установки устройства. Передача изображений отпечатка по каналам связи не

применяется из-за ее сложности, высокой стоимости и необходимости дополнительной защиты этих каналов[27].

Большое распространение получил способ, построенный на сравнении деталей отпечатков *(метод соотнесения бороздок на отпечатках)*. При этом пользователь вводит с клавиатуры идентифицирующую информацию, по которой устройство аутентификации проводит поиск необходимого списка деталей отпечатка в архиве. После этого он помещает палец на оптическое окошко устройства, и начинается процесс сканирования, в результате которого вычисляются координаты 12 точек, определяющих относительное расположение бороздок отпечатка. Сравнение проводится в ЭВМ по специальным алгоритмам[28].

Аутентификация по форме кисти руки. Принцип действия таких устройств аутентификации основан на уникальности таких характеристик руки человека, как длина пальцев, закругленность их кончиков, прозрачность кожи и т.д. Информация об этих параметрах может получаться различными способами, например, при освещении руки, помещенной на панель из фоторезисторов, ярким светом. Преимуществом подобных систем является большое число анализируемых параметров, что уменьшает вероятность ошибки [11].

Аутентификация с помощью автоматического анализа подписи. Известно, что почерк каждого человека строго индивидуален, еще более индивидуальна его подпись. Она становится чрезвычайно стилизованной и со временем приобретает характер условного рефлекса. В настоящее время существуют два принципиально разных способа анализа подписи: визуальное сканирование и исследование динамических характеристик движения руки

---

[27] *Запечников. Информационная безопасность открытых систем. В 2-х т. Т.2 - Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ, 2018. - 558 с.*

[28] *Darren Death. The Information Security Handbook. Packt Publishing - ebooks Account (December 8, 2017). Paperback 330 pages, eBook PDF*

при выполнении подписи *(ускорения, скорости, давления, длительности пауз)*. Считается, что второй способ предпочтительнее, так как очевидно, что две подписи одного и того же человека не могут быть абсолютно идентичными. С другой стороны, обладая оригиналом подписи, можно научиться повторять ее практически точно.

При втором способе аутентификации предполагается применение специальных измерительных авторучек с датчиками, чувствительными к указанным выше динамическим характеристикам движения. Эти параметры уникальны для каждого человека, их невозможно подделать. Специалисты считают, что система установления подлинности подписи при меньшей стоимости и большей социальной приемлемости не уступает по надежности устройствам, сверяющим отпечатки пальцев.

Аутентификация по характеру голоса. По мнению ряда специалистов, данный метод является наиболее надежным средством аутентификации пользователей. Это направление очень перспективно потому, что для аутентификации могут быть использованы телефонные каналы связи, а алгоритм опознавания может быть реализован в центральной ЭВМ. Устройства аутентификации пользователей по их голосам анализируют спектры голосов, которые сугубо индивидуальны для каждого человека.

Основным выводом, следующим из опыта создания устройств аутентификации, является то, что получение высокой точности опознавания пользователя возможно только при сочетании различных методов. Необходимо отметить, что все рассмотренные методы аутентификации в случае не подтверждения подлинности должны осуществлять временную задержку перед обслуживанием следующего запроса. Это необходимо для снижения угрозы подбора идентифицирующих признаков в автоматическом режиме [11].

Защита информации от утечки за счет побочных электромагнитных излучений и наводок.

Для защиты информации от утечки за счет побочных электромагнитных излучений и наводок применяются пассивный, активный и комбинированный методы.

Пассивная защита заключается в снижении уровней излучения до величин, соизмеримых с естественными шумами, с помощью специальной элементной базы и конструктивной доработки техники, обрабатывающей конфиденциальную информацию. Существуют различные способы реализации этого метода. Одно из самых простых технических решений состоит в том, чтобы поместить все оборудование в безопасную и экранирующую радиоизлучения среду. Это применяется для малогабаритной аппаратуры, что позволяет сохранить ее стоимость на приемлемом уровне. Для больших систем экранирование целых залов и даже зданий может быть чрезвычайно дорогим, поэтому проблемы обеспечения электронной зашиты для них рассматриваются на стадии проектирования. Например, для систем связи определяются требования безопасности отдельных компонентов каждой секции всей системы. Разработчик может потребовать экранирования отдельных устройств системы при помощи металлического защитного покрытия или использовать стандартные экранированные корпуса для блоков аппаратуры. Там, где экранирование компонентов нецелесообразно, предусматривается достаточная изоляция линий данных и питания за счет различных сочетаний фильтров, устройств подавления сигнала. Должны также экранироваться кабели. При этом лучшим вариантом защиты линий связи является применение волоконно-оптической технологии. Надежное экранирование абонентской аппаратуры связи чрезвычайно усложняет задачу электронного подслушивания.

Активная защита предполагает сокрытие информационных сигналов за счет шумовой или заградительной помехи с помощью специальных генераторов шума. Активная радиотехническая маскировка заключается в формировании и излучении маскирующего сигнала в непосредственной близости от маскируемой системы. В данном случае различают

энергетический и неэнергетический методы активной радиотехнической маскировки.

При энергетической маскировке получается широкополосный шумовой сигнал с уровнем, существенно превышающим во всем частотном диапазоне уровень излучения системы. Энергетическая маскировка может быть реализована только в случае, если уровень излучений существенно меньше установленного существующими стандартами на электромагнитную совместимость и медицинскими требованиями.

Неэнергетический метод активной радиотехнической маскировки заключается в изменении вероятностной структуры сигнала, который может быть принят приемником злоумышленника.

Одним из видов угроз деятельности государственных и коммерческих предприятий, организаций, фирм является несанкционированный съем служебной, коммерческой и личной информации.

Основным направлением специальной защиты является поиск техники слухового контроля. Это направление является наиболее распространенным способом защиты. Поисковые работы могут проводиться как в отдельном помещении, так и во всем здании; быть одноразовым предприятием или повторяться с определенной периодичностью. Частота поиска зависит от режима использования помещения, обстановки вокруг объекта, степени важности обсуждаемых в этом помещении вопросов. Поиск техники подслушивания может продолжаться от нескольких часов до нескольких дней [11].

Специалисты по поиску техники подслушивания начинают свою работу, как правило, с опроса персонала фирмы и изучения режима использования и посещений проверяемого помещения. Техника подслушивания не может появиться сама по себе: ее должен кто-то принести в «интересный» кабинет и правильно там установить. На рабочем столе можно подменить какой-нибудь предмет на точно такой же, но с электронной начинкой, а затем вернуть все на свое место. «Жучки» могут быть спрятаны в

подарки или сувениры, которыми украшен кабинет или комната для переговоров. Особо привлекательным для установки разнообразной техники подслушивания является капитальный или косметический ремонт кабинета.

Понятие специального (выделенного) помещения. Существенной преградой на пути негласного съема информации является создание на объектах особых, защищенных от подслушивания помещений. Таким помещениям присваивается статус специальных: они оборудуются с учетом следующих требований[29]:

- здание, где размещаются такие особые помещения, должно иметь круглосуточную охрану и систему сигнализации;
- помещение располагается по возможности в центре здания, рядом с кабинетами руководства объекта;
- если в помещении должны быть окна, то желательно, чтобы они не имели балконов и не выходили на соседние с объектом здания, а смотрели бы на внутренний двор или закрывались бы глухими ставнями;
- внутри помещения должно быть минимальное количество мебели: конструкция мебели должна быть максимально приспособлена для работы специалиста по поиску техники подслушивания;
- в помещении не должно быть радиоэлектронных устройств, компьютеров, телевизоров, магнитофонов;
- если возможно, лучше отказаться от любых видов связи, вызывая, например, секретаря с помощью самой простой звонковой кнопки.

При выборе способа защиты помещений следует помнить о том, что эффективность ее будет высокой только при строгом соблюдении режима посещений и работы в таком специальном кабинете. Необходима и периодическая его проверка специалистом по поиску техники подслушивания. Практика показывает, что строгое соблюдение всего

[29] *Darren Death. The Information Security Handbook. Packt Publishing - ebooks Account (December 8, 2017). Paperback 330 pages, eBook PDF*

комплекса мер безопасности в сочетании с личной заинтересованностью сотрудников в процветании своей фирмы может создавать непреодолимый психологический барьер для конкурентов и злоумышленников.

Удаление носителей данных. Для удаления компьютерных носителей информации, которые больше не нужны, требуются надежные и проверенные процедуры. Конфиденциальная информация может просочиться за пределы организации и попасть в руки лиц, не имеющих соответствующих прав, вследствие небрежного удаления компьютерных носителей данных. Для сведения такого риска к минимуму следует определить четкие процедуры надежного удаления носителей информации [11].

Защита носителей информации во время транспортировки. Компьютерные носители данных могут быть уязвимы по отношению к несанкционированному доступу, использованию и повреждению во время транспортировки. Для защиты компьютерных носителей информации, транспортируемых из одной организации в другую, предлагаются следующие средства контроля:

- использование надежных курьеров и транспорт. Согласование списка курьеров, наделенных соответствующими полномочиями, с руководством и реализация процедуры идентификации курьеров;
- обеспечение надлежащей защиты содержимого упаковки от возможного физического повреждения во время транспортировки в соответствии с инструкциями производителей;
- принятие специальных мер *(по необходимости)* для защиты конфиденциальной информации от несанкционированного раскрытия или модификации: использование контейнеров закрытого типа; доставка посредством курьеров; упаковка, защищенная от постороннего вмешательства *(которая позволяет выявить попытки ее вскрытия)*; в исключительных случаях разделение груза на несколько частей и их посылка разными маршрутами.

Методы защиты от компьютерных вирусов.

Компьютерный вирус - это программа, обладающая двумя основными функциями: способностью к само репродукции и способностью осуществлять определенные манипуляции в вычислительной системе. Компьютерный вирус может существовать в следующих четырех фазах: «спячка», распространение в вычислительной системе или сети, запуск вируса, разрушение программ и данных или другие негативные эффекты [11].

Фаза «спячки» может использоваться автором вируса для создания у пользователя уверенности в правильной работе системы.

Фаза распространения обязательна для любой программы-вируса. В этой фазе в результате загрузки и выполнения программы, зараженной вирусом, происходит заражение других программ путем многократного самокопирования вируса в другие программы и системные области.

Запуск вируса осуществляется, как правило, после некоторого события, например, наступления определенной даты или заданного числа копирований.

В последней фазе происходит разрушение программ и данных или какие-либо другие негативные действия, предусмотренные автором вируса.

Многие вирусы не опасны и созданы не злонамеренно, а ради шутки или эксперимента с существующей техникой. Степень опасности вируса характеризует потенциально наносимый им вред. Можно предложить следующую шкалу степени опасности[30]:

- вирус имеет не деструктивную фазу проявления *(звуковые или визуальные эффекты*), все зараженные файлы могут быть корректно восстановлены;
- вирус имеет не деструктивную фазу проявления, из-за ошибок он может некорректно заразить и тем самым испортить некоторые программы;

[30] *Darren Death. The Information Security Handbook. Packt Publishing - ebooks Account (December 8, 2017). Paperback 330 pages, eBook PDF*

- фаза проявления вируса связана с воздействием на систему *(эффект замедления, блокировка клавиатуры)*, никакие файлы преднамеренно не портятся;
- фаза проявления *(помимо вышеназванных эффектов)* связана с преднамеренной порчей или стиранием программных, или других файлов, файловая система остается работоспособной;
- вирус частично портит некоторые важные части файловой системы на гибком или жестком диске, возможно их восстановление вручную;
- вирус полностью портит файловую систему на жестком диске, форматирует винчестер и т.п.;
- вирус физически портит аппаратуру *(прожигание экрана монитора, вывод из строя микросхем за счет нарушения теплового режима и т.п.)*.

Рассмотрим основные классы антивирусных программ.

Программы проверки целостности программного обеспечения. Такие программы не могут препятствовать заражению, однако дают пользователю ценную информацию о зараженных или измененных программах.

Программы контроля. Программы этого класса используют режим прерывания работы ЭВМ. Если, по мнению автора антивирусной программы, они замечают что-либо подозрительное; то прерывают работу ЭВМ и выдают оператору рекомендацию о дальнейших действиях.

Программы удаления вирусов. Такие программы проверяют наличие на магнитном диске только известных вирусов. Обнаружив вирус, они сообщают об этом оператору или удаляют вирус.

Копии. Копирование программ является методом защиты, однако оно не гарантирует отсутствия вирусов.

Анализ разработанных на сегодня теоретические основы борьбы с компьютерными вирусами позволяет заключить, что абсолютная защита может быть достигнута только абсолютной изоляцией компьютера от внешней среды, что, естественно, на практике является неприемлемым решением. Анализ показывает, что в настоящее время любая используемая

автоматизированная система общего назначения открыта, по крайней мере, для ограниченной вирусной атаки. В современных условиях как достаточно надежная предпосылка безопасности любой компьютерной системы должен рассматриваться контроль ее целостности.

Проблемы опознавания пользователя. Реализация конкретных схем защиты информации от несанкционированного доступа должна опираться на соответствующие административные *(процедурные)* мероприятия и технические средства, направленные в первую очередь на опознавание *(идентификацию и аутентификацию)* пользователей [11].

Идентификация пользователей заключается в установлении и закреплении за каждым из них уникального идентификатора в виде номера, шифра, кода и т.п. Для целей идентификации в различных автоматизированных системах широко применяется, например, так называемый персональный идентификационный номер *(PIN - Personal Identification Number)*, социальный безопасный номер *(SSN - Social Security Number)*, личный номер, код безопасности и т.д. Такие идентификаторы используются при построении различных систем разграничения доступа и защиты информации.

Аутентификация заключается в проверке подлинности пользователя по предъявленному им идентификатору, например, при входе в систему. Такая проверка должна исключать фальсификацию пользователей в системе и их компрометацию. Без проверки подлинности теряется смысл в самой идентификации пользователей и применении средств разграничения доступа, построенных на базе личных идентификаторов.

Вопросы для самоконтроля

1. Какие виды ущерба может нанести нарушение информационной безопасности?
2. Что подразумевается под средствами защиты информации?

3. Как обычно классифицируют средства обеспечения защиты информации?

4. Расскажите о биометрических средствах контроля и доступа?

5. Что Вы понимаете под компьютерным вирусом?

6. Расскажите о шкале степени опасности компьютерных вирусов.

7. Рассмотрите основные классы антивирусных программ. Какой из них наиболее эффективен?

ГЛАВА 2. СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ОРГАНИЗАЦИЯ ЗАЩИТЫ СЕТИ

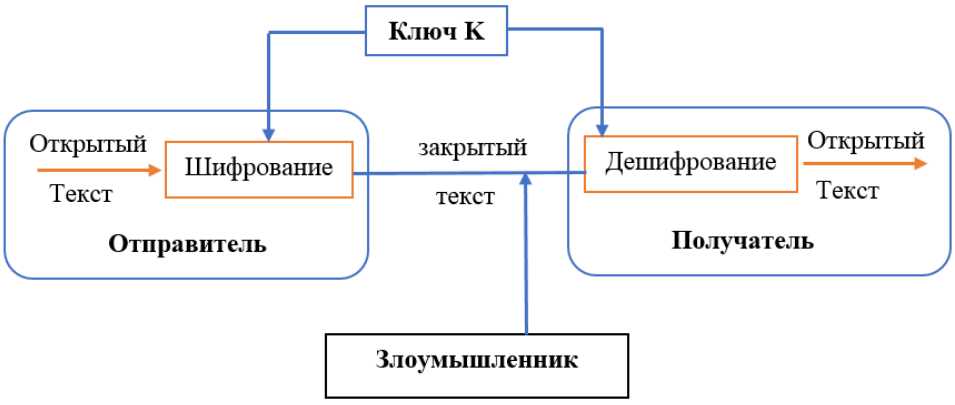
==========

7-§. Основы симметрической криптосистемы

Ключевые слова: *симметричные криптосистемы, шифрование методом замены, шифрование методом Цезаря, шифрование таблицы Трисемуса, шифр Гронсфельда, система шифрования Вижинера, шифрование методом Вернама, шифрование методом перестановки, шифрование методом гаммирования, линейный конгруэнтный метод*

В *симметричных криптосистемах* (*криптосистемах с секретным ключом*) *шифрование* и *дешифрование* информации осуществляется на одном ключе *K*, являющемся секретным. Рассекречивание ключа шифрования ведет к рассекречиванию всего защищенного обмена. Для того, чтобы подчеркнуть факт использования одного и того же ключа в шифраторе источника и дешифраторе получателя сообщений, криптосистемы с секретными ключами называют также *одноключевыми*[31].

Функциональная схема взаимодействия участников симметричного криптографического обмена приведена на рис.2.7.1.



(рис.2.7.1). Функциональная схема симметричной криптосистемы

[31] *В.Ф. Шаньгин. Защита информации и информационная безопасность. Часть I. Основы информационной безопасности. Симметричные криптосистемы: Учеб. пос. для вузов. М: МИЭТ -1999-140 с.*

В симметричной криптосистеме секретный ключ необходимо передать всем участникам криптографической сети по некоторому защищенному каналу. Традиционные симметричные криптосистемы можно разделить на следующие основные виды:

- шифры замены;
- шифры перестановки;
- шифры гаммирования.

Шифрование методом замены

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее оговоренной схемой замены. Данные шифры являются наиболее древними. Принято делить шифры замены на *моноалфавитные* и *многоалфавитные*.

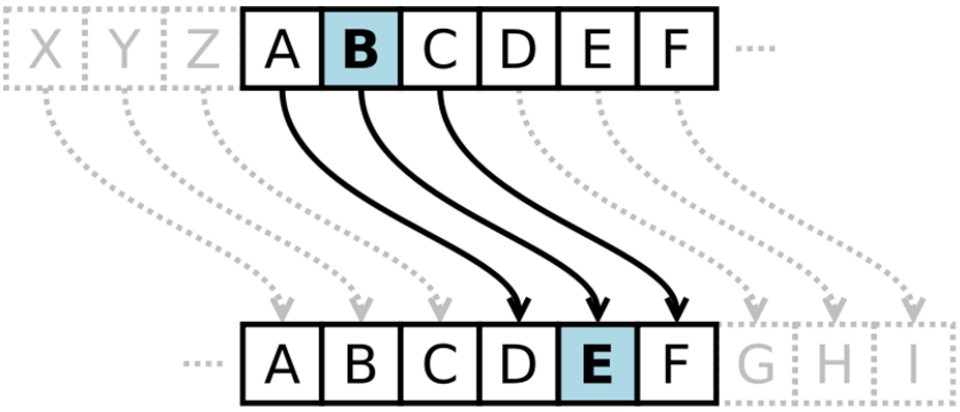
При моноалфавитной замене каждой букве алфавита открытого текста ставится в соответствие одна и та же буква шифротекста из этого же алфавита одинаково на всем протяжении текста [55].

Рассмотрим наиболее известные шифры моноалфавитной замены.

Шифрование методом Цезаря

Свое название данный шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном *(около 50 г. до н.э)*. При шифровании исходного текста по данному методу каждая буква заменяется на другую букву того же алфавита путем ее смещения в используемом алфавите на число позиций, равное K. При достижении конца алфавита выполняется циклический переход к его началу.

Шифр Цезаря – это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется буквой, находящейся на некоторое постоянное число позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 A была бы заменена на D, B станет E, и так далее. Рис.2.7.2.



(рис.2.7.2). Шифр Цезаря

Общая формула шифра Цезаря имеет следующий вид:

$$C=P+K \pmod M, \quad (1)$$

где P – номер символа открытого текста, C - соответствующий ему номер символа шифротекста, K – ключ шифрования (коэффициент сдвига), M – размер алфавита (для русского языка M=32)

Для данного шифра замены можно задать фиксированную таблицу подстановок, содержащую соответствующие пары букв открытого текста и шифротекста.

Пример 1.

Таблица подстановок для символов русского текста при ключе K=3 представлена в таблице 2.7.1. Данной таблице соответствует формула

$$C=P+3 \pmod{32}, \quad (2)$$

А	→	Г		Р	→	У
Б	→	Д		С	→	Ф
В	→	Е		Т	→	Х
Г	→	Ж		У	→	Ц
Д	→	З		Ф	→	Ч
Е	→	И		Х	→	Ш
Ж	→	Й		Ц	→	Щ
З	→	К		Ч	→	Ь
И	→	Л		Ш	→	Ы
Й	→	М		Щ	→	Ъ
К	→	Н		Ь	→	Э

Л	→	О		Ы	→	Ю
М	→	П		Ъ	→	Я
Н	→	Р		Э	→	А
О	→	С		Ю	→	Б
П	→	Т		Я	→	В

(табл.2.7.1). Таблица подстановок шифра Цезаря для ключа K=3

Согласно формуле *(2)* открытый текст «ТЕХНОЛОГИЯ» будет преобразован в шифротекст «ХИШРСОСЖЛВ».

Дешифрование закрытого текста, зашифрованного методом Цезаря согласно *(1)*, осуществляется по формуле

$$C=P-K \ (mod\ M),\ (3)$$

Простая моноалфавитная замена

Шифр простой моно алфавитной замены является обобщением шифра Цезаря и выполняет шифрование по следующей схеме:

$$C=a*P+K \ (mod\ M),\ (4)$$

где $0 \le a, K < M$ - ключ шифрования, *НОД(a, M=1).*

Преобразование согласно схеме *(4)* является взаимно однозначным отображением только в том случае, если *a* и *M* взаимно простые. В этом случае для дешифрования закрытого текста выполняют обратное преобразование по формуле[32] *(5)*

$$P=a^{-1}*(C-K) \ (mod\ M),\ (5)$$

Пример 2.

Пусть *M=26, a=3, K=6, НОД(3,26) = 1.* Тогда получаем следующую таблицу подстановок для шифра простой моноалфавитной замены *(в таблице 2.7.2 указаны коды букв)*.

A	B	C	D	E	F	G	H	I	G	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	0	3

[32] *В.Ф. Шаньгин. Защита информации и информационная безопасность. Часть I. Основы информационной безопасности. Симметричные криптосистемы: Учеб. пос. для вузов. М: МИЭТ -1999-140 с.*

(таб.2.7.2). Таблица подстановок

Тогда открытый текст «HOME» будет преобразован в шифротекст «BWQS».

Шифрующие таблицы Трисемуса.

Данный шифр был предложен в 1508 году аббатом из Германии Иоганом Трисемусом. Для получения данного шифра замены им было предложено использовать таблицу для записи букв алфавита и ключевого слова или фразы. В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. При шифровании в построенной таблице находят очередную букву открытого текста и записывают в шифротекст букву, расположенную ниже ее в том же столбце. Если буква открытого текста оказывается в нижней строке таблицы, тогда для шифротекста берут самую верхнюю букву из того же столбца.

Для русского алфавита шифрующая таблица может иметь размер 4x8.

Пример 3.

Выберем в качестве ключа слово «ПАМЯТНИК». Шифрующая таблица с данным ключом представлена в (таблице 2.7.3).

П	А	М	Я	Т	Н	И	К
Б	В	Г	Д	Е	Ж	З	Й
Л	О	Р	С	У	Ф	Х	Ц
Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю

(табл.2.7.3). Шифрующая таблица Трисемуса

Тогда открытый текст «НЕРУКОТВОРНЫЙ» будет преобразован в закрытый текст «ЖУЩЫЙШЕОШЩЖТЦ».

Достоинством методов моно алфавитной замены является простота шифрования и дешифрования.

Основным недостатком данных методов является то, что подстановки, выполняемые в соответствие с данными методами, не маскируют частоты

появления различных букв закрытого текста. Это позволяет легко атаковать данные методы шифрования путем анализа частотности символов закрытого текста. Особенности реализации данного метода крипто анализа будут рассмотрены далее.

При многоалфавитной замене каждой букве алфавита открытого текста в различных ситуациях ставятся в соответствие различные буквы шифротекста в зависимости от соответствующего ей элемента ключа. В данном случае для шифрования каждого символа открытого текста применяют свой шифр моно алфавитной замены, причем смена алфавитов осуществляется последовательно и циклически, т.е. первый символ заменяется соответствующим символом первого алфавита, второй - символом второго алфавита и т. д. до тех пор, пока не будут использованы все выбранные алфавиты. После этого использование алфавитов повторяется.

Многоалфавитные шифры замены предложил и ввел в практику криптографии Леон Батист Альберти. Рассмотрим ряд примеров шифров многоалфавитной замены.

Шифр Гронсфельда

Данный шифр представляет собой модификацию *шифра Цезаря* с числовым ключом. При реализации данного шифра под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Получение символа шифротекста осуществляют также, как это делается в шифре Цезаря, при этом смещение символа открытого текста производят на количество позиций, соответствующего цифре ключа, стоящей под ним[33].

Пример 4.

Пусть необходимо зашифровать исходное сообщение «НОЧЕВАЛА ТУЧКА ЗОЛОТАЯ», в качестве ключа возьмем *К*=193431.

---

[33] *М.А. Иванов. Криптографические методы защиты информации в компьютерных системах и сетях. "КУДИЦ-ОБРАЗ" Москва 2001*

Сообщение	Н	О	Ч	Е	В	А	Л	А	Т	У	Ч	К	А	З	О	Л	О	Т	А	Я
Ключ	1	9	3	4	3	1	1	9	3	4	3	1	1	9	3	4	3	1	1	9
Шифротекст	О	Ч	Ь	Й	Е	Б	М	Й	Х	Ч	Ь	Л	Б	Р	С	П	С	У	Б	И

(табл. 2.7.4). Ночевала тучка золотая

Для того, чтобы зашифровать первую букву сообщения Н, необходимо сдвинуть ее в алфавите русских букв на число позиций 1, в результате чего получим букву О.

Дешифрование шифротеста предполагает сдвиг его символов на необходимое число позиций в обратную сторону.

Система шифрования Вижинера

Отличие системы Вижинера от шифра Гронсфельда заключается в том, что элементами ключа в данном случае могут быть не только цифры от 0 до 9, но и произвольные символы некоторого алфавита [36].

При шифровании исходного сообщения его, как и в шифре Гронсфельда, выписывают в строку, а под ним записывают ключевое слово или фразу. Если ключ оказался короче сообщения, то его циклически повторяют. Все символы используемого алфавита пронумерованы от *0* до *M-1*, где *M* – размер алфавита. Преобразование символа открытого текста осуществляется по формуле

$$C_i=P_i+K_i \ (mod\ M),\ (6)$$

где P_i - номер символа открытого текста, K_i – номер расположенного под ним символа ключа, C_i – номер символа шифротекста.

Преобразование символа закрытого текста в символ открытого осуществляется по формуле[34]

$$P_i=C_i-K_i \ (mod\ M).$$

Пример 6.

[34] *М.А. Иванов. Криптографические методы защиты информации в компьютерных системах и сетях. "КУДИЦ-ОБРАЗ" Москва 2001*

Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ДНЕМ» по методу Вижинера с помощью ключевого слова СИСТЕМА

Сообщение	П	Р	И	Л	Е	Т	А	Ю		Д	Н	Е	М
Ключ	С	И	С	Т	Е	М	А	С		И	С	Т	Е
Шифротекст	А	Ш	В	Э	К	Ю	А	П		М	Ю	Ч	С

(табл. 2.7.5). Шифрования сообщения «ПРИЛЕТАЮ ДНЕМ»

В данном случае буквы русского алфавита пронумерованы от 0 до 31: А-0, Б-1, В-2, ..., Я-31.

Шифрование методом Вернама

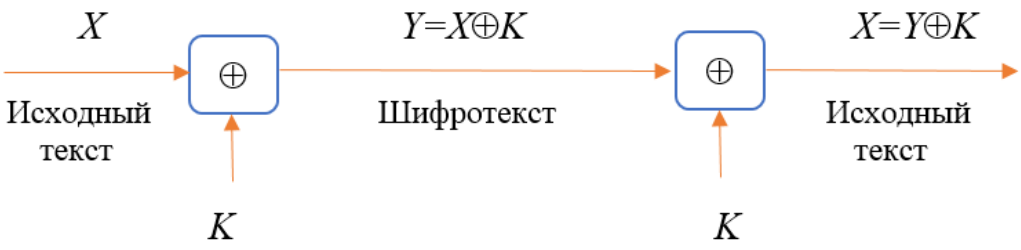
Система шифрования Вернама является частным случаем системы шифрования Вижинера при значении модуля M=2.

При шифровании открытого текста, каждый его символ представляется в двоичном виде. Ключ шифрования также представляется в двоичной форме. Шифрование исходного текста осуществляется путем сложения по модулю 2 двоичных символов открытого текста с двоичными символами ключа согласно *(7)*.

$$Y=P\oplus K, \ (7)$$

Дешифрование состоит в сложении по модулю 2 символов шифротекста с ключом.

Общая схема системы шифрования Вернама представлена на (рис. 2.7.3).



(рис.2.7.3). Схема системы шифрования Вернама

Модификация системы шифрования Вернама используется для криптографической защиты информации в архиваторе *ARJ*. Формула *(7)* в этом случае преобразуется в следующую:

$$Y=P\oplus(K+VALUE), (8)$$

где *VALUE* – фиксированное значение.

(рис.2.7.4). Схема системы шифрования Вернама

Пример 7.

Зашифруем с помощью системы Вернама открытый текст «БЛАНК» с помощью ключа «ОХ».

Преобразуем открытый текст «БЛАНК» в ASCII коды: Б=193, Л=203, А=192, Н=205, К=202. В двоичном виде последовательность 193, 203, 192, 205, 202 представится в виде 11000001 11001011 11000000 11001101 11001010.

Преобразуем ключ «ОХ» в ASCII коды: О=206, Х=213. В двоичном виде последовательность 206, 213 представится в виде 11001110 11010101.

Подпишем циклически ключ под открытым текстом и выполним сложение по модулю 2 соответствующих битов.

Открытый текст	1	1	0	0	0	0	0	1	1	1	0	0	1	0	1	1	1	1	0	0
Ключ	1	1	0	0	1	1	1	0	1	1	0	1	0	1	0	1	1	1	0	0
Закрытый текст	0	0	0	0	1	1	1	1	0	0	0	1	1	1	1	0	0	0	0	0

Открытый текст	0	0	0	0	1	1	0	0	1	1	0	1	1	1	0	0	1	0	1	0
Ключ	1	1	1	0	1	1	0	1	0	1	0	1	1	1	0	0	1	1	1	0

Закрытый текст	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0

(табл.2.7.6). Открытый текст «БЛАНК»

G-контурная многоалфавитная замена

Данный метод шифрования предполагает многократное использование системы шифрования Вижинера при использовании различных ключей. *n*-контурная многоалфавитная замена предполагает наличие *n* различных ключей – K_1, K_2, ..., K_n. Открытый текст *T* в начале шифруется с помощью ключа K_1, затем результат шифрования обрабатывается с помощью ключа K_2 и т.д. до ключа K_n. Полученный в результате шифрования на ключе K_n текст и является искомым шифротекстом.

Шифрование методами перестановки

Шифрование перестановкой заключается в том, что символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста. Данные преобразования приводят к изменению только порядка следования символов исходного сообщения [36].

При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

При шифровании *методом простой перестановки* производят деление открытого текста на блоки одинаковой длины, равной длине ключа. Ключ длины *n* представляет собой последовательность неповторяющихся чисел от 1 до *n*, в этом случае каждое из данных чисел встретится в ключе ровно один раз. Символы открытого текста внутри каждого из блоков переставляют в соответствие с символами ключа. Элемент ключа K_i в заданной позиции блока говорит о том, что на данное место будет помещен символ открытого текста с номером K_i из соответствующего блока[35].

[35] *М.А. Иванов. Криптографические методы защиты информации в компьютерных системах и сетях. "КУДИЦ-ОБРАЗ" Москва 2001*

Пример 8.

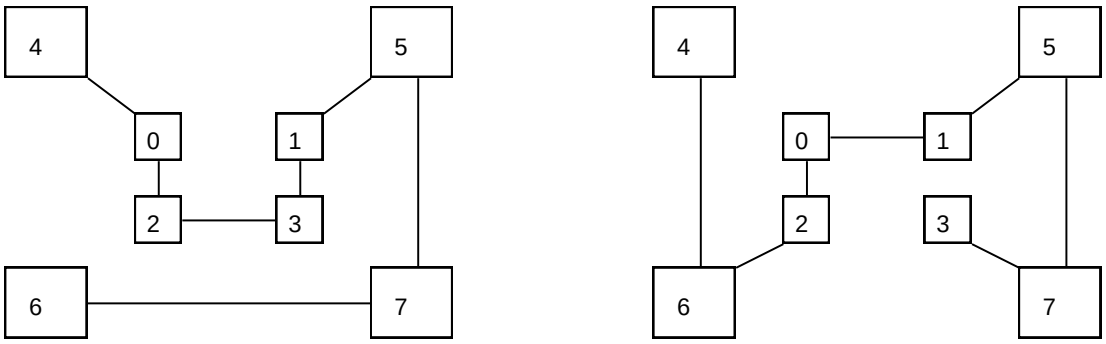
Зашифруем открытый текст «ПРИЕЗЖАЮ ДНЕМ» методом перестановки с ключом *К*=3142.

П	Р	И	Е	З	Ж	А	Ю	Д	Н	Е	М
3	1	4	2	3	1	4	2	3	1	4	2
И	П	К	Р	А	З	Ю	Ж	Е	Д	М	Н

(табл. 2.7.7). Открытый текст «ПРИЕЗЖАЮ ДНЕМ»

Для дешифрования шифротекста необходимо символы шифротекста перемещать в позицию, указанную соответствующим им символом ключа [36] K_i.

Весьма высокую стойкость шифрования можно обеспечить усложнением перестановок по *маршрутам типа гамильтоновских*. При этом, для записи символов шифруемого текста используются вершины некоторого гиперкуба, а знаки зашифрованного текста считываются по маршрутам Гамильтона, причем используется восемь различных маршрутов. Размер ключа перестановки в данном случае равен восьми. Для примера, два из маршрутов Гамильтона представлено на (рис.2.7.5). Первому маршруту соответствует перестановка 4-0-2-3-1-5-7-6, второму 4-6-2-0-1-5-7-3 *(нумерация символов в блоке осуществляется с нуля).*



(рис.2.7.5). Пример маршрутов Гамильтона

Пример 9.

---

[36] *М.А. Иванов. Криптографические методы защиты информации в компьютерных системах и сетях. "КУДИЦ-ОБРАЗ" Москва 2001*

Зашифруем открытый текст «ВОСЕМЬ МАРШРУТОВ» с помощью перестановок Гамильтона при использовании в качестве ключа двух перестановок, представленных на рисунке.

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
В	О	С	Е	М	Ь		М	А	Р	Ш	Р	У	Т	О	В
4	0	2	3	1	5	7	6	4	6	2	0	1	5	7	3
М	В	С	Е	О	Ь	М		У	О	Ш	А	Р	Т	В	Р

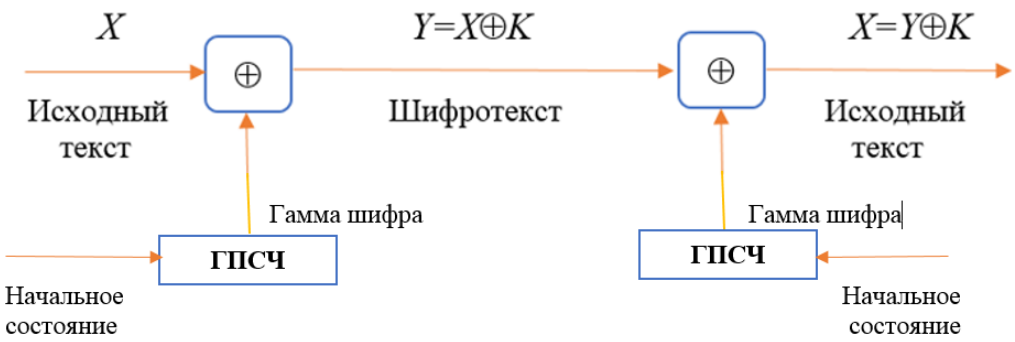
(табл.2.7.8). Открытый текст «ВОСЕМЬ МАРШРУТОВ»

Шифрование методом гаммирования

Определение 1. *Под гаммированием* понимают наложение на открытые данные по определенному закону гаммы шифра.

Определение 2. *Гамма шифра* - псевдослучайная последовательность, вырабатываемая по определенному алгоритму, используемая для зашифровки открытых данных и дешифровки шифротекста.

Общая схема шифрования методом гаммирования представлена на (рис. 2.7.6).



(рис.2.7.6). Схема шифрования методом гаммирования

Принцип шифрования заключается в формировании генератором псевдослучайных чисел *(ГПСЧ)* гаммы шифра и наложении этой гаммы на открытые данные обратимым образом, например, пути сложения по модулю два. Процесс дешифрования данных сводится к повторной генерации гаммы шифра и наложении гаммы на зашифрованные данные. Ключом шифрования в данном случае является начальное состояние генератора псевдослучайных

чисел. При одном и том же начальном состоянии ГПСЧ будет формировать одни и те же псевдослучайные последовательности [36].

Перед шифрованием открытые данные обычно разбивают на блоки одинаковой длины, например, по 64 бита. Гамма шифра также вырабатывается в виде последовательности блоков той же длины. Схему шифрования можно записать в этом случае в виде

$$T_{Ш}^{(i)} = Г_{Ш}^{(i)} \oplus T_{О}^{(i)}, i = \overline{1, N}$$

где $T_{Ш}^{(i)}$ - i-ый блок шифротекста, $Г_{Ш}^{(i)}$ - i-ый блок гаммы шифра, $T_{О}^{(i)}$ - i-ый блок открытого текста, N – количество блоков открытого текста.

Дешифрование в данном случае осуществляется по следующей формуле:

$$T_{О}^{(i)} = Г_{Ш}^{(i)} \oplus T_{Ш}^{(i)}, i = \overline{1, N}$$

Стойкость шифрования методом гаммирования определяется главным образом свойствами гаммы - длиной периода и равномерностью статистических характеристик. Последнее свойство обеспечивает отсутствие закономерностей в появлении различных символов в пределах периода. Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей. По сути дела, гамма шифра должна изменяться случайным образом для каждого шифруемого блока.

Обычно разделяют две разновидности гаммирования - с конечной и бесконечной гаммами. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной периода гаммы. При этом, если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретически является абсолютно стойким, т.е. его нельзя вскрыть при помощи статистической обработки зашифрованного текста, а

можно раскрыть только прямым перебором. Криптостойкость в этом случае определяется размером ключа[37].

В настоящее время разработано множество алгоритмов работы генераторов псевдослучайных чисел, которые обеспечивают удовлетворительные характеристики гаммы. Рассмотрим несколько примеров данных алгоритмов.

Метод фон Неймана

Суть данного метода состоит в том, что каждое последующее случайное число получается путем возведения в квадрат предыдущего числа с отбрасыванием цифр младших и старших разрядов.

Пусть A_0 – четырехзначное число - начальное состояние ГПСЧ. Тогда i - ое псевдослучайное число A_i получается из предыдущего числа A_{i-1} в результате следующих преобразований [36]:

1. Возведение A_{i-1} в квадрат, то есть нахождение числа A_{i-1}^2.
2. В качестве A_i выбирают четыре средние цифры числа A_{i-1}^2.

Пример 10.

Пусть A_0=1204, A_0^2=1449616. Тогда A_1=4496, A_1^2=20214016, A_2=2140 и т.д.

Однако метод фон Неймана является очень ненадежным, обладает множеством недостатков, в связи с чем, используется достаточно редко.

Линейный конгруэнтный метод

Данный генератор вырабатывает последовательность псевдослучайных чисел $Y_1, Y_2, ..., Y_{i-1}, Y_i, ...$, используя соотношение

$$Y_i = (a*Y_{i-1}+b) \bmod m, \quad (10)$$

где Y_i – i-ое *(текущее)* число последовательности; Y_{i-1} – предыдущее число последовательности; a, b, m – константы; m – модуль; a – коэффициент; b – приращение; Y_0 – начальное состояние ГПСЧ.

---

[37] *М.А. Иванов. Криптографические методы защиты информации в компьютерных системах и сетях. "КУДИЦ-ОБРАЗ" Москва 2001*

Обычно значение модуля m берется равным 2^n, либо простому числу. Приращение b должно быть взаимно простым с m, коэффициент a должен быть нечетным числом.

Линейный конгруэнтный метод является одним из самых простейших методов генерации псевдослучайных последовательностей. Существует ряд методов, формирующих намного более криптографический стойкие псевдослучайные последовательности.

Вопросы для самоконтроля

1. Охарактеризуйте подход к криптографической защите, используемый в симметричных криптосистемах.
2. Перечислите недостатки симметричных криптосистем.
3. Охарактеризуйте шифры замены.
4. В чем отличие методов моно алфавитной замены от методов многоалфавитной замены? Приведите примеры шифров каждого из этих классов.
5. Опишите подход к шифрованию, используемый в шифре Цезаря.
6. В чем заключается разница между шифром Цезаря и простой моно алфавитной заменой?
7. В чем заключаются сходство и различие шифров Цезаря, Гронсфельда и Вижинера. Попарно сравните данные шифры.
8. Опишите подход к криптографической защите, используемый в шифре Вернама? В чем его недостатки?
9. В чем заключается шифрование методами перестановки?
10. Опишите подход к шифрованию методами перестановки, основанный на маршрутах Гамильтона.
11. В чем заключается подход к шифрованию методом гаммирования?
12. Дайте определение гаммы шифра.
13. Что является ключом шифрования в шифрах гаммирования?

14. Опишите линейный конгруэнтный метод формирования псевдослучайных последовательностей.

8-§. Защита в информационных системах

Ключевые слова: *требования к защите информации, системы защиты информации, ядро системы защиты информации, ресурсы системы защиты информации*

Требования к защите информации:

Конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации, определяются совокупностью следующих факторов[38]:

- характером обрабатываемой информации;
- объемом обрабатываемой информации;
- продолжительностью пребывания информации в автоматизированной системе обработки информации;
- структурой автоматизированной системы обработки данных;
- видом защищаемой информации;
- технологией обработки информации;
- организацией информационно-вычислительного процесса в автоматизированной системе обработки данных;
- этапом жизненного цикла автоматизированной системы обработки данных.

Информация должна защищаться во всех структурных элементах информационной системы. На (рис.2.8.1.) представлена структурная схема автоматизированной системы обработки информации с мэйнфреймовой

[38] *С.В. Запечников. Информационная безопасность открытых систем. В 2-х т. Т.2 - Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ, 2018. - 558 с.*

структурой *(одним центральным вычислителем и пользовательскими местами в виде терминалов)*. Именно такая система обеспечивает наиболее эффективную защиту информации. Если терминалами пользователя являются персональные компьютеры, необходимо сделать конструктивно невозможными бесконтрольные снятие и ввод информации через устройства ввода-вывода *(например, физически заблокировать или удалить все разъемы подключения USB-устройств, порты ввода-вывода, устройства чтения гибких и лазерных дисков)*.

(рис.2.8.1). Структурная схема информационной системы

Защита информации в терминалах пользователей[33]:

- защищаемая информация может находиться только во время сеанса;
- должна быть исключена возможность просмотра отображаемой информации со стороны;
- информация, имеющая ограничительный гриф, должна выдаваться *(отображаться)* совместно с этим грифом.

Защита информации в устройствах группового ввода-вывода:

✓ в устройствах группового ввода-вывода информация может находиться только во время решения задач либо с нормированной длительностью хранения;

✓ устройства отображения и фиксации информации должны исключать возможность просмотра отображаемой информации со стороны;

✓ информация, имеющая ограничительный гриф, должна выдаваться *(отображаться)* совместно с этим грифом.

Защита информации в аппаратуре и линиях связи:

- в аппаратуре и линиях связи защищаемая информация должна находиться только в течение сеанса;
- линии связи, по которым защищаемая информация передается в явном виде, должны находиться под непрерывным контролем на все время сеанса передачи;
- перед началом каждого сеанса передачи должна осуществляться проверка адреса выдачи данных;
- при передаче большого объема защищаемой информации проверка адреса передачи должна производиться периодически *(через заданные промежутки времени или после передачи заданного числа знаков сообщения)*;
- при наличии в составе аппаратуры связи процессоров и запоминающих устройств должна вестись регистрация данных обо всех сеансах передачи защищаемой информации.

Защита информации в центральном вычислителе [33]:

- ✓ защищаемая информация в оперативном запоминающем устройстве может находиться только во время сеансов решения соответствующих задач, во внешних запоминающих устройствах - минимальное время, определяемое технологией решения соответствующей прикладной задачи в автоматизированной системе обработки данных;
- ✓ устройства отображения и фиксации информации должны исключать возможность просмотра отображаемой информации со стороны;
- ✓ информация, имеющая ограничительный гриф, должна выдаваться *(отображаться)* совместно с этим грифом;
- ✓ при обработке защищаемой информации должно осуществляться установление подлинности всех участвующих в обработке устройств и пользователей с ведением протоколов их работы;
- ✓ всякое обращение к защищаемой информации должно проверяться на санкционированность;

✓ при обмене защищаемой информации, осуществляемом с использованием линий связи, должна осуществляться проверка адресов корреспондентов.

Защита информации во внешних запоминающих устройствах.

- сменные носители информации должны находиться на устройствах управления в течение минимального времени, определяемого технологией автоматизированной обработки информации;
- устройства управления внешних запоминающих устройств, на которых установлены носители с защищаемой информацией, должны иметь замки, предупреждающие несанкционированное изъятие или замену носителя.

Защита информации в хранилище носителей[33]:

✓ все носители, содержащие защищаемую информацию, должны иметь четкую и однозначную маркировку, которая, однако, не должна раскрывать содержания записанной на них информации;

✓ носители, содержащие защищаемую информацию, должны храниться таким образом, чтобы исключались возможности несанкционированного доступа к ним;

✓ при выдаче и приемке носителей должна осуществляться проверка личности

✓ получающего *(сдающего)* и его санкции на получение *(сдачу)* этих носителей.

Защита информации для всех устройств: для всех устройств должна быть предусмотрена возможность аварийного уничтожения информации.

Системы защиты информации.

С целью всесторонней защиты информации рекомендуется создать единую, целостную систему, являющуюся функционально самостоятельной подсистемой любого объекта обработки информации. Такое решение позволяет объединить все ресурсы, средства и методы, а также полноценно координировать мероприятия по защите информации.

Организационно система защиты информации *(СЗИ)* должна состоять из трех механизмов:

- обеспечения защиты информации;
- управления средствами защиты;
- общей организации работы системы.

Ядро системы защиты информации

Ядро системы защиты предназначено для объединения всех подсистем системы защиты информации в единую целостную систему и организации ее функционирования.

Ядро может включать в себя организационные и технические составляющие.

Организационная составляющая представляет собой совокупность специально выделенных для защиты информации сотрудников, выполняющих свои функции в соответствии с разработанными правилами, а также нормативную базу, регламентирующую выполнение этих функций.

Техническая составляющая обеспечивает техническую поддержку организационной составляющей и представляет собой совокупности технических средств отображения состояний элементов системы защиты информации, контроля доступа к ним, управления их включением и т. д. Чаще всего эти средства объединены в соответствующий пульт управления системы защиты информации [33].

Ядро системы защиты информации должно обеспечивать выполнение двух функций.

- Включение компонентов системы защиты информации в работу при поступлении запросов на обработку защищаемой информации и блокирование бесконтрольного доступа к ней. Для этого требуется:
  - ✓ оборудование объекта средствами охранной сигнализации;
  - ✓ хранение носителей защищаемой информации в отдельных хранилищах *(документация, шифры, магнитные носители и т. д.)*;

✓ включение блокирующих устройств, регулирующих доступ к элементам системы защиты информации при предъявлении соответствующих полномочий и средств сигнализации.

- Организация и обеспечение проверок правильности функционирования системы защиты информации. При этом реализуется проверка:

✓ аппаратных средств - по тестовым программам и организационно;

✓ физических средств - организационно *(плановые проверки средств охранной сигнализации, сигнализации о повышении давления в кабелях и т. д.)*;

✓ программных средств — по специальным контрольным суммам *(на целостность)* и по другим идентифицирующим признакам.

Ресурсы системы защиты информации

Ресурсы информационно-вычислительной системы, необходимые для создания и поддержания функционирования системы защиты информации, как и любой другой автоматизированной системы, объединяются в техническое, математическое, программное, информационное и лингвистическое обеспечение.

Техническое обеспечение - совокупность технических средств, необходимых для технической поддержки решения всех тех задач защиты информации, которые возникают в процессе функционирования системы защиты информации.

Математическое обеспечение - совокупность математических методов, моделей и алгоритмов, необходимых для оценки уровня защищенности информации и решения других задач защиты.

*Программное обе*спечение - совокупность программ, реализующих программные средства защиты, а также программ, необходимых для решения задач управления механизмами защиты. К ним должны быть отнесены также сервисные и вспомогательные программы системы защиты информации.

Информационное обеспечение - совокупность систем классификации и кодирования данных о защите информации, массивы данных системы защиты информации, в также входные и выходные документы системы защиты информации.

Лингвистическое обеспечение - совокупность языковых средств, необходимых для обеспечения взаимодействия компонентов системы защиты информации между собой, с компонентами объекта обработки информации, с внешней средой.

Организационное построение

Организационное построение системы защиты информации в самом общем случае может быть представлено совокупностью следующих рубежей защиты[39]:

- территории, занимаемой системой защиты информации;
- зданий, расположенных на территории;
- помещений внутри здания, в которых расположены ресурсы системы защиты информации и защищаемая информация;
- ресурсов, используемых для обработки и хранения информации и самой защищаемой информации;
- линий связи, проходящих в пределах одного и того же здания;
- линий *(каналов)* связи, проходящих между различными зданиями, расположенными на одной и той же охраняемой территории;
- линий *(каналов)* связи, соединяющих системы защиты информации с другими объектами вне охраняемой территории.

Вопросы для самоконтроля

1. Что такое «*система защиты информации*»?

[39] *С.В. Запечников. Информационная безопасность открытых систем. В 2-х т. Т.2 - Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ, 2018. - 558 с.*

2. Какие способы защиты информации вам известны?
3. В чем заключается нарушение достоверности? Приведите пример.
4. В чем заключается нарушение целостности? Приведите пример.
5. В чем заключается нарушение доступности? Приведите пример.
6. Каким образом можно классифицировать угрозы информации?
7. Какие факторы влияют на требования к защите информации в конкретной информационной системе?
8. При помощи каких средств реализуется защита информации?
9. Какие семь рубежей защиты в системе защиты информации вам известны?

9-§. Организация защиты сети

Ключевые слова: *сеть, безопасность сети, службы безопасности сети, автоматизированные системы, корпоративная сеть*

Безопасность сети включает политики, практические методы и технологии, позволяющие предотвращать атаки на сети и доступные сетевые ресурсы организации.

Сеть - это компонент, подверженный большому риску. Обычно сеть и определяет реальный периметр безопасности. Поэтому при попытке доступа к ИТ-ресурсам первым шагом злоумышленников часто является проникновение в сеть.

Безопасность сети - это обязательное условие общей кибербезопасности, поскольку сеть является важнейшей линией защиты против атак извне.

Поскольку практически все данные и приложения связаны с сетью, надежная система безопасности сети гарантированно защитит от утечки данных. Однако при все более активном использовании сети, внедрении беспроводной связи и подключении устройств множества разных типов обеспечение безопасности сети становится все более сложной задачей. Чтобы ресурсы были полностью защищены, процесс обеспечения безопасности сети должен быть полностью согласован со всеми этими изменениями.

Безопасность сети - это прежде всего *защита сети* и всех подключенных к ней ресурсов от всяческих угроз. Безопасность сети включает физические и программные меры противодействия, призванные защитить инфраструктуру сети от несанкционированного доступа, некорректной работы, неправомерного использования, модификации и разрушения.

С другой стороны сетевая безопасность - прикладная научная дисциплина, отрасль информатики. Занимается вопросами обеспечения информационной безопасности сети и её ресурсов, в частности, хранящихся в ней и передающихся по ней данных и работающих с ней пользователей. Является расширением компьютерной безопасности *(как дисциплины)* и подразделом информационной безопасности. Занимается изучением и разработкой методов и практических правил работы с сетью, в том числе протоколами связи и обмена данными и криптографическими методами защиты информации [33].

Среди рисков, которым подвергается компьютерная сеть и предотвращение которых является целью сетевой безопасности как дисциплины: несанкционированный доступ к сетевым ресурсам *(например, несанкционированное чтение файлов)* и предотвращение атак, целью которых является отключение тех или иных предоставляемых сетью услуг.

Кроме дисциплины, под термином «сетевая безопасность» может пониматься комплекс процедур, стандартов, правил и средств, призванных обеспечить безопасность сети. Среди как аппаратных, так и программных средств и устройств, для этой цели применяемых: межсетевые экраны *(файрволлы)*, антивирусные программы, средства мониторинга сети, средства обнаружения попыток несанкционированного доступа *(вторжения)*, прокси-серверы и серверы аутентификации.

Обеспечение сетевой безопасности является одно из важных аспектов деятельности.

Службы безопасности сети

Службы безопасности сети указывают направления нейтрализации возможных угроз безопасности. Службы безопасности находят свою практическую реализацию в различных механизмах безопасности. Одна и та же служба безопасности может быть реализована с использованием разных механизмов безопасности или их совокупности. Международная организация стандартизации *(МОС)* определяет следующие службы безопасности[40]:

1. аутентификация *(подтверждение подлинности)*;
2. обеспечение целостности;
3. засекречивание данных;
4. контроль доступа;
5. защита от отказов.

Обеспечение безопасности информации в крупных *автоматизированных системах* является сложной задачей. Реальную стоимость содержащейся в таких системах информации подсчитать сложно, а безопасность информационных ресурсов трудно измерить или оценить. Объектом защиты в современных АИС выступает территориально

[40] *С.В. Запечников. Информационная безопасность открытых систем. В 2-х т. Т.2 - Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ, 2018. - 558 с.*

распределенная гетерогенная сеть со сложной структурой, предназначенная для распределенной обработки данных, часто называемая *корпоративной сетью*. Характерной особенностью такой сети является то, что в ней функционирует оборудование самых разных производителей и поколений, а также неоднородное программное обеспечение, не ориентированное изначально на совместную обработку данных [33].

Решение проблем безопасности АИС заключается в построении целостной системы защиты информации. При этом защита от физических угроз, например, доступа в помещения и утечки информации за счет ПЭМИ, не вызывает особых проблем. На практике приходится сталкиваться с рядом более общих вопросов *политики безопасности*, решение которых обеспечит надежное и бесперебойное функционирование информационной системы.

Главными этапами построения политики безопасности являются следующие:

- обследование информационной системы на предмет установления ее организационной и информационной структуры и угроз безопасности информации;
- выбор и установка средств защиты;
- подготовка персонала работе со средствами защиты;
- организация обслуживания по вопросам информационной безопасности;
- создание системы периодического контроля информационной безопасности ИС.

В результате изучения структуры информационных систем *(ИС)* и технологии обработки данных в ней разрабатывается *Концепция информационной безопасности ИС*, на основе которых в дальнейшем проводятся все работы по защите информации в ИС. В концепции находят отражение следующие основные моменты:

- организация сети организации;

- существующие угрозы безопасности информации, возможности их реализации и предполагаемый ущерб от этой реализации;
- организация хранения информации в ИС;
- организация обработки информации *(на каких рабочих местах и с помощью какого программного обеспечения)*;
- регламентация допуска персонала к той или иной информации;
- ответственность персонала за обеспечение безопасности.

В конечном итоге на основе Концепции информационной безопасности ИС создается *схема безопасности,* структура которой должна удовлетворять следующим условиям [33]:

1. защита от несанкционированного проникновения в корпоративную сеть и возможности утечки информации по каналам связи;
2. разграничение потоков информации между сегментами сети;
3. защита критичных ресурсов сети;
4. защита рабочих мест и ресурсов от несанкционированного доступа *(НСД)*;
5. криптографическая защита информационных ресурсов.

В настоящее время не существует однозначного решения, аппаратного или программного, обеспечивающего выполнение одновременно всех перечисленных условий. Требования конкретного пользователя по защите информации в ИС существенно разнятся, поэтому каждая задача решается часто индивидуально с помощью тех или иных известных средств защиты. Считается нормальным, когда 10 – 15% стоимости информации тратится на продукты, обеспечивающие безопасность функционирования сетевой информационной системы.

Некоторые зарубежные средства обеспечения информационной безопасности в сетях

Средства управления доступом	
Аутентификация *(authentication)*	Symark - Symark PowerPassword®
Авторизация *(authorization)*	Computer Associates - eTrustIM Access Control; Symark *(http://www.symark.com*) - Symark PowerBroker®.
Управление идентификацией *(identity management)*	Entegrity - AssureAccess; Entrust - GetAccess; IBM® Tivoili - Access Manager; Netegrity - Identity Minder; Novell - IChain; Novell - Nsure and Secure Access; Oblix - IDLink; OpenNetwork - nCross Platform Active Directory; RSA Security Identity Management; Secure Computing - Safe Word
Средства фильтрации	
Межсетевые экраны *(firewalls)*	CyberGuard *(http://www.cyberguaid.com)* - SL3200, KS1500; TippingPoint Technologies, Inc. - UnityOneTM Intrusion Prevention Systems & Appliances; Akonix® Systems, Inc. Akonix L7 Enterprise; Astaro Corporation - Astaro Security Linux; Check Point Software Technologies Ltd - VPN-l/FireWall-lTM Next Generation with Application Intelligence; Fortinet - FortiGate Antivirus Firewalls; NetScreen - 5000 Series; Secure Computing - Sidewinder G2 Firewall; Stonesoft, Inc. StoneGate;

	Zone Labs, Inc. - Zone Labs IntegrityTM
Активный контекстный мониторинг/ фильтрация *(active content monitoring/filtering)*	Computer Associates *(http://www.ca.com)* - eTrustIM Secure Content Manager; NetlQ *(http://www.netiq.com)* - WebMarshal; TippingPoint Technologies, Inc. *(http://www.tippingpoint.com)* - UnityOne™ Intrusion Prevention Systems & Appliances; Vericept *(http://www.vericept.com)* - Vericept Intelligent Early Warning (VIEW) Monitoring Solutions; Vericept - Vericept Intelligent Early Warning *(VIEW)* Filter Solutions; Cerberian - Cerberian Web Manager; Fast Data Technology - FastTracker; PestPatrol, Inc. - PestPatrol; SurfControl - Total Filtering Solution; 8e6 Technologies - R3000 Internet Filter
Защита от распределенных атак "отказ в обслуживании" *(antiDDoS tools)*	Arbor Network - Peakflow; PestPatrol - PestPatrol
Защита от компьютерных червей *(anti-worm solutions)*	ForeScout Technologies *(http://www.forescout.com)* - WormScout
Защита от спама *(spam protection)*	Computer Associates - eTrustIM Secure Content Manager; Frontbridge Technologies - TrueProtect™ Message Management System;

	NetlQ - MailMarshal; Sunbelt Software *(http://www.sunbeltsoftware.com)* - iHateSpam™ Server Edition; Sunbelt Software - iHateSpam™ Gateway Edition; Aladdin Knowledge Systems - eSafe Advanced Anti-Spam Module; Barracuda Networks Barracuda Spam Firewall; FutureSoft DynaComm i:mail™
Средства защиты, использующие криптографические методы	
Удостоверяющий центр. *(certificate authority)*	Ubizen, Inc. *(http://www.ubizen.com)* – Ubizen OnlineGuardian® Certificate Management
Шифрование файлов и сеансов связи. *(file and session encryption)*	Absolute Software Corporation - Absolute®Encrypt; F-Secure, Inc.® - F-Secure® SSHTM; Global Technologies Group, Inc. - CompuSec - Free Encryption Software; Vormetric, Inc. - CoreGuardTM Core Security System
Виртуальные частные сети и защищенные коммуникации. *(virtual private networks and cryptographic communications)*	CyberGuard - SL3200, KS1500; V-ONE Corporation - SmartGate®; Communication Devices, Inc. - Port Authority Secure Out of Band Management

Виртуальные частные сети на основе протокола. SSL *(SSL VPNs)*	Whale Communications - e-Gap Remote Access SSL VPN; Avential - EX1500TM SSL VPN Appliance; Neoteris - SA 1000/3000/5000 Series; Aspelle - Aspelle Everywhere V.3.0; PortWise - PortWise mVPN; Seagull Software Systems – Seagull Secure FTP Pro™; Array Networks - Array SP/SP-C; Netilla Networks - Netilla® Security Platform *(NSP)*; F5 Networks - FirePass™ Product Family; InfoExpress, Inc. - CvberArmor
Системы отражения вторжений и поиска уязвимостей	
Системное обнаружение вторжений. *(host-based intrusion detection)*	Configuresoft *(http://www.configuresoft.com)* – Enterprise Configuration Manager; Configuresoft - Security Update Manager; NetlQ - Security Manager; Sunbelt Software - Sunbelt Server Event Manager
Сетевое обнаружение вторжений. *(network-based intrusion detection)*	Computer Associates - eTrustIM Intrusion Detection; Lancope - StealthWatch
Сервисы безопасности: тесты на возможность проникновения. *(security services:*	BindView Penetration Testing *(http://www.bindview.com)*; Qualys - QualysGuard Consultant

penetration testing)	
Сетевые сканеры уязвимостей. *(network-based vulnerability scanners)*	BindView - bv-Control for Internet Security; eEye Digital Security - Retina® Network Security Scanner; Harris Corp *(http://www.harris.com)* - STAT Scanner, STAT Analyzer; Harris Corp - STAT DVM, STAT Scanner Console; Qualys - QualysGuard Enterprise; Qualys - QualysGuard Express; Sunbelt Software - Sunbelt Network Security Inspector™; Application Security, Inc. - AppDetective; Lumeta - IPsonar 2.5; nCircle Network Security - IP360 Vulnerability Management System; Tenable Network Security - NeWT and NeVO; Visionael® - Visionael® Security Audit™
Средства управления безопасностью сети	
Реализация ПБ организации. *(enterprise security policy implementation)*	BindView Policy Compliance Suite; Configuresoft – Enterprise Configuration Manager; Configuresoft - Security Update Manager; CyberGuard - Global Command Center, Central Management; eEye Digital. Security - eEye's Enterprise Vulnerability Assessment & Remediation Solution; TippingPoint Technologies, Inc. - UnityOne™ Intrusion Prevention Systems & Appliances; NetVision Inc. NVPolicy Resource Center.
Разработка ПБ *(Policy development)*	Vericept - Vericept Professional Services

Средства администрирования безопасности организации. *(Enterprise security administration)*	BindView Vulnerability Management Suite: BindView Policy Compliance Suite; Computer Associates - eTrust™ Admin; Configuresoft - Enterprise Configuration Manager; Configuresoft - Security Update Manager; CyberGuard Global Command Center; eEye Digital Security *(http://www.eeye.com)* - REMTM Remote Enterprise Management; NetlQ - Security Administration Suite; NetlQ - Group Policy Administrator; Sunbelt Software - Directory Inspector™; Sunbelt Software - LanHound™; TippingPoint Technologies, Inc. - UnityOne™ Intrusion Prevention Systems & Appliances; FireVue Security Systems - LogAppliance; Symmetricom - SyncServer® S100 Network Time Server; SSH Communications Security, Inc. - SSH Tectia™
Свободно распространяемые средства защиты в сетях различного назначениями.	Nessus; Snort/Snarf; Ethereal; Nmap; ActivePorts; TCPView; Logcheck; Sara; Tripwire

(табл. 2.9.1). Зарубежные средства обеспечения информационной безопасности

Вопросы для самоконтроля

1. Что такое сеть?
2. Что включает в себя безопасность сети?

3. Какие службы безопасности сети определяет Международная организация стандартизации (МОС)?
4. Что такое корпоративная сеть?
5. Каковы главные этапы построения политики безопасности?
6. Перечислите некоторые зарубежные средства обеспечения информационной безопасности в сетях.

10-§. Организация защиты сети интернет

Ключевые слова: *принципы защиты информации, аутентификация, классификация средств защиты информации, подстановка, перестановка, гаммирование.*

Обзор защиты информации в интернете

Сегодня одной из самых актуальных проблем в сфере информационно-вычислительных систем является защита информации в интернете. Действительно, мало кто мыслит свою жизнь без электронной глобальной сети. Люди ведут различные финансовые операции в интернете, заказывают товары, услуги, пользуются кредитными карточками, проводят платежи, разговаривают и переписываются, совершают много других действий, требующих обеспечения конфиденциальности и защиты.

Конфиденциальная информация в сети интернет

Конфиденциальная информация, которая передается по сети интернет, проходит через определенное количество маршрутизаторов и серверов, прежде чем достигнет пункта назначения. Обычно маршрутизаторы не отслеживают проходящие сквозь них потоки информации, но возможность того, что информация может быть перехвачена, существует. Более того, информация может быть изменена и передана адресату в измененном виде. К сожалению, сама архитектура сети интернет всегда оставляет возможность для недобросовестного пользователя осуществить подобные действия.

Всегда существует проблема выбора между необходимым уровнем защиты и эффективностью работы в сети. В некоторых случаях пользователями или потребителями меры по обеспечению безопасности могут быть расценены как меры по ограничению доступа и эффективности[41].

Принципы защиты информации в сети интернет

Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на четыре основных типа[37]:

- *перехват информации* - целостность информации сохраняется, но ее конфиденциальность нарушена;
- *модификация информации* - исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;
- *подмена* авторства информации;
- *перехват сообщения* с его изъятием.

Данная проблема может иметь серьезные последствия. Например, кто-то может послать письмо от вашего имени *(этот вид обмана принято называть спуфингом)* или *web-сервер* может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров.

В соответствии с перечисленными проблемами при обсуждении вопросов безопасности под самим термином "*безопасность*" подразумевается совокупность трех различных характеристик обеспечивающей безопасность системы:

1. *Аутентификация* - это процесс распознавания пользователя системы и предоставления ему определенных прав и полномочий. Каждый раз, когда заходит речь о степени или качестве аутентификации, под этим следует понимать степень защищенности системы от посягательств сторонних лиц на эти полномочия.

---

[41] *В.П. Леонтьев. Безопасность в сети интернет. Москва ОЛМА Медиа Групп 2008.*

2. *Целостность* - состояние данных, при котором они сохраняют свое информационное содержание и однозначность интерпретации в условиях различных воздействий. В частности, в случае передачи данных под целостностью понимается идентичность отправленного и принятого.

3. *Секретность* - предотвращение несанкционированного доступа к информации. В случае передачи данных под этим термином обычно понимают предотвращение перехвата информации.

Информационная безопасность

Этим термином принято обозначать само состояние информации, означающее, что система функционирует нормально, данные защищены и обеспечена безопасность их целостности, конфиденциальности и доступности. Также он может относиться и к определению этого процесса. Основные составляющие информационной безопасности подразумевают следующее: Если к данным есть доступ лишь у тех пользователей, кто авторизован, значит, они конфиденциальны [37].

Понятие доступности предполагает, что к ресурсам и связанным с ними активам будет обеспечен доступ для авторизованных пользователей, если возникает такая необходимость. Это три принципа защиты информации. Кроме них, еще выделяют принцип аутентичности, который означает, что должна быть обеспечена подлинность субъекта и объекта доступа. Проблемы и риски информационной безопасности источников, из которых может исходить угроза или несанкционированный доступ к вашим данным, существует несколько.

Первые – это источники антропогенного характера. Сюда относятся действия различных субъектов. Они могут быть преднамеренными либо случайными. Они разделяются на внешний и внутренний типы. Первый означает незаконное вторжение постороннего лица из внешней сети общего назначения.

Второй подразумевает собой действие изнутри, то есть со стороны сотрудников, к примеру. Все, что приводит к сбою или отказу работы

программного и технического средства, относится к техногенным источникам. Здесь могут быть виноваты банальные ошибки программного обеспечения, устаревшие устройства или системы, сбои оборудования *(кабельная или дисковая система, проблемы с сервером, рабочей станцией)*.

Всегда следует делать поправку и на какие-то чрезвычайные обстоятельства, поэтому выделяют стихийные источники. К ним относятся как любые случаи форс-мажорного характера, так и всяческие природные катаклизмы. Причин, по которым могут происходить утечка информации и осуществляться несанкционированный доступ к ней в сетях, достаточно много:

- она может быть перехвачена;
- модификация информации *(изменение исходного документа или сообщения либо его абсолютная подмена с последующей отсылкой адресату)*;
- фальсификация авторства *(если посылают любые данные от вашего имени)*;
- к серверу аппаратуры или линии связи может быть осуществлено незаконное подключение;
- кто-то может замаскироваться под авторизованного пользователя и присвоить себе его данные и полномочия;
- вводятся новые пользователи;
- после преодоления мер защиты носители информации и файлы могут быть скопированы;
- неправильное хранение архивных данных;
- некорректная работа обслуживающего персонала или пользователей;
- внедрение компьютерного вируса;
- недостатки вашей операционной системы или прикладных программных средств могут быть использованы против вас.

Система интернет зарождалась как абсолютно корпоративная. Но получилось так, что со временем она стала оперировать не только сетями образовательного, коммерческого, государственного, ведомственного, военного характера, что сами по себе подразумевают некий ограниченный доступ, но и простыми пользователями, которые легко получают прямой доступ в интернет с любого домашнего компьютера с помощью обычного модема и телефонной сети общего пользования [37].

При этом используются единый стек протоколов *TCP/IP* и единое адресное пространство. Такая простота доступа в интернет негативным образом сказывается на безопасности информации в сетях. А хуже всего то, что вы можете даже и не узнать, что ваши файлы или программы были скопированы, не говоря уже о возможности их порчи и корректировки. Защита информации в интернете является одной из главных проблем любой организации. Любая организация, которая хранит и обрабатывает данные в информационных системах, нуждается в средствах защиты информации:

- финансово-кредитные организации;
- коммерческие и государственные организации, у которых есть подключения в сетях общего пользования;
- территориально-распределенные организации;
- организации, которые вынуждены предоставлять внешний доступ к своим ресурсам информации;
- операторы связи.

Конечно, это далеко не весь перечень. И организации, которые вынуждены обезопасить свои информационные данные, становятся перед проблемой выбора между тем, насколько эффективной будет их работа в сетях, и необходимым уровнем защиты. Очень часто пользователи или потребители могут расценить такие меры безопасности как ограничение доступа либо снижение эффективности. Поэтому подбор средств для защиты информации каждая организация осуществляет индивидуально.

Классификация и обзор средств защиты информации.

Из-за того, что проблемы с безопасностью, как и источники угроз, бывают разными, возникла необходимость в создании различных видов ее обеспечения. Их классифицируют на несколько групп:

- средства аппаратного *(или технического)* характера;
- программные меры защиты;
- средства, которые относят к смешанному виду;
- меры организационного или административного характера.

К первой группе относятся разные устройства. Они могут быть электронными, механическими или электромеханическими, но специфика их работы предполагает защиту информации посредством аппаратных средств. Применение этих устройств позволит воспрепятствовать физическому проникновению или замаскировать данные, если доступ все же был открыт. Технические средства надежны, независимы от субъективных факторов и обладают высокой устойчивостью к модификации. Но у них есть и свои недостатки. В первую очередь это достаточно высокая цена. Также они недостаточно гибкие и практически всегда обладают большими массой и объемом [37].

Второй вид оперирует разнообразными программами, для того чтобы контролировать доступ, проводить идентификацию пользователей, тестировать контроль системы защиты информации. Кроме того, средства, относящиеся к этой группе, могут шифровать данные и удалять рабочую *(остаточную)* информацию *(вроде временных файлов)*. Если система использует программные средства для защиты, она получает массу преимуществ. Они гибкие и надежные, универсальные и достаточно просты в установке, а еще способны к модификации и предполагают определенное развитие. Однако этот вид средств очень чувствителен к случайным и преднамеренным изменениям. К другим недостаткам программной защиты можно отнести использование части ресурсов файл-сервера и рабочих станций, ограниченную функциональность сети и то, что ее средства могут зависеть от типа компьютера и его аппаратных средств.

Третья группа сочетает в себе свойства первой и второй. В последний вид входят средства защиты информации организационно-технического и организационно-правового характера. Сюда можно отнести[42]:

- контроль доступа в помещения, их подготовку и оснащение;
- разработку стратегий безопасности организации;
- подборку и изучение национальных законодательств с последующим их применением;
- учреждение правил работы и контроль их соблюдения.

Полноценная защита информации в интернете может быть достигнута при использовании всех этих средств в комплексе. Наиболее эффективные методы программных средств для того чтобы обеспечить необходимую секретность, часто обращаются за помощью к специалистам по криптографии или шифрованию информации. При создании зашифрованных данных используют определенный алгоритм или устройство, которое его реализует. Изменяющийся код ключа осуществляет управление шифрованием. Именно с его помощью вы сможете извлечь информацию. Среди классических алгоритмов, которые используются, выделяют несколько основных [37]:

Подстановка. Она может быть, как самой простой, одноалфавитной, так и многоалфавитной сложной *(однопетлевой и многопетлевой)*;

Перестановка. Различают простую и усложненную;

Гаммирование. Речь идет о смешивании, в котором могут использовать длинную, короткую, неограниченную маски. В первом случае исходный алфавит заменяется альтернативными. Это самый легкий способ шифрования. Данные, зашифрованные алгоритмом перестановки, будут более защищенными, ведь в нем используются цифровые ключи или эквивалентные слова. Система, отдавшая предпочтение гаммированию, получит гарантию надежности и безопасности информации, потому что для осуществления

[42] *В.П. Леонтьев. Безопасность в сети интернет. Москва ОЛМА Медиа Групп 2008.*

этого способа шифрования будет проведена серьезная криптографическая работа.

Для защиты используются нелинейные преобразования данных, методы рассечения-разнесения, компьютерная стеганография и прочее. К тому же существует различие между симметричным и несимметричным шифрованием. Первое означает, что для шифровки и дешифровки берутся одинаковые ключи *(это называется система с закрытыми ключами)*. Тогда как система с открытыми ключами подразумевает собой использование открытого ключа для шифра и закрытого – для его расшифровки [37].

Советы: Если же вы хотите обезопасить себя от возможных модификаций или подмены информации, тогда стоит воспользоваться электронной цифровой подписью. Так называется тоже зашифрованное сообщение, только для его шифровки берется закрытый ключ. Еще стоит проводить аутентификацию. Это означает, что должна быть установлена подлинность каждого пользователя, который представил идентификатор, либо осуществлена проверка. Ведь сообщить этот идентификатор может и совсем другое устройство *(лицо)*, а не тот пользователь, за которого оно себя выдает.

В этих целях обычно используются пароли, секретные вопросы. Эффективной является схема одноразовых паролей. Не стоит путать аутентификацию с авторизацией. При прохождении авторизации проверяются полномочия или права пользователя на то, имеет ли он доступ к конкретному ресурсу и может ли выполнять там какие-либо операции. Методы безопасности в компьютерных сетях если условно разделить все существующие средства защиты, то любая система должна обеспечить безопасность своих внутренних информационных ресурсов и защитить данные в процессе их передачи в интернете. К функциям первой области относятся межсетевые экраны *(или брандмауэры-firewalls)*, которые устанавливают в разрыв всех соединений внутренней сети с глобальной.

Что такое брандмауэр?

Брандмауэр представляет собой программный или аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и, в зависимости от настроек брандмауэра, блокирует их или позволяет им пройти в компьютер.

Брандмауэр поможет предотвратить проникновение хакеров или вредоносного программного обеспечения *(такого как черви)* в ваш компьютер через сеть или Интернет. Брандмауэр также помогает предотвратить отправку вредоносных программ на другие компьютеры.
Следующая иллюстрация показывает работу брандмауэра.

(рис. 2.10.1). Брандмауэр

Как кирпичная стена создает физическую преграду, брандмауэр создает препятствие между Интернетом и компьютером.

С их помощью можно разделить локальную сеть на две части или даже использовать межсетевые экраны для внутреннего деления, чтобы защитить одну подсеть от другой *(особенно актуально такое решение для крупных организаций, где необходимы независимые подразделения)*. Система может пострадать из-за любого вторжения в ее ресурс, ведь злоумышленники используют всевозможные средства для этого. Ваши данные могут быть стерты с помощью вируса, под вашим именем кто-то получит доступ к операционной системе, прочтет конфиденциальную информацию, заменит ее ложной, выведет все устройства и оборудование из рабочего состояния. Поэтому межсетевой экран должен уметь распознать, какие пользователи являются легальными, а какие-нет, правильно провести классификацию

сетевой активности, чтобы не допустить вредоносной, но и не помешать нужной. Набор правил, который будет сформирован, поможет определить условия, по каким пакетам должны проходить из одной части сети в другую. Если же организации нужно обеспечить безопасность информации в сетях, которая уже находится «в пути», тогда обычно обращаются к помощи средств виртуальных частных сетей *(VPN)*.

Очень важно, чтобы передаваемые данные, до того, как дойдут к месту назначения, не были искажены, уничтожены или просмотрены посторонними. Способы, используемые в этой области средств, тоже могут быть различными.

Существуют разграничения трафика, его шифрование, так что если у кого-то и получится добраться до самого пользовательского *IP-пакета*, то он сможет лишь удалить его, но не прочитает, не исказит и не подменит данные.

Организация, которая хочет защитить свои ресурсы самым надежным образом, должна применять комплексный подход. Кроме вышеназванных, понадобится система, которая будет осуществлять обнаружение вторжений, предотвращать их, не допускать утечек конфиденциальной информации. Еще желательно использование средств мониторинга сетей, анализа и моделирования информационных потоков, качественных антивирусных программ, не нужно забывать об архивировании и дублировании данных, резервном копировании, анализаторах протоколов, организационных и административных мерах, которые бы помогли предотвратить физический доступ посторонних к ее информации.

Вопросы для самоконтроля

1. На какие четыре основных типа можно разделить проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях?
2. Что такое аутентификация?
3. Что такое брандмауэр?
4. Информационная безопасность - это...

5. Какие характеристики обеспечивают безопасность системы?
6. Расскажите о классификации средств защиты информации.
7. Что такое гаммирование?

11-§. Организация защиты электронной почты

Ключевые слова: *электронная почта, угрозы электронной почте, фальшивые адреса отправителя, перехват писем, почтовые бомбы, угрожающие письма, способы защиты электронной почты*.

Особое место в новой информационной индустрии играет *Интернет, электронная почта* и *средства телекоммуникаций*. Интернет, открыв практически неограниченные возможности для быстрой и конфиденциальной связи. Как средство связи Интернет традиционно применяется для пересылки электронной почты, Интернет-телефонии и прочие. Электронная почта становится все более важным условием ведения повседневной деятельности.

Электронная почта - это способ передачи писем с помощью персональных компьютеров и средств телекоммуникаций. В качестве писем по электронной почте могут пересылаться самые различные текстовые файлы, изображения, программы и наборы данных.

(рис.2.11.1). Электронная почта

Исторически первый и наиболее распространенный вид работы в *телекоммуникационных сетях* - меж персональный обмен текстовыми

сообщениями, известный под названием «электронная почта» *(или E-mail).* Как и при обычной почтовой связи, здесь происходит обмен сообщениями, но не на бумаге, а в виде файлов. Преимущества электронной почты над обычной велики: многократно большая скорость доставки информации, компьютерная подготовка сообщений, передача информации в виде, допускающем последующую ее компьютерную обработку получателем *(редактирование, помещение в различные документы, базы данных и т.д.)*.

Система электронной почты организуется как совокупность региональных узловых станций, периодически связывающихся друг с другом для обмена корреспонденцией, для чего могут использоваться различные каналы связи. Для того, чтобы попасть с точки А в точку В, сообщение может проходить через несколько промежуточных узлов. На каждом узле работают специальные программы, которые получают сообщение и разбираются, куда его отправлять дальше[43].

Абоненты электронной почты обслуживаются «электронными узлами связи». Для обмена корреспонденцией между абонентом и узлом, как правило, используется обычная телефонная линия [37].

Абонентская станция состоит из персонального компьютера и модема. Каждый пользователь имеет свой почтовый ящик с уникальным адресом. Все письма, посланные по этому адресу, попадают в почтовый ящик пользователя. Пользователь может просмотреть, уничтожить или сохранить письма. Естественно, любой пользователь может послать письмо по любому адресу или сразу по нескольким адресам.

Происходящее сейчас бурное развитие компьютерных сетей и коммуникаций значительно расширяют возможности применения информационных технологий для обмена информацией между различными категориями пользователей. Вместе с внедрением в повседневную работу различных средств обмена информацией в электронном виде, все актуальнее

[43] *В.П. Леонтьев. Безопасность в сети интернет. Москва ОЛМА Медиа Групп 2008.*

становится проблема обеспечения ее безопасности: конфиденциальности, целостности и авторства.

Пользователь все больше хочет быть уверен, что отправленные им сообщения никто не прочитает, кроме указанного адресата. Получатель же хочет быть уверен, что информация получена именно из того источника, от которого он их ожидал. Для решения целей обеспечения безопасности передаваемой информации во всем мире все активнее применяются технологии криптографической защиты с использованием открытых ключей.

Угрозы, связанные с электронной почтой

Основные протоколы передачи почты *(SMTP, POP3, IMAP4)* обычно не осуществляют надёжной аутентификации, что позволяет легко создать письма с фальшивыми адресами. Ни один из этих протоколов не использует криптографию, которая могла бы гарантировать конфиденциальность электронных писем. Хотя существуют расширения этих протоколов, решение использовать их должно быть явно принято, как составная часть политики администрации почтового сервера. Некоторые такие расширения используют уже имеющиеся средства аутентификации, а другие позволяют клиенту и серверу согласовать тип аутентификации, который будет использоваться в данном соединении.

Фальшивые адреса отправителя

Адресу отправителя в электронной почте Интернета нельзя доверять, так как отправитель может указать фальшивый обратный адрес, или заголовок может быть модифицирован в ходе передачи письма, или отправитель может сам соединиться с *SMTP-портом* на машине, от имени которой он хочет отправить письмо, и ввести текст письма.

Перехват письма

Заголовки и содержимое электронных писем передаются в чистом виде. В результате содержимое сообщения может быть прочитано или изменено в процессе передачи его по Интернету. Заголовок может быть модифицирован,

чтобы скрыть или изменить отправителя, или для того чтобы перенаправить сообщение [37].

Почтовые бомбы

Почтовая бомба - это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока она не выйдет из строя. Как это может случиться, зависит от типа почтового сервера и того, как он сконфигурирован.

Некоторые провайдеры Интернета дают временные логины любому для тестирования подключения к Интернету, и эти логины могут быть использованы для начала подобных атак.

Типовые варианты выхода почтового сервера из строя:

- *Почтовые сообщения принимаются до тех пор*, пока диск, где они размещаются, не переполнится. Следующие письма не принимаются. Если этот диск также основной системный диск, то вся система может аварий, но завершиться.
- *Входная очередь переполняется сообщениями*, которые нужно обработать и передать дальше, до тех пор, пока не будет достигнут предельный размер очереди. Последующие сообщения не попадут в очередь.
- *У некоторых почтовых систем* можно установить максимальное число почтовых сообщений или максимальный общий размер сообщений, которые пользователь может принять за один раз. Последующие сообщения будут отвергнуты или уничтожены.
- *Может быть превышена квота диска для данного пользователя*. Это помешает принять последующие письма, и может помешать ему выполнять другие действия. Восстановление может оказаться трудным для пользователя, так как ему может понадобиться дополнительное дисковое пространство для удаления писем.
- *Большой размер почтового ящика* может сделать трудным для системного администратора получение системных предупреждений и сообщений об ошибках.

- *Посылка почтовых бомб* в список рассылки может привести к тому, что его члены могут отписаться от списка.

Угрожающие письма

Так как любой человек в мире может послать вам письмо, может оказаться трудным заставить его прекратить посылать их вам. Люди могут узнать ваш адрес из списка адресов организации, списка лиц, подписавшихся на список рассылки, или писем в *Usenet*. Если вы указали ваш почтовый адрес какому-нибудь web-сайту, от него может продать ваш адрес "почтовым мусорщикам". Некоторые веб-браузеры сами указывают ваш почтовый адрес, когда вы посещаете web-сайт, поэтому вы можете даже не понять, что вы его дали. Много почтовых систем имеют возможности фильтрации почты, то есть поиска указанных слов или словосочетаний в заголовке письма или его теле, и последующего помещения его в определённый почтовый ящик или удаления. Но большинство пользователей не знает, как использовать механизм фильтрации. Кроме того, фильтрация у клиента происходит после того, как письмо уже получено или загружено, поэтому таким образом тяжело удалить большие объёмы писем.

Одним часто используемым средством защиты, применяемым некоторыми пользователями *Usenet*, является конфигурирование своих клиентов для чтения новостей таким образом, что в поле *Reply-To (обратный адрес)* письма, посылаемого ими в группу новостей, помещается фальшивый адрес, а реальный адрес помещается в сигнатуре или в теле сообщения. Таким образом программы сбора почтовых адресов, собирающие адреса из поля *Reply-To*, окажутся бесполезными.

Способы защиты электронной почты

Защита от фальшивых адресов. От этого можно защититься с помощью использования шифрования для присоединения к письмам электронных подписей. Одним популярным методом является использование шифрования с открытыми ключами. Однонаправленная хэш-функция письма шифруется, используя секретный ключ отправителя. Получатель использует открытый ключ отправителя для расшифровки хэш-функции и сравнивает его с хэш-функцией, рассчитанной по полученному сообщению. Это гарантирует, что сообщение на самом деле написано отправителем, и не было изменено в пути.

Защита от перехвата. От него можно защититься с помощью шифрования содержимого сообщения или канала, по которому он передается. Если канал связи зашифрован, то системные администраторы на обоих его концах все-таки могут читать или изменять сообщения. Было предложено много различных схем шифрования электронной почты, но ни одна из них не стала массовой. Одним из самых популярных приложений является *PGP*.

PGP включает в себя плагины для нескольких популярных почтовых программ, что делает ее особенно удобной для включения в письмо электронной подписи и шифрования письма клиентом. Последние версии PGP используют лицензированную версию алгоритма шифрования с открытыми ключами RSA [37].

Корректное использование электронной почты.

Взаимодействие с помощью почты не должно быть неэтичным, не должно восприниматься как конфликтная ситуация, или содержать конфиденциальную информацию.

Политика защиты электронных писем и почтовых систем.

Защита писем, почтовых серверов и программ должна соответствовать важности информации, передаваемой по сетям. Как правило, должно осуществляться централизованное управление сервисами электронной почты. Должна быть разработана политика, в которой указывался бы нужный уровень защиты.

Вопросы для самоконтроля

1. Что такое электронная почта?
2. Назовите исторически первый и наиболее распространенный вид работы в телекоммуникационных сетях.
3. Расскажите об угрозах, связанных с электронной почтой.
4. Как происходит перехват электронных писем?
5. Что такое почтовая бомба?
6. Способы защиты электронной почты.

ГЛАВА 3. ТЕЛЕКОММУНИКАЦИИ И УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

==========

12-§. Системы управления подключением, методология

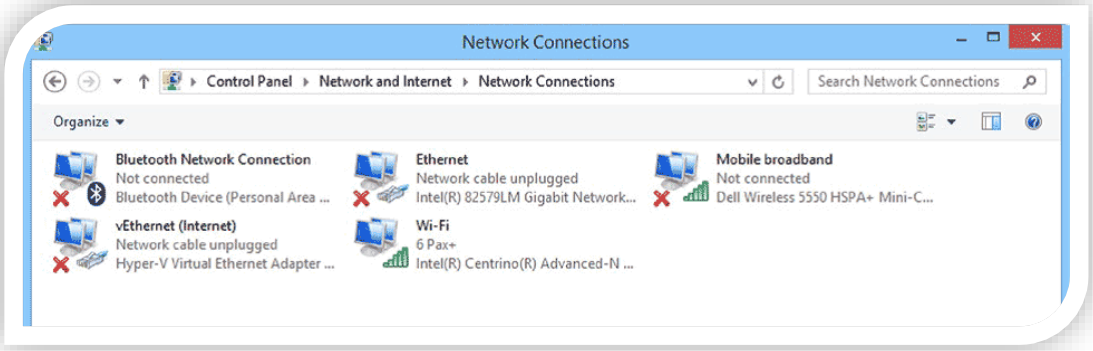
Ключевые слова: *управление сетевыми подключениями, управление сетями, защита сетей.*

Управление сетевыми подключениями

Для управления основным сетевым оборудованием, будь то *Ethernet, Bluetooth, Wi-Fi*, мобильный интернет или подключения других типов, также можно использовать "*Сеть*" - "Центр управления сетями и общим доступом ". Доступ к нему можно получить двумя способами: забив название в поле поиска кнопок или щелкнув правой кнопкой мыши по значку сети на рабочем столе.

Для просмотра, установленного на компьютере сетевого оборудования нужно щелкнуть в левой панели на ссылке *"Изменение параметров адаптера"*.

Открывшееся окно содержит все имеющиеся на компьютере сетевые подключения.



(рис. 3.12.1). Сетевое подключение

Щелчок правой кнопкой мыши на соединении позволит выполнить различные действия, они также доступны на панели инструментов в верхней части окна:

- *Отключить соединение*, так чтобы оно сохранялось в настройках сети, но доступ к нему был закрыт.
- *Подключить* и *отключить* от сети.
- *Проверить состояние сети*, полезно при трудностях с подключением.
- *Диагностировать проблемы* или *неисправности подключения*. Это автоматическое средство для устранения неполадок, сбрасывает соединение к его состоянию по умолчанию.
- *Проверить свойства соединения*. Здесь можно изменить настройки сетевого адаптера. Компьютер можно использовать для обмена с другими компьютерами, превращая его в мобильную точку доступа, или *включите/отключите* конкретные функции, которые могут быть причиной возникших проблем, например, *IPv6*.
- Какой-либо *опции для удаления соединения*, изменения функции автосоединения или параметров пароля не существует. Чтобы удалить подключение, выделите его и нажмите клавишу *Delete (Del)* на клавиатуре.

Внимание: *Windows 8.1* позволяет только выбирать состояние сетевого или Интернет-соединения. Иногда проще удалить соединение и восстановить его при перезапуске.

1. Управление сетями.
2. Защита Wi-Fi сетей.
3. Управление использованием данных в мобильной широкополосной сети.

Управление сетями.

Если управляете сетью дома или на работе, следует получить полное представление о безопасности и сетевом управлении, включая знание того, кто будет использовать эту сеть.

Конечно маршрутизатор, который позволяет устанавливать многократные основные и гостевые *SSID* соединения стоит приличных денег, особенно для маленьких учреждений.

Много высокопроизводительных маршрутизаторов предлагают эту функциональность, и на рабочем месте сложно рекомендовать что-то лучшее. Такой маршрутизатор полезен и дома, особенно если использовать совместное сетевое хранение, например, подключенный к маршрутизатору диск *NAS* или жесткий *USB* диск, на котором сохранены резервные копии и частные файлы [34].

Главное всегда удостоверяться, что у маршрутизатора два пароля: один для администрирования через интерфейс и другой для *Wi-Fi*. Эти пароли должны всегда отличаться. Если есть маршрутизатор, который поддерживает многократный *SSID*, у каждого должен быть его собственный *уникальный пароль*[44].

Подсказка: Чтобы создать безопасный пароль, удостоверьтесь, что он состоит по крайней мере из 12 символов и включает смесь прописных и строчных букв, чисел, и символов. Можно также использовать некоторые числа и символы, чтобы заменить ими буквы, например, "*5*" вместо "*Д*", "*1*" вместо "*А*" и так далее.

Защита Wi-Fi сетей.

При создании своей *Wi-Fi* сети, может встать вопрос - какой использовать тип безопасности. Можно выбрать WEP, *WPA-Personal, WPA2-Personal, WPA-Enterprise* или *WPA2-Enterprise*. Поскольку все они - комбинация букв и чисел, хорошо бы узнать, что действительно каждый

[44] *В.И. Завгородний. Комплексная защита информации в компьютерных системах. Москва. Логос-2001*

означает. Есть искушение выбрать основной тип шифрования, такой как *WEP*, потому что он позволяет использование коротких легко запоминающихся паролей. Но короткий пароль небезопасен. Чем выше уровень шифрования, тем более сложные требования к паролю по умолчанию.

Надо сказать, что *WEP, WPA*, и *WPA2* далеко не безопасны, особенно в деловом пространстве, и вполне по зубам опытным и решительным хакерам. Хотя, если маршрутизатор не предлагает дополнительные опции безопасности, например, шифрование *AES* или сервер аутентификации *RADIUS* – никак полностью не защититься.

Каждый новый добавленный к сети *Wi-Fi* тип безопасного шифрования и аутентификации делает пароль длиннее с более строгими требованиями. Самый простой вводится в компьютер только однажды; но более сложный требует постоянного ввода [34].

Большинство энтузиастов и специалистов по ИТ, имеют в своих сетях те же самые типы файлов, что и любой потребитель, но в них есть и деловые файлы. Однако только если в сети имеются особенно важные данные *(например, работаете в наукоемкой отрасли или для правительственного учреждения) – это вероятная цель для хакера*. Хотя прошлые годы показали, что хищение правительственных данных, намного более вероятно изнутри чем снаружи.

Для домашних пользователей рекомендуется *WPA2* шифрование. Минимальная длина пароля в нем чуть длиннее легкой для запоминания, но профессионалы по безопасности всегда рекомендуют иметь длинные пароли. Да и никто ведь не мешает записать свой пароль на бумажке, маловероятно, что кто-то физически ворвется к вам в здание, чтобы получить доступ к *Wi-Fi* сети. А *WEP* и *WPA* просто не дают достаточной безопасности.

Управление использованием данных в мобильной широкополосной сети.

Windows 8.1 может помочь контролировать и ограничивать используемый объем данных, показывая его в сетевой панели соединений. Когда происходит соединение с мобильной широкополосной сетью, Windows

показывает до сих пор использованный объем данных. На ежемесячном контракте с установленным объемом данных, счетчик можно сбрасывать каждый месяц, щелкая по *Reset*.

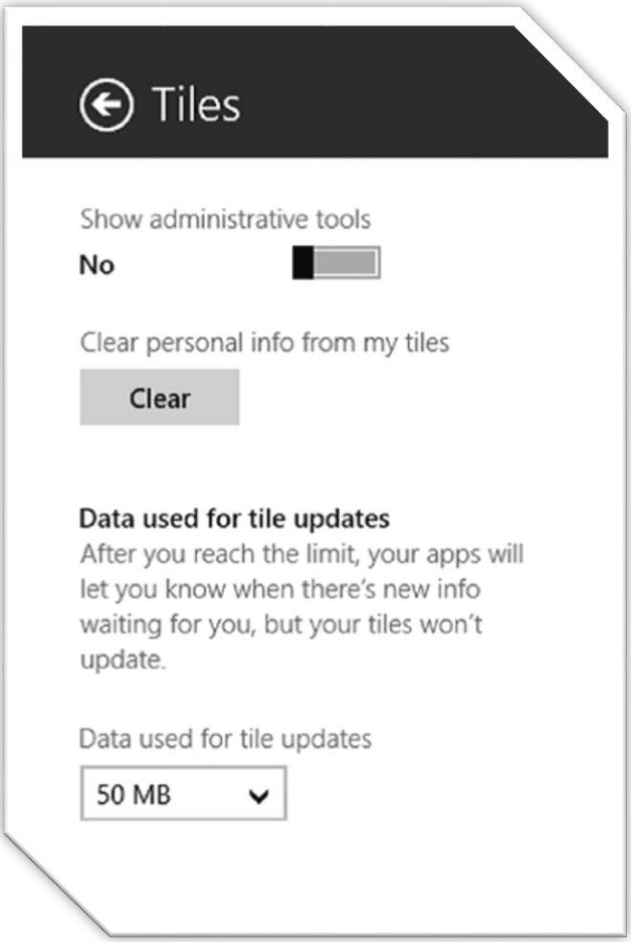
Однако потребуется включить эту функцию для каждой сети *(также можно сделать и для Wi-Fi сетей)*:

1. Открыть Настройки ПК.
2. Щелкнуть по настройкам *Network (сети)*.
3. Щелкнуть по названию сети, для которой нужно, чтоб отображалось использование данных.

В разделе *Data Usage (использование данных)*, переключите переключатель под "Отображать мое использование данных в списке сетей" и, дополнительно, можно отметить чтоб Windows 8.1 обрабатывал эту сеть как измеряемое соединение. Эта установка препятствует отправлению и получению Windows и приложениями слишком большого объема данных, что спасает от чрезмерных затрат по трафику.

Подсказка: Здесь для мобильных широкополосных сетей имеется опция, защищающая информационное соединение *ПИН-кодом*. Ее можно использовать для предотвращения несанкционированного использования сети. Живые плитки на стартовом экране Windows 8.1 выводят новые данные каждый раз при их обновлении автоматически. Однако можно ограничить используемый объем данных, для этого [34]:

1. Со стартового экрана, откройте "Настройки" *(Win+I с клавиатуры)*.
2. В верхнем правом углу экрана, щелкните по *Tiles (плитки)*. Если открыть "Настройки" с рабочего стола, эта опция не появляется.



(рис. 3.12.2). Плитка

Окно плиток позволяет определять максимальный объем данных, который живые плитки могут использовать в течении месяца. Как только этот предел достигнут, живые плитки по мобильному широкополосному соединению больше обновляться не будут.

Вопросы для самоконтроля

1. Расскажите об управлении сетевыми подключениями.
2. Как происходит управление сетями?
3. Что включает в себя защита Wi-Fi сетей?
4. Управление использованием данных в мобильной широкополосной сети включает в себя...
5. Что является лучшей гарантией превосходной безопасности в сети?

6. Какие действия можно выполнить в панели "Изменение параметров адаптера"?

13-§. Телекоммуникации

Ключевые слова: *телекоммуникации, отрасли телекоммуникаций, некриптографические средства защиты информации, стеганография, стеганографический метод защиты информации.*

Термин телекоммуникации состоит из двух слов: теле *(в переводе с греческого означает – "далеко")* и коммуникация *(в переводе с латыни – "сообщение, связь")* и означает *"дальняя связь"* или *"связь, сообщение на расстоянии"*.

Телекоммуникации - это любые формы связи, способы передачи информации на большие расстояния[45].

Телекоммуникации - это также процессы передачи, получения и обработки информации на расстоянии с применением электронных, электромагнитных, сетевых, компьютерных и информационных технологий.

Знания и умения специалиста по телекоммуникационным технологиям примерно наполовину - это информационные технологии *(программирование, настройка, конфигурирование, использование телекоммуникационных систем, оборудования, протоколов связи)* и наполовину - знание принципов работы, умение проектировать телекоммуникационное оборудование, устройства и системы[46].

Основными отраслями телекоммуникаций на сегодняшний день являются: Интернет, мобильная связь, сети передачи данных *(беспроводные,*

[45] *Проскурин Г.В. Криптография. Методы защиты информации в телекоммуникационных сетях //Connect! Мир связи. -1999. - №6-С.124-126.*

[46] *В.И. Завгородний. Комплексная защита информации в компьютерных системах. Москва. Логос-2001*

оптоволоконные и т.д.), спутниковые системы связи, цифровое и аналоговое телевидение, телефонная связь, электронный банкинг.

(рис. 3.13.1). Диаграмма телекоммуникации

Направление телекоммуникации

- Компьютеры, операционные системы, сети
- Программирование *(C/C++, Matlab, Simulink)*
- Веб-программирование *(PHP, Java, Java Script, HTML+CSS, MySQL, Joomla)*
- Интернет-технологии *(телекоммуникационное оборудование, протоколы, выбор, конфигурирование, настройка, сопровождение)*
- Радиосвязь
- Оптоволоконная связь, проводная связь
- Цифровое и аналоговое телевидение
- Мобильная связь, мобильные телефоны
- Спутниковая связь
- Системы глобального позиционирования
- IP-телефония
- Локальные и глобальные сети
- Электронный банкинг, электронная коммерция
- Защита информации в телекоммуникационных системах

"*Телекоммуникации*" является вершиной эволюции радиоэлектронных и компьютерных специальностей, самой последней и современной из них, наиболее сбалансированной по получаемым знаниям и практическим навыкам, самой востребованной, высокооплачиваемой и дефицитной на рынке труда из всех технических специальностей, по которым осуществляется обучение в вузах [34].

Проблема защиты информации в современных *телекоммуникационных* и *компьютерных сетях* общего пользования в настоящее время является весьма актуальной. Профессиональные исследования в этой области, направленные на обеспечение безопасности информации, проводятся в основном применительно к системам штабного или офисного типа. Методы информационной защиты индивидуального пользователя сети Интернет до последнего времени активно не развивались. До настоящего времени четко не сформулированы эффективные методические подходы к решению задачи гарантированной Конституцией защиты персональной информации и тайны переписки при использовании частным владельцем компьютера современных общедоступных инфокоммуникационных технологий.

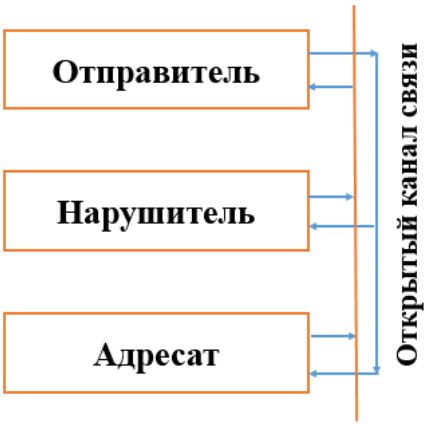
Постановка задачи защиты информации применительно к индивидуальному пользователю коммуникационными сетями общего пользования формулируется следующим образом.

В сфере современных информационных технологий можно выделить три типа субъектов *(заинтересованных сторон)*: *отправитель, адресат, нарушитель (похититель информации)*.

Отправитель - субъект, который владеет конфиденциальной информацией и желает передать её адресату без течки.

Адресат - субъект, которому отправитель передаёт информацию.

Похититель - субъект, стремящийся получить конфиденциальную информацию вопреки действиям отправителя *(рис.3.13.2)*.



(рис.3.13.2.) Обмен информацией в открытой сети

Все стороны способны свободно передавать и принимать информацию через открытый канал связи, в частности через сеть *Internet*. Перед отправителем стоит *цель* - защитить своё сообщение от любых возможных способов перехвата. Рассмотрим практически реализуемые способы достижения поставленной цели и проведем их анализ с точек зрения эффективности и простоты пользования [34].

Возможности криптографических методов защиты информации Основной метод защиты информации в казанной ситуации– криптография *(от греч. «крипто» - тайна и γράφω - «пищу»).* Используемый метод – представление данных в форме, недоступной для понимания злоумышленника.

Криптография – это раздел математики, занимающийся изучением методов преобразования информации и обеспечивающий её конфиденциальность, и аутентичность. Любой криптографический алгоритм *(крипто алгоритм)* требует наличия секретной последовательности - ключа, известной отправителю и адресату, но неизвестной злоумышленнику. Из данного выше определения следует, что криптография решает более широкий круг задач, чем защита данных. Применение методов крипто графии позволяет выявлять и предотвращать следующие виды нарушений при передаче конфиденциальной информации:

- отказ *(отправитель заявляет, что он не посылал сообщение адресату, хотя на самом деле он его все-таки посылал)*;
- модификация *(адресат изменяет сообщение и утверждает, что данное (измененное) сообщение послал ему отправитель)*;
- подделка *(адресат формирует сообщение и утверждает, что данное (измененное) сообщение послал ему отправитель)*;
- активный перехват *(злоумышленник перехватывает сообщения между отправителем и адресатом с целью их скрытой модификации)*;
- маскировка *(злоумышленник посылает адресату сообщение от имени отправителя)*.

Для борьбы с вышеперечисленными действиями сторон информационного обмена наряду с криптографией используются методы цифровых сигнатур, имитовставок и цифровых подписей.

Отправной точкой современной криптографии является работа Клода Шеннона «*Теория связи в секретных системах*», в которой были сформулированы теоретические принципы криптографической защиты. В 70-х гг. для реализации крипто алгоритмов стали применять ЭВМ. В связи с этим, началась активная разработка специализированных компьютерных алгоритмов шифрования. Одним из первых появился американский стандарт шифрования *DES (1978 г.)*. На основе используемой в DES блочной модели разработаны лучшие современные алгоритмы включая ASE и отечественные стандарты шифрования. В наши дни криптография используется не только государственными структурами и корпорациями, но и простыми пользователями ПК. Шифрование используется в некоторых сетевых протоколах. Криптографию используют для защиты информации Internet браузеры. Возможность криптографической защиты файлов предусмотрена во многих программах продуктах *(WinRar, MS Word)* [34].

Современные крипто алгоритмы могут быть реализованы как аппаратно, так и программно. На практике наибольший интерес представляет

программная их реализация. Независимо от метода реализации к любой криптографической системе предъявляются следующие требования:

- знание алгоритма не должно снижать стойкости шифра;
- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- шифр должен оставаться стойким даже при попадании к злоумышленнику большого количества исходных данных и соответствующих им зашифрованных данных;
- число операций, необходимых для дешифрования информации путём перебора всех возможных ключей, должно иметь строгую математическую оценку;
- незначительное изменение ключа или исходного текста должно приводить к существенному изменению зашифрованного текста;
- длина зашифрованного текста должна равняться длине исходного текста.

Приведённый список требований не является полным. Он лишь даёт представления о свойствах криптографической защиты и её эффективности.

Учитывая всё вышесказанное, можно сделать вывод, что грамотно построенная криптосистема обеспечивает идеальную защиту информации *(любой пользователь может быть спокоен за свои данные, отправляя их через Internet)*. Но это далеко не так на практике.

Брюс Шнайер - один из ведущих специалистов в области защиты информации утверждает, что криптография сама по себе лишь математическая абстракция. В отрыве от реальных условий она не способна обеспечить высокий уровень безопасности. Автор предлагает рассматривать криптографию не саму по себе, а в контексте её применения. С этой целью разрабатываются методы выбора крипто алгоритма и длины ключа применительно к конкретным условиям, гибкого сравнения качества защиты для разных алгоритмов.

Несмотря на высокую эффективность, криптографические методы находят ограниченное применение не только в индивидуальной пользовательской практике, но даже и в офисных условиях, поскольку они требуют организации специализированной инфраструктуры для их внедрения и поддержания в состоянии работоспособности.

Некриптографические методы защиты информации в телекоммуникационных сетях.

Рассмотрим возможности не криптографических методов защиты информации в сетях общего пользования. Они основаны на применении альтернативных не криптографических средств защиты[47].

Хорошо известны и широко используются в современных телекоммуникационных сетях следующие методы защиты информации [34]:

1. Ограничение физического доступа к каналу передачи;
2. Маскирование передаваемых данных.

Первый метод эффективен для защиты локальных сетей, размещающихся на ограниченном пространстве. Злоумышленник не имеет возможности получить доступ к линии передачи данных. В идеальном случае ему неизвестны даже используемое оборудование и топология сети. Подобная защита полностью ликвидирует грозу течки информации. Однако при переходе на глобальный уровень данный метод становится неприемлемым. Любой человек может стать полноправным пользователем глобальной сети и получить свободный доступ к потокам информации, циркулирующим в ней.

Второй метод часто применяется в радиотехнике. Метод универсален для всех линий передачи, обладающих значительным уровнем собственных шумов. Яркий пример: воздушные радиоканалы. В качестве защитного фонового сигнала выступает белый шум природного происхождения. В компьютерных сетях зашумление часто применяют для пресечения

---

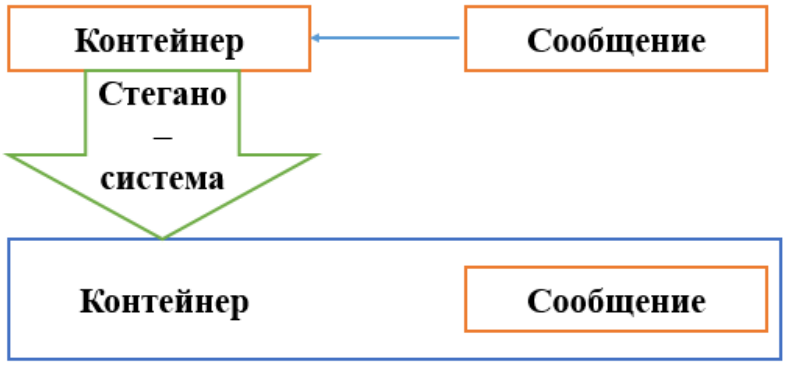
[47] *В.И. Завгородний. Комплексная защита информации в компьютерных системах. Москва. Логос-2001*

электромагнитных течек, несущих информационный сигнал. К глобальным компьютерным сетям такой метод неприменим, поскольку злоумышленник получает доступ к тому же потоку, что и адресат. Метод зашумления сигнальной информации в открытых каналах связи также не может найти широкого применения в индивидуальной пользовательской практике, поскольку он ориентирован на применение достаточно сложной и дорогостоящей специальной аппаратуры.

Более подходящим с практической точки зрения для защиты цифровой информации в пользовательских сетях является третий из указанных выше способов *(способ маскирования данных путем стеганографии)*.

Стеганографический метод защиты информации

Наука, разрабатывающая методы маскирование данных, называется стеганография *(от греч. στεγανός— «скрытый» и γράφω— «пишу», буквально «скрытнопись»)*. Используемый стеганографией метод - скрытие сообщений в больших массивах информации *(контейнерах, рис.3.13.3)*. Теоретически, контейнером может являться любой файл или поток, имеющий подходящий размер.



(рис.3.13.3). Принцип стеганографии

Стеганографические методы защиты информации - это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

Существуют разработки, позволяющие, помимо скрытия информации, решать следующие задачи с помощью стеганографии:

- защита от копирования;

- скрытая аннотация документа;
- аутентификация *(цифровые водяные знаки)*.

Как и криптография, стеганография имеет глубокие корни. По некоторым данным, «скрытнописью» пользовались древние шумеры.

В ранние годы использования цифровой техники стеганография не получила широкого распространения. Главная причина её непопулярности в тот период - неизбежный рост объёма передаваемой информации *(возможно на порядок)*. Нишу по защите компьютерной информации заняла криптография. Стеганография в этот период ходит в тень. Но она не прекратила развиваться. Однако общая теория стеганографии по-прежнему остаётся непроработанной. До недавнего времени передача сообщений с использованием стеганографической защиты была ограничена возможностями систем передачи информации. Однако сейчас в связи с бурным развитием сети Internet отпала необходимость жёсткого контроля размеров потока. Затраты энергии на передачу больших массивов информации пренебрежимо малы. Таким образом, главный недостаток стеганографии больше не является определяющим фактором. В связи с этим следует обратить внимание на её преимущества [34]:

- скрытие самого факта передачи;
- возможность применения защиты от искажений;
- возможность предварительного использования криптографии.

Современная стеганография развивается в рамках компьютерных систем. Наиболее распространены два подхода к реализации стеганографических алгоритмов. Первый *(компьютерная стеганография)* основан на использовании особенностей операционной системы: зарезервированные поля файловой системы или неиспользуемые области в файлах наиболее распространённых форматов. При передаче по сетям общего пользования секретные данные можно встроить в заголовки IP-пакетов. Несомненным достоинством данных методов является их естественность.

Выбранный файл или дисковое пространство сами по себе являются контейнерами.

Дополнительных математических алгоритмов обработки не требуется. Недостатками являются низкая вместимость контейнеров и низкая стойкость *(для вскрытия достаточно знать лишь факт использования алгоритмов)*. По указанным причинам область применения подобных методов ограничена и широкого их распространения ожидать не приходится.

Второй подход *(цифровая стеганография)* основан на встраивании секретных данных непосредственно в информационную область контейнера, что вызывает при этом некоторое искажение информации контейнера. Как правило, в качестве контейнеров используется мультимедийные файлы *(изображения, аудио, видео)*, являющиеся оцифрованными аналоговыми сигналами. Внесение небольших изменений не приводит к заметному для человеческого восприятия искажению данных.

Для цифровых методов актуальным параметром является уровень обеспечиваемой секретности. В этой связи выделяют три типа стеганосистем: теоретически устойчивые, практически устойчивые и неустойчивые. Для таких систем невозможно определить факт записи сообщения в контейнер без его сравнения с исходным незаполненным контейнером. В данной случае математические основы не будут рассматриваться, обратимся лишь к некоторым практическим деталям реализации стеганографической защиты информации в сетях общего пользования.

Рассмотрим возможность использования различных форматов данных в качестве контейнеров. Отметим, что в стеганосистеме нет никаких ограничений на использование файлов любых форматов. К ним относятся, например, текстовые, графические, аудио, видео файлы, файлы проектов систем автоматического проектирования, системные файлы. Важнейшее требование, предъявляемое к контейнеру - вместимость. Поэтому, либо сам файл должен иметь большой объём, либо их число должно компенсировать недостаток вместимости.

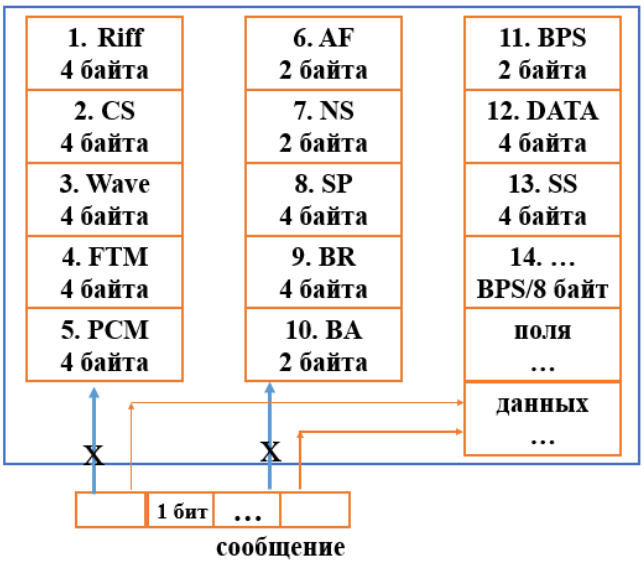
Другим существенным обстоятельством является возможность преднамеренного искажения данных в файле без обнаружения этого факта и без изменения работоспособности файла-носителя. Неработоспособность файла явно указывает на его изменение, что является косвенным указанием на использование стеганографии. Использование таких преобразований контейнера допустимо лишь для построения низкоэффективных систем защиты.

Для сохранения работоспособности файлов необходимо учитывать структуру применяемого контейнера. Данные любого файла можно разделить на две части: заголовок и область данных. Заголовок содержит метки формата, сведения о строении файла и структуре данных. Эта область жёстко или почти жёстко регламентирована. Вносить в неё изменения без потери читаемости практически невозможно. Исключения составляют зарезервированные поля форматов. Вторая часть содержит полезную информацию и может легко варьироваться в некоторых пределах без потери работоспособности [34].

Пример применения стеганоалгоритма

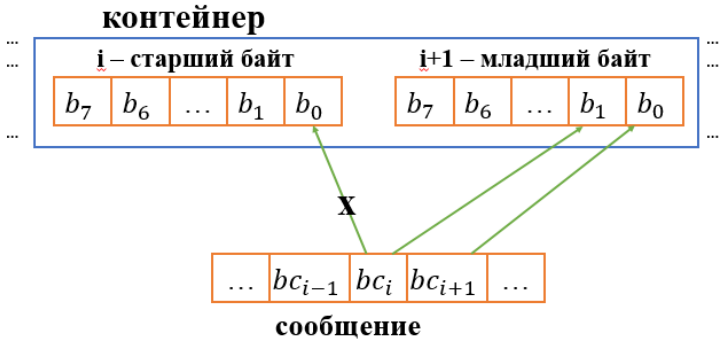
Для наглядности рассмотрим стеганосистемы, построенные на основе аудио формата wave. Wave-файл содержит последовательность дискретных отсчётов звукового сигнала. Заголовок *(обозначен толстыми линиям на рис. 3.13.4)* включает в себя строки *“RIFF” (1), “WAVE” (3), “fmt” (4)* и *“data” (12)* в коде ASCII, код формата *(6)*, частоту дискретизации *(8)*, количество бит, кодирующих *1* отсчёт *(11)*, количество байт в области данных *(13)*. Все поля жёстко регламентированы. Изменения в них не допустимы. Для преобразования остаётся доступной область данных *(14)*, в которой хранятся амплитуды отсчётов аудиозаписи[48].

[48] *В.И. Завгородний. Комплексная защита информации в компьютерных системах. Москва. Логос-2001*



(рис.3.13.4). Использование Wave-файла

Звуковые отсчёты можно преобразовать одним из стеганоалгоритмов. Простейший способ сводится к последовательному суммированию младших бит отсчетов и бит сообщения или простой заменой одного бита другим. При этом следует учитывать длину одного отсчёта *(11)*. Кроме последовательной замены младшего бита можно прибегнуть к методам псевдослучайного интервала и квантования. Следует только помнить, что на кодирование одного отсчёта отводится BPS/8 байт. Эта величина может равняться 1, 2, 4 или 8 байт *(соответственно 8, 16, 32 или 64 бит)*. Поэтому, модификация бит должна производится только в младших байтах области данных *(рис.3.13.5)*.



(рис.3.13.5). Замена младшего бита.

Надо заметить, что правило замены младших бит действует строго лишь с точки зрения визуальной оценки. Построение контейнера математическим путём может дать другие результаты. К настоящему времени широкое распространение получили сжатые форматы данных. В отличие от форматов

пространственного хранения, описанных выше, сжатые файлы содержат данные в частотной области. Для их получения используют алгоритмы компрессии. Самые популярные алгоритмы основаны на дискретных модификациях преобразования Фурье, косинусного преобразования и вейвлет-преобразования. Их применение позволяет достичь уменьшения объёма на порядок, внося лишь незначительные потери в исходную информацию. Поэтому, появился ряд специальных методов, позволяющих повысить стойкость стеганосистемы. Основная идея этих методов– использовать для встраивания сообщения в контейнер алгоритм, похожий на алгоритм компрессии.

Вопросы для самоконтроля

1. Этимология слова "телекоммуникация".
2. Что такое телекоммуникации?
3. Перечислите основные отрасли телекоммуникаций.
4. Криптография - это...
5. Расскажите о некриптографических методах защиты информации в телекоммуникационных сетях.
6. Что такое стеганография?

14-§. Сетевая безопасность

Ключевые слова: *сеть, безопасность сети, сетевая безопасность, службы безопасности сети.*

Сетевая безопасность включает политику, практические методы и технологии, позволяющие предотвращать атаки на сети и доступные сетевые ресурсы организации.

Сеть - это компонент, подверженный большому риску. Обычно сеть и определяет реальный периметр безопасности. Поэтому при попытке доступа к *ИТ-ресурсам* первым шагом злоумышленников часто является проникновение в сеть.

Сеть - группа компьютеров и других устройств *(например, принтеры и сканеры)*, взаимодействующих или с помощью беспроводной коммуникации, или с помощью физического соединения, такого как кабель Internet или телефонная линия.

Безопасность сети - это обязательное условие общей кибербезопасности, поскольку сеть является важнейшей линией защиты против атак извне[34].

Поскольку практически все данные и приложения связаны с сетью, надежная система безопасности сети гарантированно защитит от утечки данных. Однако при все более активном использовании сети, внедрении беспроводной связи и подключении устройств множества разных типов обеспечение безопасности сети становится все более сложной задачей. Чтобы ресурсы были полностью защищены, процесс обеспечения безопасности сети должен быть полностью согласован со всеми этими изменениями[49].

[49] *В.И. Завгородний. Комплексная защита информации в компьютерных системах. Москва. Логос-2001*

Сетевая безопасность - это прежде всего *защита сети* и всех подключенных к ней ресурсов от всяческих угроз. Безопасность сети включает физические и программные меры противодействия, призванные защитить инфраструктуру сети от несанкционированного доступа, некорректной работы, неправомерного использования, модификации и разрушения.

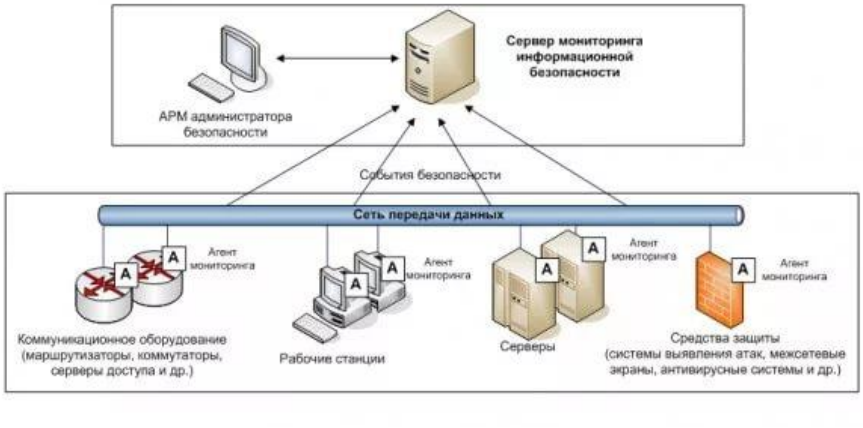
С другой стороны, сетевая безопасность - прикладная научная дисциплина, отрасль информатики. Занимается вопросами обеспечения информационной безопасности сети и её ресурсов, в частности, хранящихся в ней и передающихся по ней данных и работающих с ней пользователей. Является расширением компьютерной безопасности *(как дисциплины)* и подразделом информационной безопасности. Занимается изучением и разработкой методов и практических правил работы с сетью, в том числе протоколами связи и обмена данными и криптографическими методами защиты информации.

Среди рисков, которым подвергается компьютерная сеть и предотвращение которых является целью сетевой безопасности как дисциплины: несанкционированный доступ к сетевым ресурсам *(например, несанкционированное чтение файлов)* и предотвращение атак, целью которых является отключение тех или иных предоставляемых сетью услуг [34].

Кроме дисциплины, под термином «сетевая безопасность» может пониматься комплекс процедур, стандартов, правил и средств, призванных обеспечить безопасность сети. Среди как аппаратных, так и программных средств и устройств, для этой цели применяемых: межсетевые экраны *(файрволлы)*, антивирусные программы, средства мониторинга сети, средства обнаружения попыток несанкционированного доступа *(вторжения)*, прокси-серверы и серверы аутентификации.

Обеспечение сетевой безопасности является одно из важных аспектов деятельности.

Службы безопасности сети



(рис.3.14.1). Службы безопасности сети

Службы безопасности сети указывают направления нейтрализации возможных угроз безопасности. Службы безопасности находят свою практическую реализацию в различных механизмах безопасности. Одна и та же служба безопасности может быть реализована с использованием разных механизмов безопасности или их совокупности. Международная организация стандартизации *(МОС)* определяет следующие службы безопасности:

1. аутентификация *(подтверждение подлинности)*;
2. обеспечение целостности;
3. засекречивание данных;
4. контроль доступа;
5. защита от отказов.

Обеспечение безопасности информации в крупных *автоматизированных системах* является сложной задачей. Реальную стоимость содержащейся в таких системах информации подсчитать сложно, а безопасность информационных ресурсов трудно измерить или оценить. Объектом защиты в современных АИС выступает территориально распределенная *гетерогенная сеть* со сложной структурой, предназначенная для распределенной обработки данных, часто называемая *корпоративной сетью.* Характерной особенностью такой сети является то, что в ней функционирует оборудование самых разных производителей и поколений, а

также неоднородное программное обеспечение, не ориентированное изначально на совместную обработку данных.

Решение проблем безопасности АИС заключается в построении целостной системы защиты информации. При этом защита от физических угроз, например, доступа в помещения и утечки информации за счет ПЭМИ, не вызывает особых проблем. На практике приходится сталкиваться с рядом более общих вопросов политики безопасности, решение которых обеспечит надежное и бесперебойное функционирование информационной системы[50].

Главными этапами построения политики безопасности являются следующие [34]:

- обследование информационной системы на предмет установления ее организационной и информационной структуры и угроз безопасности информации;
- выбор и установка средств защиты;
- подготовка персонала работе со средствами защиты;
- организация обслуживания по вопросам информационной безопасности;
- создание системы периодического контроля информационной безопасности ИС.

В результате изучения структуры информационных систем *(ИС)* и технологии обработки данных в ней разрабатывается *Концепция информационной безопасности ИС*, на основе которых в дальнейшем проводятся все работы по защите информации в ИС. В концепции находят отражение следующие основные моменты:

- организация сети организации;
- существующие угрозы безопасности информации, возможности их реализации и предполагаемый ущерб от этой реализации;

---

[50] *В.И. Завгородний. Комплексная защита информации в компьютерных системах. Москва. Логос-2001*

- организация хранения информации в ИС;
- организация обработки информации *(на каких рабочих местах и с помощью какого программного обеспечения)*;
- регламентация допуска персонала к той или иной информации;
- ответственность персонала за обеспечение безопасности.

В конечном итоге на основе Концепции информационной безопасности ИС создается схема безопасности, структура которой должна удовлетворять следующим условиям:

1. защита от несанкционированного проникновения в корпоративную сеть и возможности утечки информации по каналам связи;
2. разграничение потоков информации между сегментами сети;
3. защита критичных ресурсов сети;
4. защита рабочих мест и ресурсов от несанкционированного доступа (*НСД*);
5. криптографическая защита информационных ресурсов.

В настоящее время не существует однозначного решения, аппаратного или программного, обеспечивающего выполнение одновременно всех перечисленных условий. Требования конкретного пользователя по защите информации в ИС существенно разнятся, поэтому каждая задача решается часто индивидуально с помощью тех или иных известных средств защиты. Считается нормальным, когда *10 – 15%* стоимости информации тратится на продукты, обеспечивающие безопасность функционирования сетевой информационной системы.

Некоторые зарубежные средства обеспечения информационной безопасности в сетях

Средства управления доступом	
Аутентификация *(authentication)*	Symark - Symark PowerPassword®
Авторизация	Computer Associates - eTrustIM Access Control;

(authorization)	Symark *(http://www.symark.com)* - Symark PowerBroker®.
Управление идентификацией *(identity management)*	Entegrity - AssureAccess; Entrust - GetAccess; IBM® Tivoili - Access Manager; Netegrity - Identity Minder; Novell - IChain; Novell – Nsure and Secure Access; Oblix - IDLink; OpenNetwork - nCross Platform Active Directory; RSA Security Identity Management; Secure Computing - Safe Word
Средства фильтрации	
Межсетевые экраны *(firewalls)*	CyberGuard *(http://www.cyberguaid.com)* - SL3200, KS1500; TippingPoint Technologies, Inc. - UnityOneTM Intrusion Prevention Systems & Appliances; Akonix® Systems, Inc. Akonix L7 Enterprise; Astaro Corporation - Astaro Security Linux; Check Point Software Technologies Ltd - VPN-l/FireWall-lTM Next Generation with Application Intelligence; Fortinet - FortiGate Antivirus Firewalls; NetScreen - 5000 Series; Secure Computing - Sidewinder G2 Firewall; Stonesoft, Inc. StoneGate; Zone Labs, Inc. - Zone Labs IntegrityTM
Активный контекстный мониторинг/фильтрация *(active content monitoring/filtering)*	Computer Associates *(http://www.ca.com)* - eTrustIM Secure Content Manager; NetlQ *(http://www.netiq.com)* - WebMarshal; TippingPoint Technologies, Inc. *(http://www.tippingpoint.com)* - UnityOne™ Intrusion Prevention Systems & Appliances;

	Vericept *(http://www.vericept.com)* - Vericept Intelligent Early Warning (VIEW) Monitoring Solutions; Vericept - Vericept Intelligent Early Warning (VIEW) Filter Solutions; Cerberian - Cerberian Web Manager; Fast Data Technology - FastTracker; PestPatrol, Inc. - PestPatrol; SurfControl - Total Filtering Solution; 8e6 Technologies - R3000 Internet Filter
Защита от распределенных атак "отказ в обслуживании" *(antiDDoS tools)*	Arbor Network - Peakflow; PestPatrol - PestPatrol
Защита от компьютерных червей *(anti-worm solutions)*	ForeScout Technologies *(http://www.forescout.com)* - WormScout
Защита от спама *(spam protection)*	Computer Associates - eTrustIM Secure Content Manager; Frontbridge Technologies - TrueProtect™ Message Management System; NetlQ - MailMarshal; Sunbelt Software (http://www.sunbeltsoftware.com) - iHateSpam™ Server Edition; Sunbelt Software - iHateSpam™ Gateway Edition; Aladdin Knowledge Systems - eSafe Advanced Anti-Spam Module; Barracuda Networks Barracuda Spam Firewall; FutureSoft DynaComm i:mail™
Средства защиты, использующие криптографические методы	

Удостоверяющий центр. *(certificate authority)*	Ubizen, Inc. *(http://www.ubizen.com)* - Ubizen OnlineGuardian® Certificate Management
Шифрование файлов и сеансов связи. *(file and session encryption)*	Absolute Software Corporation - Absolute®Encrypt; F-Secure, Inc.® - F-Secure® SSHTM; Global Technologies Group, Inc. - CompuSec - Free Encryption Software; Vormetric, Inc. - CoreGuardTM Core Security System
Виртуальные частные сети и защищенные коммуникации. *(virtual private networks and cryptographic communications)*	CyberGuard - SL3200, KS1500; V-ONE Corporation - SmartGate®; Communication Devices, Inc. - Port Authority Secure Out of Band Management
Виртуальные частные сети на основе протокола. *SSL (SSL VPNs)*	Whale Communications - e-Gap Remote Access SSL VPN; Avential - EX1500TM SSL VPN Appliance; Neoteris - SA 1000/3000/5000 Series; Aspelle - Aspelle Everywhere V.3.0; PortWise - PortWise mVPN; Seagull Software Systems – Seagull Secure FTP Pro™; Array Networks - Array SP/SP-C; Netilla Networks - Netilla® Security Platform (NSP); F5 Networks - FirePass™ Product Family; InfoExpress, Inc. - CvberArmor
Системы отражения вторжений и поиска уязвимостей	

Системное обнаружение вторжений. *(host-based intrusion detection)*	Configuresoft (http://www.configuresoft.com) – Enterprise Configuration Manager; Configuresoft - Security Update Manager; NetlQ – Security Manager; Sunbelt Software - Sunbelt Server Event Manager
Сетевое обнаружение вторжений. *(network-based intrusion detection)*	Computer Associates - eTrustIM Intrusion Detection; Lancope - StealthWatch
Сервисы безопасности: тесты на возможность проникновения. *(security services: penetration testing)*	BindView Penetration Testing *(http://www.bindview.com)*; Qualys - QualysGuard Consultant
Сетевые сканеры уязвимостей. *(network-based vulnerability scanners)*	BindView - bv-Control for Internet Security; eEye Digital Security - Retina® Network Security Scanner; Harris Corp *(http://www.harris.com)* - STAT Scanner, STAT Analyzer; Harris Corp - STAT DVM, STAT Scanner Console; Qualys – QualysGuard Enterprise; Qualys - QualysGuard Express; Sunbelt Software – Sunbelt Network Security Inspector™; Application Security, Inc. - AppDetective; Lumeta - IPsonar 2.5; nCircle Network Security - IP360 Vulnerability Management System;

	Tenable Network Security - NeWT and NeVO; Visionael® - Visionael® Security Audit™
Средства управления безопасностью сети	
Реализация ПБ организации. *(enterprise security policy implementation)*	BindView Policy Compliance Suite; Configuresoft – Enterprise Configuration Manager; Configuresoft - Security Update Manager; CyberGuard - Global Command Center, Central Management; eEye Digital. Security - eEye's Enterprise Vulnerability Assessment & Remediation Solution; TippingPoint Technologies, Inc. - UnityOne™ Intrusion Prevention Systems & Appliances; NetVision Inc. NVPolicy Resource Center.
Разработка ПБ *(policy development)*	Vericept - Vericept Professional Services
Средства администрирования безопасности организации. *(enterprise security administration)*	BindView Vulnerability Management Suite: BindView Policy Compliance Suite; Computer Associates - eTrust™ Admin; Configuresoft – Enterprise Configuration Manager; Configuresoft - Security Update Manager; CyberGuard Global Command Center; eEye Digital Security *(http://www.eeye.com)* - REMTM Remote Enterprise Management; NetIQ - Security Administration Suite; NetIQ - Group Policy Administrator; Sunbelt Software - Directory Inspector™; Sunbelt Software - LanHound™; TippingPoint Technologies, Inc. - UnityOne™ Intrusion Prevention Systems & Appliances;

	FireVue Security Systems - LogAppliance; Symmetricom - SyncServer® S100 Network Time Server; SSH Communications Security, Inc. - SSH Tectia™
Свободно распространяемые средства защиты в сетях различного назначениями.	Nessus; Snort/Snarf; Ethereal; Nmap; ActivePorts; TCPView; Logcheck; Sara; Tripwire

(табл. 3.14.1). Зарубежные средства обеспечения информационной безопасности в сетях

Вопросы для самоконтроля

1. Что такое сеть?
2. Что включает в себя безопасность сети?
3. Какие службы безопасности сети определяет Международная организация стандартизации (МОС)?
4. Что такое корпоративная сеть?
5. Каковы главные этапы построения политики безопасности?
6. Перечислите некоторые зарубежные средства обеспечения информационной безопасности в сетях.

15-§. Практическое управление безопасностью

Ключевые слова: *стандарты ISO, стандарты IEC, семейство стандартов СУИБ, системы управления ИБ, информационная безопасность*.

Сегодня безопасность цифрового пространства показывает новый путь национальной безопасности каждой страны. В соответствии с ролью информации как ценного товара в бизнесе, её защита, безусловно, необходима. Для достижения этой цели, каждой организации, в зависимости

от уровня информации, требуется разработка системы управления информационной безопасностью *(СУИБ)*, пока существует возможность, защиты своих информационных активов.

В организациях, существование которых значительно зависит от информационных технологий (*ИТ*), могут быть использованы все инструменты для защиты данных. Тем не менее, безопасность информации необходима для потребителей, партнеров по сотрудничеству, других организаций и правительства. В связи с этим, для защиты ценной информации, необходимо чтобы каждая организация стремилась к той или иной стратегии и реализации системы безопасности на её основе [30].

СУИБ является частью комплексной системы управления, основанной на оценке и анализов рисков, для разработки, реализации, администрирования, мониторинга, анализа, поддержания и повышения информационной безопасности *(ИБ)* и ее реализации, полученных из целей организации и требования, требования безопасности, используемых процедур и размерах и структуре ее организации[51].

Зарождение принципов и правил управления ИБ началось в Великобритании в 1980-х годах. В те годы Министерство торговли и промышленности Великобритании *(Department of Trade and Industry, DTI)* организовало рабочую группу для разработки свода лучших практик по обеспечению ИБ.

В 1989 году «*DTI*» опубликовало первый стандарт в этой области, который назывался *PD 0003* «*Практические правила управления ИБ*».

[51] *А.А. Гладких, В.Е. Дементьев. Базовые принципы информационной безопасности вычислительных систем./ Издательство: УлГТУ, 2009. - 168 с.*

(рис.3.15.1). Система управления информационной безопасности

В 1995 году Британский институт стандартов *(British Standards Institution, BSI)* принял национальный стандарт *BS 7799-1 «Практические правила управления ИБ»*. Она описывал 10 областей и 127 механизмов контроля, необходимых для построения *СУИБ (Information Security Management System, ISMS)*, определенных на основе лучших примеров из мировой практики. Этот стандарт и стал прародителем всех международных стандартов СУИБ. Как и любой национальный стандарт BS 7799 в период 1995-2000 годов пользовался, скажем так, умеренной популярностью только в рамках стран британского содружества.

В конце 1999 года были пересмотрены и гармонизированы с международными стандартами систем управления качеством ISO/IEC 9001 и экологией ISO/IEC 14001, а год спустя без изменений BS 7799-1 был принят в качестве международного стандарта ISO/IEC 17799:2000 «Информационные технологии *(ИТ)*. Практические правила управления ИБ». В 2002 году была обновлена и первая часть стандарта *BS 7799-1 (ISO/IEC 17799)*, и вторая часть BS 7799-2. Что же касается официальной сертификации по ISO/IEC 17799, то она изначально не была предусмотрена *(полная аналогия с BS 7799)*. Была предусмотрена только сертификация по BS 7799-2, который представлял

собой ряд обязательных требований *(не вошедших в BS 7799-1)* и в приложении перечень условно обязательных *(на усмотрение сертификатора)* наиболее важных требований BS 7799-1 *(ISO/IEC 17799)*.

25 сентября 2013 года были опубликованы новые версии стандартов ISO/IEC 27001 и 27002. С этого момента стандарты серии ISO/IEC 27k *(управление ИБ)* полностью интегрированы со стандартами серии ISO/IEC 20k *(управление ИТ-сервисами)*. Вся терминология из ISO/IEC 27001 перенесена в ISO/IEC 27000, который определяет общий терминологический аппарат для всего семейства стандартов ISO/IEC 27k.

Стандарт ISO/IEC 27000-2014

Последнее обновление стандарта ISO/IEC 27000 «ИТ. СУИБ. Общий обзор и терминология» состоялось 14 января 2014 года.

Стандарт состоит из следующих разделов:

- введение;
- сфера применения;
- термины и определения;
- системы управления ИБ;
- семейство стандартов СУИБ.

Международные стандарты системы управления представляют модель для налаживания и функционирования системы управления. Эта модель включает в себя функции, по которым эксперты достигли согласия на основании международного опыта, накопленного в этой области.

При использовании семейства стандартов СУИБ организации могут реализовывать и совершенствовать СУИБ и подготовиться к ее независимой оценке, применяемой для защиты информации, такой как финансовая информация, интеллектуальная собственность, информация о персонале, а также информация, доверенная клиентами или третьей стороной. Эти стандарты могут использоваться организацией для подготовки независимой оценки своей СУИБ, применяемой для защиты информации [30].

Семейство стандартов СУИБ

Семейство стандартов СУИБ, имеющее общее название «Information technology. Security techniques» *(Информационная технология. Методы защиты)*, предназначено для помощи организациям любого типа и размера в реализации и функционировании СУИБ и состоит из следующих международных стандартов:

- ISO/IEC 27000 СУИБ. Общий обзор и терминология;
- ISO/IEC 27001 СУИБ. Требования;
- ISO/IEC 27002 Свод правил по управлению ИБ;
- ISO/IEC 27003 Руководство по реализации СУИБ;
- ISO/IEC 27004 УИБ. Измерения;
- ISO/IEC 27005 Управление рисками ИБ;
- ISO/IEC 27006 Требования для органов, обеспечивающих аудит и сертификацию СУИБ;
- ISO/IEC 27007 Руководство по проведению аудита СУИБ;
- ISO/IEC TR 27008 Руководство по аудиту механизмов контроля ИБ;
- ISO/IEC 27010 УИБ для межсекторных и межорганизационных коммуникаций;
- ISO/IEC 27011 Руководство по УИБ для телекоммуникационных организаций на основе ISO/IEC 27002;
- ISO/IEC 27013 Руководство по интегрированной реализации стандартов ISO/IEC 27001 и ISO/IEC 20000-1;
- ISO/IEC 27014 Управление ИБ высшим руководством;
- ISO/IEC TR 27015 Руководство по УИБ для финансовых сервисов;
- ISO/IEC TR 27016 УИБ. Организационная экономика;
- ISO/IEC 27035 Управление инцидентами ИБ *(в стандарте не указан)*.

Международный стандарт, не имеющие этого общего названия:

- ISO 27799 Информатика в здравоохранении. УИБ по стандарту ISO/IEC 27002.

Цель стандарта

Стандарт предоставляет обзор СУИБ и определяет соответствующие условия.

Семейство стандартов СУИБ содержит стандарты, которые:

- определяют требования к СУИБ и сертификации таких систем;
- содержат прямую поддержку, детальное руководство и разъяснение целого процесса создания, внедрения, сопровождения и улучшения СУИБ;
- включают в себя отраслевые руководящие принципы для СУИБ;
- руководят проведением оценки соответствия СУИБ.

Сфера применения

Стандарт предоставляет обзор СУИБ, а также условий и определений, широко использующихся в семействе стандартов СУИБ. Стандарт применим ко всем типам и размерам организаций *(например, коммерческие предприятия, правительственные учреждения, неприбыльные организации)*.

Термины и определения

Раздел содержит определение 89 терминов, например,

- информационная система - приложения, сервисы, ИТ активы и другие компоненты обработки информации;
- информационная безопасность *(ИБ)* - сохранение конфиденциальности, целостности и доступности информации;
- доступность - свойство быть доступным и готовым к использованию по запросу уполномоченного лица;
- конфиденциальность - свойство информации быть недоступной или закрытой для неуполномоченных лиц;
- целостность - свойство точности и полноты;
- неотказуемость - способность удостоверять наступление события или действие и их создающих субъектов;

- событие ИБ - выявленное состояние системы *(сервиса или сети)*, указывающее на возможное нарушение политики или мер ИБ, или прежде неизвестная ситуация, которая может касаться безопасности;
- инцидент ИБ - одно или несколько событий ИБ, которые со значительной степенью вероятности приводят к компрометации бизнес-операций и создают угрозы для ИБ;
- управление инцидентами ИБ - процессы обнаружения, оповещения, оценки, реагирования, рассмотрения и изучения инцидентов ИБ;
- система управления - набор взаимосвязанных элементов организации для установления политик, целей и процессов для достижения этих целей;
- мониторинг - определение статуса системы, процесса или действия;
- политика - общее намерение и направление, официально выраженное руководством;
- риск - эффект неопределенности в целях;
- угроза - возможная причина нежелательного инцидента, который может нанести ущерб;
- уязвимость - недостаток актива или меры защиты, которое может быть использовано одной или несколькими угрозами.

Системы управления ИБ

Раздел «СУИБ» состоит из следующих основных пунктов:

- описание СУИБ;
- внедрение, контроль, сопровождение и улучшение СУИБ;
- преимущества внедрения стандартов семейства СУИБ.

Описание СУИБ

Описание СУИБ предусматривает следующие составляющие:

- положения и принципы;
- информация;
- информационная безопасность;

- управление;
- система управления;
- процессный подход;
- важность СУИБ.

Информация

Информация - это актив, который наряду с другими важными бизнес-активами важен для бизнеса организации и, следовательно, должен быть соответственно защищен. Информация может храниться в различных формах, включая такие как цифровая форма *(например, файлы с данными, сохраненные на электронных или оптических носителях)*, материальная форма *(например, на бумаге)*, а также в нематериальном виде в форме знаний сотрудников [30].

Информация может быть передана различными способами, включая курьера, электронную или голосовую коммуникацию. Независимо от того, в какой форме представлена информация и каким способом передается, она должна быть должным образом защищена[52].

Во многих организациях информация зависит от информационной и коммуникационной технологии. Эта технология является существенным элементом в любой организации и облегчает создание, обработку, хранение, передачу, защиту и уничтожение информации.

Информационная безопасность

Информационная безопасность включает в себя три основных измерения *(свойства)*: конфиденциальность, доступность и целостность. ИБ предусматривает применение и управление соответствующими мерами безопасности, которые включают в себя рассмотрение широкого диапазона угроз, с целью обеспечения длительного успеха и непрерывности бизнеса и минимизации влияний инцидентов ИБ.

---

[52] *А.А. Гладких, В.Е. Дементьев. Базовые принципы информационной безопасности вычислительных систем./ Издательство: УлГТУ, 2009. - 168 с.*

ИБ достигается применением соответствующего набора мер защиты, определенного с помощью процесса управления рисками и управляемого с использованием СУИБ, включая политики, процессы, процедуры, организационные структуры, программные и аппаратные средства, чтобы защитить идентифицированные информационные активы.

Эти меры защиты должны быть определены, реализованы, проконтролированы, проверены и при необходимости улучшены, чтобы гарантировать, что уровень ИБ соответствует бизнес-целям организации. Соответствующие меры и средства ИБ следует органично интегрировать в бизнес-процессы организации [30].

Управление

Управление включает в себя действия по руководству, контролю и непрерывному совершенствованию организации в рамках соответствующих структур. Управленческая деятельность включает в себя действия, методы или практику формирования, обработки, направления, наблюдения и контроля ресурсов. Величина управленческой структуры может варьироваться от одного человека в небольших организациях до управленческой иерархии в крупных организациях, состоящих из многих людей.

Относительно СУИБ управление включает в себя наблюдение и выработку решений, необходимых для достижения бизнес-целей посредством защиты информационных активов. Управление ИБ выражается через формулирование и использование политик ИБ, процедур и рекомендаций, которые затем применяются повсеместно в организации всеми лицами, связанными с ней.

Система управления

Система управления использует совокупность ресурсов для достижения целей организации. Система управления организации включает в себя структуру, политики, планирование, обязательства, методы, процедуры, процессы и ресурсы.

В части ИБ система управления позволяет организации:

- удовлетворять требования безопасности клиентов и других заинтересованных лиц;
- улучшать планы и деятельность организации;
- соответствовать целям ИБ организации;
- выполнять нормативы, законодательство и отраслевые приказы;
- организованно управлять информационными активами для содействия постоянному улучшению и коррекции текущих целей организации.

Модель «PDCA» для СУИБ

Планирование – Реализация – Контроль - Улучшение

1. *Планирование (разработка и проектирование)*: установление целей, политик, элементов управления, процессов и процедур СУИБ для достижения результатов, соответствующих общей политике и целям организации.
2. *Реализация (внедрение и обеспечение функционирования)*: внедрение и применение политик ИБ, элементов управления, процессов и процедур СУИБ по оценке и обработке рисков и инцидентов ИБ.
3. *Контроль (мониторинг и анализ функционирования)*: оценка результативности выполнения требований политик, целей ИБ и эффективности функционирования СУИБ и оповещение высшего руководства о результатах.
4. *Улучшение (сопровождение и усовершенствование)*: проведение корректирующих и предупреждающих действий, основанных на результатах аудита и анализа со стороны руководства для достижения улучшения СУИБ.

Важность СУИБ

Организации следует определить риски, связанные с информационными активами. Достижение ИБ требует управления риском и охватывает риски физические, человеческие и технологические, относящиеся к угрозам, касающимся всех форм информации внутри организации или используемой организацией.

Принятие СУИБ является стратегическим решением для организации, и необходимо, чтобы это решение постоянно интегрировалось, оценивалось и обновлялось в соответствии с потребностями организации [30].

Внедрение, контроль, сопровождение и улучшение СУИБ

Внедрение, контроль, сопровождение и улучшение СУИБ являются оперативными этапами развития СУИБ.

Оперативные этапы СУИБ определяют следующие составляющие:

- общие положения;
- требования ИБ;
- решающие факторы успеха СУИБ.

Оперативные этапы СУИБ обеспечивают следующие мероприятия:

- оценка рисков ИБ;
- обработка рисков ИБ;
- выбор и внедрение мер защиты;
- контроль и сопровождение СУИБ;
- постоянное улучшение.

Сертификация СУИБ

Для подтверждения соответствия существующей в организации СУИБ требованиям стандарта, а также ее адекватности существующим бизнес рискам необходима процедура добровольной сертификации. Хотя без этого можно и обойтись, в большинстве случаев сертификация полностью оправдывает вложенные средства и время.

Требования к СУИБ *(стандарт ISO/IEC 27001:2013)*

В 1998 году появилась вторая часть британского национального стандарта – BS 7799-2 «СУИБ. Спецификация и руководство по применению», в 2002 году она была пересмотрена, а в конце 2005 года была принята в качестве международного стандарта ISO/IEC 27001 «ИТ. Методы защиты. СУИБ. Требования». 25 сентября 2013 года состоялось последнее обновление стандарта.

Стандарт состоит из следующих разделов:

Предисловие

Введение

1. Сфера применения
2. Нормативные ссылки
3. Термины и определения
4. Контекст организации
5. Лидерство
6. Планирование
7. Поддержка
8. Эксплуатация
9. Оценка результативности
10. Улучшение

Этапам модели «PDCA» соответствуют следующие разделы стандарта:

- планирование;
- эксплуатация;
- оценка результативности;
- улучшение.

Стандарт был подготовлен для реализации требований по созданию, внедрению, сопровождению и постоянному улучшению СУИБ. Принятие СУИБ является стратегическим решением для организации. Разработка и внедрение СУИБ организации зависит от потребностей и целей организации, требований по безопасности, существующих процессов организации, размера и структуры организации. Все эти факторы влияния, как известно, со временем меняются [30].

СУИБ обеспечивает конфиденциальность, целостность и доступность информации за счет применения процесса управления рисками и придает уверенность заинтересованным сторонам в том, что риски адекватно управляются.

Свод правил управления ИБ *(стандарт ISO/IEC 27002:2013)*

В 2000 году первая часть британского национального стандарта BS 7799-1 «Практические правила управления ИБ» была принята в качестве международного стандарта ISO/IEC 17799 «ИТ. Практические правила управления ИБ». В 2005 году на его основе был разработан новый международный стандарт ISO/IEC 27002 «ИТ.

Методы защиты. Свод норм и правил управления ИБ», который был опубликован в июле 2007 года. Последнее обновление стандарта состоялось 25 сентября 2013 года. Стандарт предлагает рекомендации и основные принципы введения, реализации, поддержки и улучшения СУИБ в организации. Он может служить практическим руководством по разработке стандартов безопасности организации, для эффективной практики УИБ организаций и способствует укреплению доверия в отношениях между организациями.

Стандарт состоит из 14 разделов, посвященных мерам безопасности, которые все вместе содержат, в целом, 34 основные категории безопасности и 114 мер защиты:

1. политика ИБ;
2. организация ИБ;
3. безопасность, связанная с персоналом;
4. управление активами;
5. управление доступом;
6. криптография;
7. физическая и экологическая безопасность;
8. безопасность операций;
9. безопасность связи;
10. приобретение, разработка и поддержка ИС;
11. взаимоотношения с поставщиками;
12. управление инцидентами ИБ;
13. аспекты ИБ при управлении непрерывностью бизнеса;
14. соответствие требованиям.

Каждая основная категория безопасности включает в себя:

- цель ИБ;
- меры достижения этой цели.

Описание мер ИБ структурируется таким образом:

- меры и средства ИБ;
- рекомендации по их реализации.

Политика ИБ

Руководящие положения для ИБ

Цель: Реализовать требования политики ИБ и обеспечить поддержку для ИБ в соответствии с требованиями бизнеса и действующим законодательством.

Политика ИБ предполагает следующие мероприятия [30]*:*

- документирование;
- пересмотр.

Документирование

Меры и средства

Политика ИБ документируется оформлением, утверждением, опубликованием и доведением до персонала и внешних заинтересованных сторон.

Рекомендации по реализации

В лучшем случае, политика ИБ должна устанавливать ответственность руководства, а также излагать подход организации к УИБ.

Политика ИБ должна содержать требования:

- стратегии бизнеса;
- законодательства и договорных обязательств;
- защиты от существующих и потенциальных угроз ИБ.

Политика ИБ должна содержать положения по:

- определению ИБ, ее целей и принципов для руководства действиями по обеспечению ИБ;

- определению ответственности разных ролей с учетом специфики управления ИБ;
- изложения намерений руководства, поддерживающих цели и принципы ИБ в соответствии со стратегией и целями бизнеса;
- процессов управления изменениями и исключениями.

В худшем случае, политика ИБ должна поддерживаться специализированными политиками, направленными на внедрение управления ИБ и созданными специально для целевых групп внутри организации или выполнения конкретных задач[53].

Организация ИБ

Организацию ИБ определяют следующие составляющие:

- внутренняя организация;
- мобильные устройства и удалённая работа.

Внутренняя организация

Цель: Создать структуру управления для инициирования и управления внедрением и обеспечением ИБ в организации.

Внутренняя организация сферы ИБ предполагает следующие мероприятия:

- определение ответственности;
- разделение обязанностей;
- контакт с властями;
- контакт со специальными группами.

Определение ответственности

Меры и средства

Все ответственности в поле ИБ должны быть определены и закреплены.

Рекомендации по реализации

[53] *А.А. Гладких, В.Е. Дементьев. Базовые принципы информационной безопасности вычислительных систем./ Издательство: УлГТУ, 2009. - 168 с.*

Закрепление ответственности должно соответствовать политике ИБ. Ответственности за защиту индивидуальных активов и осуществления процессов ИБ должны быть определены.

Ответственности за действия по управлению рисками ИБ и, в частности, принятие остаточного риска должны быть определены. Эти ответственности должны быть дополнительно детализированы, при необходимости, для специфических мест и средств обработки информации.

Ответственные лица могут делегировать некоторые задачи безопасности другим. Впрочем, они все равно несут за это ответственность, поэтому должны обеспечить правильное оформление такого делегирования.

Сферы ответственности должны быть зафиксированы.

В частности, необходимо учесть следующее [30]*:*

- активы и процессы ИБ должны быть идентифицированы и определены;
- личная ответственность за каждый актив и процесс ИБ должна быть обозначена и ее детали задокументированы;
- уровни авторизации должны быть определены и задокументированы;
- назначенные быть ответственными в сфере ИБ должны быть компетентными и в курсе всех событий в этой сфере;
- координация и контроль аспектов ИБ взаимоотношений с поставщиками должны быть идентифицированы и задокументированы.

Многие организации назначают отдельного менеджера по ИБ, возлагая на него всю ответственность за разработку и внедрение ИБ и поддержку актуальности мер и средств ИБ. Одной из распространенных практик является назначение владельца каждого актива, отвечающего за его безопасность.

Управление доступом

Управление доступом определяют следующие составляющие:

- правила разграничения доступа;

- управление доступом пользователей;
- ответственность пользователя;
- управление доступом к системе и приложениям.

Требования разграничения доступа

Цель: Ограничить доступ к информации и средствам обработки информации.

Требования по управлению доступом определяют следующие составляющие:

- правила разграничения доступа;
- доступ к сетям и сетевым сервисам.

Правила разграничения доступа

Меры и средства

Правила разграничения доступа должны быть разработаны, задокументированы и пересматриваться на основе требований ИБ и бизнеса.

Рекомендации по реализации

Владельцы активов должны определить надлежащие правила разграничения доступа, права доступа и ограничения для определенных пользовательских ролей по отношению к их активам с детализацией и строгостью разграничений, отражающих соответствующие риски ИБ.

Разграничения доступа являются как логическими, так и физическими, и должны рассматриваться вместе. Пользователи и провайдеры услуг должны четко обозначить требования бизнеса, которые должны удовлетворить разграничения доступа.

Правила должны учесть следующее:

- требования к безопасности прикладных программ бизнеса;
- политики распространения информации и авторизации, например, общепризнанные принципы и уровни ИБ и классификацию информации;
- согласованность между правами доступом и политиками классификации информации систем и сетей;
- требования законодательства и договорные обязательства по ограничению доступа к данным или услугам;

- управление правами доступа в распределенных и сетевых средах, которые распознают все типы возможных соединений;
- разделение ролей разграничения доступа, например, запрос доступа, авторизация доступа, администрирование доступа;
- требования к формальной авторизации прав доступа;
- требования к периодическому пересмотру управления доступом;
- аннулирование прав доступа;
- архивирование записей всех серьезных событий по использованию и управлению удостоверениями пользователей и секретной информацией аутентификации;
- роли привилегированного доступа.

При разработке правил разграничения доступа необходимо учесть следующее:

- установление правил на основании предпосылки «Запрещено все, что не разрешено» вместо «Разрешено все, что не запрещено»;
- изменения информационных меток, инициированные автоматически средствами обработки информации и по усмотрению пользователя;
- изменения пользовательских разрешений, инициированные автоматически ИС и администратором;
- наличие правил, требующих определенного утверждения перед введением в действие и не требующих.

Правила разграничения доступа должны поддерживаться формальными процедурами и определять ответственности.

Разграничение ролевого доступа является тем подходом, которым пользуются многие организации для связывания прав доступа с бизнес-ролями.

Два общепризнанных принципа правил разграничения доступа:

- знание: наличие доступа только к информации, необходимой для выполнения задач (*разные задачи/роли означают разную потребность знаний и, следовательно, разный профиль доступа*);
- использование: наличие доступа только к средствам обработки информации, необходимым для выполнения задачи/работы/роли (*ИТ оборудование, приложения, процедуры, кабинеты*) [30].

Доступ к сетям и сетевым сервисам

Меры и средства

Пользователям должен предоставляться доступ к сетям и сетевым сервисам, когда они имеют официальные полномочия на это.

Рекомендации по реализации

Следует сформулировать политику использования сетей и сетевых услуг.

В политике необходимо рассмотреть:

- сети и сетевые услуги, к которым разрешен доступ;
- процедуры авторизации для определения того, кому и к каким сетям и сетевым услугам разрешен доступ;
- процедуры и средства управления по защите доступа к сетевым подключениям и сетевым услугам;
- средства доступа к сетям и сетевым услугам *(например, VPN или беспроводной сети)*;
- требования пользовательской аутентификации для доступа к разным сетевым сервисам;
- мониторинг использования сетевых сервисов.

Политика использования сетевых сервисов должна быть согласована с правилами разграничения доступа организации.

Неавторизованные и незащищенные подключения к сетевым сервисам могут повлиять на всю организацию. Такой контроль очень важен для сетевых подключений к чувствительным и критичным бизнес-приложениям или к пользователям в местах повышенного риска, например, публичных или

удаленных регионах, находящихся вне зоны контроля и управления ИБ организации.

Управление доступом пользователей

Цель: Обеспечить авторизованный доступ пользователей и предотвратить неавторизованный доступ к системам и сервисам.

Управление доступом пользователей обеспечивают следующие мероприятия:

- регистрация и ее отмена;
- предоставление доступа;
- пересмотр прав доступа;
- удаление или изменение прав доступа.

Управление доступом пользователей обеспечивает также управление следующим:

- правами привилегированного доступа;
- паролями.

Регистрация и ее отмена

Меры и средства

Формальный процесс регистрации пользователя ее отмены должен быть внедрен для предоставления прав доступа.

Рекомендации по реализации

Процесс управления идентификаторами пользователя должен включать:

- использование уникальных идентификаторов пользователя, позволяющих отследить их действия и ответственность за них; использование распространенных идентификаторов должно быть разрешено только в случае оперативной или бизнес-необходимости, задокументировано и утверждено;
- немедленную деактивацию или удаление идентификаторов пользователя после его увольнения;

- периодическую идентификацию и деактивацию или удаление ненужных идентификаторов пользователя;
- гарантию того, что деактивированные идентификаторы не достались другим пользователям.

Разрешение или запрет доступа к информации и средствам ее обработки состоит из следующих двух этапов:

- создание и активация или деактивация идентификатора пользователя;
- активация или деактивация прав доступа идентификатора пользователя.

Предоставление доступа

Меры и средства

Формальный процесс предоставления доступа должен быть внедрен для назначения или отмены прав доступа для всех типов пользователя во всех системах и сервисах.

Рекомендации по реализации

Процесс предоставления доступа должен включать:

- получение полномочий от собственника ИС или сервиса для их использования;
- проверку того, что уровень предоставленного доступа соответствует правилам доступа и другим требованиям, например, разделения обязанностей;
- гарантию того, что права доступа не будут активированы (*например, провайдером услуг*) до завершения процедур авторизации;
- ведение централизованной записи прав доступа, предоставленных идентификатору пользователя для доступа к ИС и сервисам.

Вопросы для самоконтроля

1. Расскажите про Стандарт ISO/IEC 27000-2014.

2. Из каких разделов состоит Стандарт ISO/IEC 27000-2014?
3. Какие свойства включает в себя информационная безопасность?
4. Модель «PDCA» для СУИБ - это...
5. Зачем необходима сертификация СУИБ?
6. Расскажите о доступе к сетям и сетевым сервисам.

ГЛАВА 4. ПРАВОВЫЕ ОСНОВЫ БЕЗОПАСНОСТИ И БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ *(ОС)*.

==========

16-§. Правовые базы для выявления информационной преступности

Ключевые слова: *информационно-коммуникационные технологии, компьютерные преступления, законы в области информационных технологий, информационная безопасность страны.*

Развитие и широкое применение информационно–коммуникационных технологий в последнее время стало глобальной тенденцией мирового прогресса. В современном динамично развивающемся мире информационно-коммуникационные технологий выполняют роль катализатора развития всей экономики, способствуют привлечению в страну инвестиций, созданию новых рабочих мест, внедрению прогрессивных технологий в производстве и управлении, то есть в конечном итоге– стабильному экономическому росту и повышению уровня жизни. В связи с этим развитие информационно-коммуникационных технологий очень важно и для нашей республики. Не случайно правительство республики в последнее время предпринимает значительные усилия по разработке и внедрению стратегии, обеспечивающей массовое внедрение и использование современных информационно-коммуникационных технологий во всех областях общественной и частной жизни.

За последние годы в Узбекистане осуществлены определенные меры для развития компьютеризации и информационно - коммуникационных технологий, а также начата реализация комплекса мер по совершенствованию обеспечения информационной безопасности. Об этом в частности, свидетельствует указы и постановления Президента Республики Узбекистан, законы Республики Узбекистан, постановления правительства, руководящие

документы *УзАСИ*, министерств и ведомств, связанные с регулированием различных аспектов в области информационных технологий.

В настоящее время принято говорить о новом витке в развитии общественной формации - информационном обществе. Информация становится сегодня главным ресурсом мирового сообщества. Практически любая деятельность человека тесно связана с получением, хранением, обработкой и использованием разнообразной информации. Современное общество широко пользуется благами компьютеризации и информатизации. Но пользователям компьютеров и компьютерных сетей следует учитывать, что компьютер может использоваться не только как мощное средство оптимизации и повышения эффективности всех видов юридической деятельности, но и как средство совершения противоправных действий и уголовных преступлений.

Шалости программистов с компьютерными вирусами – это лишь часть айсберга компьютерных преступлений. Чрезвычайно высокую опасность для общества и дополнительные проблемы для правоохранительных органов создают усиливающийся криминальный контроль над глобальными компьютерными сетями, телекоммуникациями и использование информационных технологий как для скрытого получения информации, подготовки и осуществления неправомерных действий в отношении организаций и частных лиц, так и для противодействия правоохранительным органам.

Исходя из сказанного выше, следует, что комплексное обеспечение защиты компьютерной информации, а в более широком смысле обеспечение информационной безопасности объектов и субъектов, связанных с информатизацией и использованием информации, является насущной необходимостью.

Одним из направлений защиты информационных прав и свобод государства и личности является организационно – правовая обеспечение их информационной безопасности.

Организационно-правовое обеспечение информационной безопасности представляет собою совокупность решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и создание, и функционирование систем защиты информации на конкретных объектах. Поэтому организационно-правовая база должна обеспечивать следующие основные функции:

- разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации;
- определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране и порядка регулирования деятельности предприятий и организаций в этой области;
- создание полного комплекса нормативно-правовых руководящих и методических материалов *(документов)*, регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте;
- определение мер ответственности за нарушение правил защиты;
- определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Разработка законодательной базы информационной безопасности любого государства является необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических и военных направлений развития каждого государства.

Со стороны западных стран особое внимание к формированию такой базы вызвано все возрастающими затратами на борьбу с "информационными" преступлениями. Так, ежегодные потери от компьютерной преступности в Великобритании составляют 2,5 миллиарда фунтов стерлингов, а в странах Западной Европы - 30 миллиардов евро. В отдельные годы рост потерь достигал 430%. Средний ущерб от одного компьютерного преступления в США составляет 450 тысяч долларов, а максимальный - 1 миллиард долларов.

Если 1990 году в США в общей сложности было израсходовано на защиту объектов с целью обеспечения безопасности информации примерно 14-16 миллионов долларов, то к настоящему времени эта цифра исчисляется миллиардами. И с каждым годом эта цифра увеличивается. Все это заставляет страны Запада серьезно заниматься вопросами законодательства по защите информации. Так, первый закон в этой области в США был принят в 1906 году, а к настоящему времени уже имеется более 500 законодательных актов по защите информации, ответственности за ее разглашение и компьютерные преступления.

Компьютерные преступления не обошли стороной и нашу республику. По данным Центра развития и внедрения компьютерных и информационных технологий Узбекистана, с декабря 2002 года атакам хакеров подверглись 316 сайтов, расположенных в доменной зоне uz. Последний крупный взлом произошел в конце июня текущего года, когда пострадали порядка 160 сайтов.

Республика Узбекистан с первых дней своей независимости тоже стремится к собственному организационно – правовому обеспечению информационной безопасности.

Парламентом Узбекистана к настоящему времени принято порядка 75 законодательных актов, связанных в той или иной мере с информацией, информационными услугами и информационными технологиями.

Только за последний месяц Законодательной палатой Олий Мажлиса в приняты законопроекты «Об электронных платежах», и *«О защите информации в автоматизированных банковских системах»* и направлены для одобрения в Сенат. Принятие данных законов будет способствовать переходу банковской системы на качественно новый правовой уровень, а также обеспечит защиту прав собственника информации. Депутатами Олий Мажлиса также ведется работа по подготовке проекта закона о внесении изменений и дополнений в Уголовный кодекс, уголовно – процессуальный кодекс и Кодекс об административной ответственности в части усиления ответственности за преступления в области информационных технологий.

Однако принятые законы являются только малой толикой тех нормативно – правовых документов, которые должны регулировать деятельность в области информации и информационных технологий, в том числе в области информационной безопасности.

Недостаточное совершенство нормативно - правового регулирования отношений в области реализаций возможностей конституционных прав на свободу получения и распространения информации вызывают справедливые нарекания при ограничении этих свобод в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства, что существенно затрудняет поддержания необходимого баланса интересов личности, общества и государства в информационном поле.

Исходя из вышеизложенного для улучшения правового обеспечение информационной безопасности Республики Узбекистан требуется[54]:

Внесение изменений и дополнений в законодательство Республики Узбекистан, регулирующие отношение в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности, имплементации норм, связанных с международными соглашениями, к которым присоединился Узбекистан.

Разработка и принятие нормативных актов Республики Узбекистан, устанавливающих ответственность юридических и физических лиц за несанкционированной доступ к информации, ее противоправное копирование, искажения и противозаконное использование, раскрытие конфиденциальной информации, использования в преступных и корыстных целях служебной информации или информации содержащей коммерческую тайну.

---

[54] *Закон Республики Узбекистан от 11.12.2003 г. N 560-II. Об информатизации.*

В этой связи представляется необходимым также разработка таких законодательных актов как:

- о персональных базах данных;
- о сделках, совершаемых в электронной форме;
- об информационных ресурсах,
- в которых также должны быть статьи, обеспечивающие информационную безопасность.

Деятельность по совершенствованию правового нормативного обеспечения информационной безопасности Республики Узбекистан должна осуществляться на основе соответствующих планов работы, предусматривающих анализ проблем правового регулирования отношений в рассматриваемой области, определение рациональных путей их решения, подготовку проектов нормативных правовых актов, а в необходимые случаи-правовые доктрины по конкретным направлениям этого регулирования. Проведение данных работ может осуществляться на основе соответствующих целевых программ

Осуществление вышеперечисленных мер повысит противодействие внешним и внутренним угрозам информационной безопасности Республики Узбекистан.

Вопросы для самоконтроля

1. Почему развитие информационно-коммуникационных технологий очень важно для Узбекистана?
2. Почему обеспечение защиты компьютерной информации является необходимостью?
3. Какие функции включает в себя организационно-правовая база?
4. Расскажите о компьютерных преступлениях в нашей стране.
5. Какие законы были приняты Законодательной палатой Олий Мажлиса в области информационных технологий?

6. Разработка каких законодательных актов является необходимой для нашей страны?

17-§. Понятие национальной безопасности. Информационная угроза.

Ключевые слова: *национальная безопасность, объект национальной безопасности, субъект национальной безопасности, виды обеспечения ИБ, виды угроз ИБ, информационная угроза.*

Национальная безопасность - это безопасность, которая отвечает за целостность государства.

Национальная безопасность - защищенность жизненно важных интересов личности, общества и государства в различных сферах жизнедеятельности от внешних и внутренних угроз, обеспечивающая устойчивое развитие страны. По другому определению - национальная безопасность - совокупность официально принятых взглядов на цели и государственную стратегию в области обеспечения безопасности личности, общества и государства от внешних и внутренних угроз политического, экономического, социального, военного, техногенного, экологического, информационного и иного характера с учетом имеющихся ресурсов и возможностей [21].

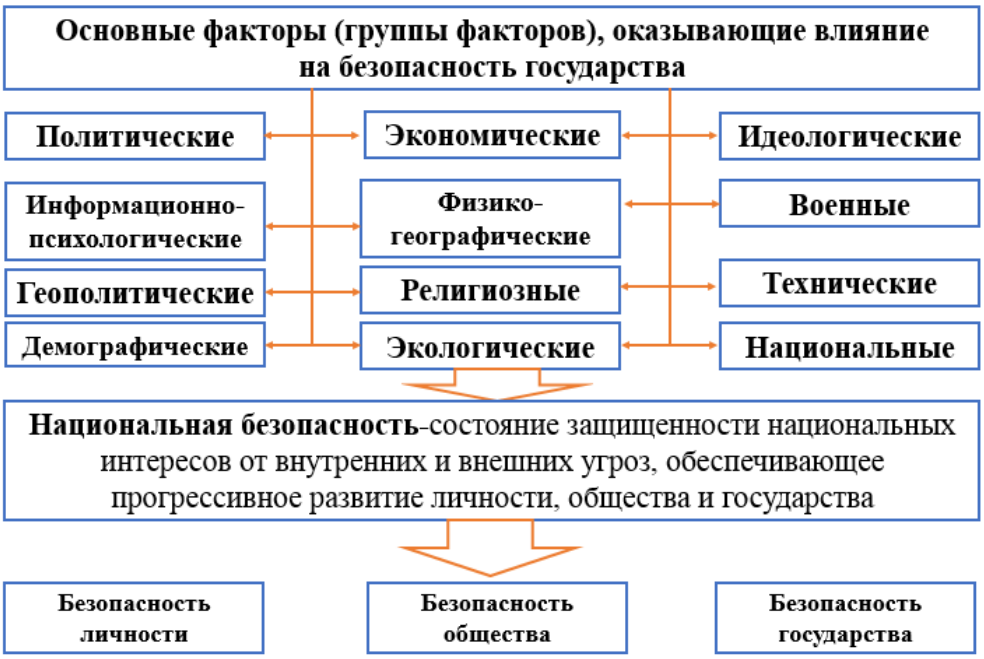
Национальная безопасность – это защищенность политических, экономических, социальных и иных отношений и организационных связей, материальных, финансовых и интеллектуальных ресурсов личности, общества и государства от угроз; это состояние системы отношений, при котором реализуются жизненно важные интересы личности, общества и государства[55].

[55] *А. Бирюков. "Информационная безопасность: защита и нападение" 2-е изд. (2017)*

Основными объектами - национальной безопасности установлены: личность - ее права и свободы; общество - материальные и духовные ценности; государство - его конституционный строй, суверенитет и территориальная целостность.

Основным субъектом обеспечения национальной безопасности является государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной власти. Закон определяет силы и средства обеспечения безопасности в структуре силовых ведомств, органов, обеспечивающих безопасное ведение работ в промышленности, энергетике, на транспорте и в сельском хозяйстве; службы обеспечения безопасности средств связи и информации, таможни, природоохранных органов, органов охраны здоровья населения и других государственных органов обеспечения безопасности, действующих на основании законодательства.

Главным объектом и субъектом национальной безопасности сейчас мы считаем человека. Человек присутствует во всех видах безопасности. Поэтому обеспечение безопасности личности становится условием обеспечения безопасности всех других ее видов и уровней. С другой стороны, положение личности определяется состоянием общества, государства (рис.4.16.1).



(рис.4.16.1). Понятие национальной безопасности

Личную безопасность каждый человек может обеспечить себе лишь частично, действуя в рамках закона и не пренебрегая интересами общества и государства. Негосударственные организации, действующие на общественных началах, могут обеспечить в какой-то степени безопасность отдельных групп населения. Основным же инструментом обеспечения безопасности жизнедеятельности призвано быть государство. Это не только его основная задача, но и исключительная обязанность [21].

Принципы обеспечения национальной безопасности - это руководящие и наиболее важные идеи, направленные на реализацию национальных целей. Основными принципами обеспечения национальной безопасности являются: законность; соблюдение баланса жизненно важных интересов личности, общества и государства; взаимная ответственность личности, общества и государства за обеспечение безопасности; интеграция с международными системами безопасности.

Государство обеспечивает национальную безопасность всей своей совокупной мощью, которая определяется его природными ресурсами, уровнем развития экономики, морально-политическим потенциалом населения, геополитическим положением страны и, наконец, состоянием

военной мощи. Поэтому, чем сильнее государство, тем надежнее обеспечивается национальная безопасность.

При выполнении даже внутренних функций главной целью использования силовых структур является нормализация обстановки, восстановление законности и правопорядка, устранение угрозы безопасности граждан, оказание необходимой помощи и создание условий для решения конфликта политическими средствами.

Конкретные задачи обеспечения национальной безопасности *(НБ)*:

- подъем экономики страны, проведение независимого и социально ориентированного курса;
- совершенствование законодательства, укрепление правопорядка и социально-политической стабильности - общества, местного самоуправления, формирование гармоничных межнациональных отношений;
- укрепление безопасности государства в оборонной и информационной сферах;
- обеспечение жизнедеятельности населения в техногенно безопасном и экологически чистом мире.

Основные принципы обеспечения НБ:

- законность;
- соблюдение баланса жизненно важных интересов личности, общества и государства;
- взаимная ответственность личности, общества и государства по обеспечению НБ;
- интеграция с международными системами безопасности;
- единство, взаимосвязь и сбалансированность всех видов безопасности, изменение их приоритетности в зависимости от ситуации;
- сочетание централизованного и децентрализованного управления силами и средствами.

Обеспечение национальной безопасности в сфере информационных угроз

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности государства.

Под информационной безопасностью понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.
Выделяются четыре основные составляющие национальных интересов в информационной сфере[56].

Первая составляющая национальных интересов в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны [21].

Вторая составляющая национальных интересов в информационной сфере включает в себя информационное обеспечение государственной политики, связанное с доведением достоверной информации о государственной политике

Третья составляющая национальных интересов в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники.

Четвертая составляющая национальных интересов в информационной сфере включает в себя защиту информационных ресурсов от

[56] *А. Бирюков. "Информационная безопасность: защита и нападение" 2-е изд. (2017)*

несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Виды угроз информационной безопасности

По своей общей направленности угрозы информационной безопасности подразделяются на следующие виды:

- угрозы информационному обеспечению государственной политики;
- угрозы развитию индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем.

Информационная угроза.

Информационная угроза (англ. Information war nformation threat) - термин, имеющий два значения:

1. *Процесс противоборства человеческих общностей*, направленный на достижение политических, экономических, военных или иных целей стратегического уровня, путём воздействия на гражданское население, власти и *(или)* вооружённые силы противостоящей стороны, посредством распространения специально отобранной и подготовленной информации, информационных материалов, и, противодействия таким воздействиям на собственную сторону. Термин «информационно-психологическая угроза» был заимствован в русский язык из словаря военных кругов США. Перевод этого термина *(information and psychological threat)* с английского языка может звучать и как *«информационное противоборство»*, и как *«информационная, психологическая угроза»*, в зависимости от контекста конкретного официального документа или научной публикации. В этом смысле также используется термин психологическая угроза - психологическое воздействие на гражданское население и *(или)*

военнослужащих другого государства с целью достижения политических или чисто военных целей[21].

2. *Целенаправленные действия,* предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем.

Существует множество определений понятия *«информационная угроза»*. В связи с этим представляется целесообразным рассмотреть самые популярные их них и выделить черты, присущие всем толкованиям этого явления.

(рис.4.16.2). Информационная угроза

Информационная угроза - это:

- воздействие на гражданское население и *(или)* военнослужащих другого государства путём распространения определенной информации.
- целенаправленные действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем;

- всеобъемлющая, целостная стратегия, обусловленная все возрастающей значимостью и ценностью информации в вопросах командования, управления, политики, экономики и общественной жизни;
- действия, предпринимаемые для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой нашей собственной информации и информационных систем;
- сбор компромата против конкурентов и его планомерное использование;
- явные и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере;
- новая форма борьбы сторон, в которой используются специальные способы и средства, воздействующие на информационную среду противника и защищающие собственную в интересах достижения стратегических целей узрозы.

Анализ определений позволяет выделить те черты, которые всегда присутствуют при ведении информационной угрозы [21]:

- воздействие на какую-либо аудиторию *(народ, военнослужащих, рабочих, интеллигенцию и т.д.)*;
- информация, передаваемая этой аудитории;
- стратегия применения информационных средств носит исключительно наступательный характер;
- цель ведения информационной угрозы - изменение мышления стороны, на которую направлено воздействие и получение более выгодного положения;
- защита собственного информационного пространства от нападения.

Составные части информационной угрозы

- психологические операции - использование информации для воздействия на аргументацию солдат врага;
- электронная угроза - не позволяет врагу получить точную информацию;
- дезинформация - предоставляет врагу ложную информацию о наших силах и намерениях;
- физическое разрушение - может быть частью информационной угрозы, если имеет целью воздействие на элементы информационных систем;
- меры безопасности - стремятся избежать того, чтобы враг узнал о наших возможностях и намерениях;
- прямые информационные атаки - прямое искажение информации без видимого изменения сущности, в которой она находится.

Информационная угроза - это средство для достижения какой - либо цели стороны, ведущей эту угрозу. Как и любое средство, информационная угроза предназначена для выполнения определённых функций[57]:

- контролировать информационное пространство для получения возможности использовать его, защищая при этом собственные информационные функции от вражеских действий *(контринформация)*.
- использовать контроль за информацией для ведения информационных атак на врага.
- повысить общую эффективность собственных сил с помощью повсеместного использования военных информационных функций.

Для осуществления информационного воздействия необходимо соблюдение некоторых условий. Для того чтобы информационная система была способна целенаправленно перепрограммировать другую подобную систему, она должна ее «понимать». Под «пониманием» в данном контексте

[57] *А. Бирюков. "Информационная безопасность: защита и нападение" 2-е изд. (2017)*

принимается такое состояние, при котором «на абсолютное большинство одинаковых входных сообщений две информационные системы выдают одинаковые по смыслу результаты». Данное утверждение включает следующие пояснения [21]:

- перепрограммирование информационной системы - означает подбор для нее таких входных данных, которые соответствуют цели стороны-агрессора;
- цель перепрограммирования - это поиск в окружающем мире или специальное создание информационного эталона, на который данная система должна стать похожей.

«Понимающие» информационные системы формируются одинаковыми эмоциональными воздействиями, минуя средства защиты, основанные на логике. В случае быстрого и массового перепрограммирования народа, нации наиболее эффективными являются приемы, имеющие эмоциональную окраску и принадлежащие таким сферам как: массовые культура, искусство, религия. Это значит, что для решения задач по перепрограммированию населения в первую очередь упор должен делаться на деятелей искусства, культуры, религиозных служителей.

Разрушение устоявшихся информационных структур способствуют увеличению возможностей для перепрограммирования систем.

Для любой информационной системы безопасно оперировать с той информацией, механизмы обработки которой уже существуют у данной системы.

Информационное воздействие - целенаправленная и спланированная череда действий. Учёными выделены некоторые модели ведения информационной угрозы. Традиционный прямой способ воздействия на сознание основан на убеждении людей. Необходимой составной частью является обращенной к разуму людей, учет реальной обстановки. При этом важно понимать расстановку сил, реальные интересы людей, проводить

научный анализ, учитывать состояние общественного сознания, давать четкие, броские, понятные лозунги.

Помимо рациональных методов применяются методы, основанные на эмоциональном воздействии. Один из самых эффективных - метод большой лжи. Он основан на том, что в большую ложь люди верят охотнее, чем в малую.

В основе другого метода лежит ограниченность восприятия людей. Человек не успевает перерабатывать массив данных, и его оперативная память ограничена, избыточную информацию он воспринимает как шум. Поэтому действительно важную роль играют простые формулировки, повторение, закрепление определенного набора положений.

Следующий метод основан на том, что в подсознании человека заложено определенное, коррелирующее поступки отдельных лиц, "стадное" чувство принадлежности к определенной общественной группе, которое стимулирует моду, синхронизацию поступков, подчинение лидерам.

Необходимо также рассмотреть *эффективность информационной угрозы*. Иными словами, какое состояние считать успешной информационной войной, какое - нет. Стоит отметить, что оно будет различными для стороны, провоцирующей войну и стороны, реагирующую на неё. Для стороны-провокатора *эффективная информационная угроза* - это изменение поведения противоположной стороны на желаемую. *Неэффективная информационная угроза* - это распознавание противоположной стороной акта информационного воздействия и осуществление ей успешных обратных действия, при которых модель мышления, подвергавшаяся изменению, осталась прежней [21].

Для стороны, подвергшейся информационной атаке, «выйти победителем - это значит вовремя понять, чему можно обучаться, а чему нельзя, т.е. какие входные данные можно обрабатывать, а какие - ни в коем случае». Проиграть - значит принять навязываемый эталон мышления и внедрить его в свою деятельность.

Методы ведения информационных угроз.

Как правило, *методами информационной угрозы* являются вброс дезинформации или представление информации в выгодном для себя ключе. Данные методы позволяют изменять оценку происходящего населением территории противника, развивать пораженческое настроение, и, в перспективе, обеспечить переход на сторону ведущего информационное воздействие. С появлением средств массовой информации и общим повышением уровня грамотности в XX веке ведение информационной угрозы стало более эффективным. Кроме традиционных средств массовой информации, в настоящее время эффективным инструментом информационной угрозы являются социальные сети.

Информационно-сетевая угроза.

В настоящее время уровень развития информационных технологий стер границы между государствами в информационном пространстве и создал беспрецедентные возможности для подавления противника без использования традиционных средств поражения. Все это давно осознали в Пентагоне, и в 1998 году Министерство Обороны США была разработана новая «Объединенная доктрина информационных операций». В ней впервые вводится термин «стратегическое информационное противоборство».

Целями воздействия в нем являются объекты противника, выбираемые по принципу «пяти колец» *(по мере убывания важности)* [21]:

- политическое и военное руководство страны;
- системы жизнеобеспечения;
- инфраструктура;
- население;
- вооруженные силы.

Поскольку воздействие на указанные объекты осуществляется с помощью сетевых технологий и методов, такое противоборство получило название *«информационно - сетевая угроза»*. Основой ее является массированное воздействие на морально - психологическое состояние

руководства и населения страны - противника. Причем, зачастую даже сам факт такого воздействия заблаговременно не может быть выявлен ее спецслужбами.

Информационно - сетевая угроза предусматривает проведение комплекса мероприятий в отношении противника[58]:

- создание атмосферы без духовности и безнравственности, что автоматически создает благоприятную атмосферу для нагнетания конфликтной обстановки внутри страны - противника и падению авторитета государственной власти;
- манипулирование общественным мнением и политической ориентацией социальных групп с целью создания обстановки политической напряженности и хаоса;
- дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигания атмосферы недоверия и подозрительности; обострение политической борьбы, провоцирование репрессий против оппозиции; развязывание в обществе гражданской угрозы;
- снижение уровня информационного обеспечения органов власти и управления с целью затруднения принятия важных решений;
- дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;
- провоцирование социальных, политических, национальных и религиозных столкновений; инициирование массовых протестных акций, забастовок, массовых беспорядков;
- подрыв международного авторитета государства;
- нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах.

---

[58] *А. Бирюков. "Информационная безопасность: защита и нападение" 2-е изд. (2017)*

При этом информационное противоборство следующего поколения характеризуется следующими особенностями:

Одна из целей информационно - сетевых угроз - провоцирование социальных, политических, национальных и религиозных столкновений, инициирование забастовок, массовых беспорядков и протестных акций, перенос агрессии из военно-географического в информационно - сетевое измерение.

Современный исследователь В.М. Коровин пишет так*: «Сетевая угроза никогда не ведется прямым образом. Заказчик никогда напрямую не связан с исполнителем. И даже если провести линию через множество посредников от исполнителей к заказчику - прямой не получится. И кривой не получится. Совокупность проведенных линий образует сеть. Если у вас получилась прямая или даже кривая - то перед вами не сетевая операция, а обычная, классическая операция эпохи модерна, в которой связь между заказчиком и исполнителем, даже при отсутствии некоторых промежуточных элементов, вполне установима. Сетевая угроза ведется на более тонком уровне, с использованием информационных технологий, дипломатических сетей, неправительственных организаций, с подключением журналистов, политиков, СМИ. Это многоуровневая операция, в которой обычному оружию нет места, но тем не менее результатом ее становится отторжение территорий - конкретная «военная» победа».*

Вопросы для самоконтроля

1. Что подразумевает под собой понятие национальная безопасность?
2. Назовите объекты изучения национальной безопасности.
3. Что является субъектом изучения национальной безопасности?
4. Принципы обеспечения национальной безопасности - это ...
5. Перечислите основные принципы обеспечения национальной безопасности.

6. Расскажите об обеспечении национальной безопасности в сфере информационных угроз.

18-§. Средства безопасности в операционной системе Windows

Ключевые слова: *операционная система, безопасность ОС, административные меры защиты, политика безопасности, стандарты безопасности.*

Понятие защищенной операционной системы

Операционная система есть специально организованная совокупность программ, которая управляет ресурсами системы *(ЭВМ, вычислительной системы, других компонентов ИВС)* с целью наиболее эффективного их использования и обеспечивает интерфейс пользователя с ресурсами.

Под механизмами защиты ОС будем понимать все средства и механизмы защиты данных, функционирующие в составе ОС. Операционные системы, в составе которых функционируют средства и механизмы защиты данных, часто называют защищенными системами [42].

Под безопасностью ОС будем понимать такое состояние ОС, при котором невозможно случайное или преднамеренное нарушение функционирования ОС, а также нарушение безопасности находящихся под управлением ОС ресурсов системы[59].

Операционную систему можно назвать защищенной, если она предусматривает средства защиты от основных угроз конфиденциальности, целостности и доступности информации, актуализированных с учетом особенностей эксплуатации данного конкретного экземпляра операционной системы. В практически значимых ситуациях защищенная операционная система обычно содержит средства управления доступом пользователей к

[59] *Н.В. Макарова, В.Б. Волков. Информатика. «ООО» Издательство «Питер», 2011.*

различным ресурсам, средства проверки подлинности пользователя, начинающего работу с операционной системой, а также средства регистрации действий пользователей, потенциально опасных с точки зрения безопасности. Кроме того, защищенная операционная система должна содержать средства противодействия случайному или преднамеренному выводу операционной системы из строя.

Политика безопасности – это набор норм, правил и практических приемов, регламентирующих порядок хранения и обработки ценной информации. В применении к операционной системе политика безопасности определяет то, какие пользователи могут работать с операционной системой, какие пользователи имеют доступ к каким объектам операционной системы, какие события должны регистрироваться в системных журналах и т.д.

Адекватная политика безопасности – это такая политика безопасности, которая обеспечивает достаточный уровень защищенности операционной системы. Следует особо отметить, что адекватная политика безопасности не обязательно является той политикой безопасности, при которой достигается максимально возможная защищенность системы.

Основные подходы к построению защищенных операционных систем

Существуют два основных подхода к созданию защищенных операционных систем - *фрагментарный* и *комплексный*. При фрагментарном подходе вначале организуется защита от одной угрозы, затем от другой и т.д. Примером фрагментарного подхода может служить ситуация, когда за основу берется незащищенная операционная система, на нее устанавливаются антивирусный пакет, затем система шифрования, система регистрации действий пользователей и т.д.

Основной недостаток фрагментарного подхода очевиден - при применении этого подхода подсистема защиты операционной системы представляет собой набор разрозненных программных продуктов, как правило, произведенных разными производителями. Эти программные средства работают независимо друг от друга, организовать их тесное

взаимодействие практически невозможно. Кроме того, отдельные элементы такой подсистемы защиты могут некорректно работать в присутствии друг друга, что приводит к резкому снижению общей надежности системы. Поскольку подсистема защиты, созданная на основе фрагментарного подхода, не является неотъемлемой компонентой операционной системы, при отключении отдельных защитных функций в результате несанкционированных действий пользователя-нарушителя остальные элементы операционной системы продолжают нормально работать, что еще сильнее снижает надежность защиты.

При комплексном подходе к организации защиты защитные функции вносятся в операционную систему еще на этапе проектирования архитектуры операционной системы и являются ее неотъемлемой частью. Отдельные элементы подсистемы защиты, созданной на основе комплексного подхода, тесно взаимодействуют друг с другом при решении различных задач, связанных с организацией защиты информации. Поскольку вся подсистема защиты разрабатывается и тестируется в совокупности, конфликты между ее отдельными компонентами практически невозможны. Подсистема защиты, созданная на основе комплексного подхода, может быть устроена так, что при фатальных сбоях в функционировании ее ключевых элементов подсистемы защиты она вызывает аварийное завершение работы операционной системы, что не позволяет нарушителю отключать защитные функции системы. При использовании фрагментарного подхода такая организация подсистемы защиты невозможна.

Как правило, подсистему защиты операционной системы, созданную на основе комплексного подхода, проектируют так, что отдельные ее элементы являются заменяемыми и соответствующие программные модули могут быть заменены другими модулями, реализующими предусмотренный и должным образом документированный интерфейс взаимодействия соответствующего программного модуля с другими элементами подсистемы защиты [58].

Административные меры защиты

Организация эффективной и надежной защиты операционной системы невозможна с помощью одних только программно-аппаратных средств. Эти средства обязательно должны дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже самая надежная программно-аппаратная защита оборачивается фикцией.

К основным административным мерам защиты относятся следующие:

- постоянный контроль корректности функционирования операционной системы и, в особенности, ее подсистемы защиты. При этом могут и должны использоваться средства аудита, встроенные в операционную систему, и, при необходимости, дополнительные средства аудита;
- организация и поддержание адекватной политики безопасности. Политика безопасности должна постоянно корректироваться, оперативно реагируя на изменения в конфигурации операционной системы, установку и удаление, и изменение конфигурации прикладных программных продуктов и расширений операционной системы, попытки злоумышленников преодолеть защиту операционной системы и т.д.;
- инструктирование пользователей операционной системы о необходимости соблюдения мер безопасности при работе с операционной системой, контроль над соблюдением пользователями этих мер;
- регулярное создание и обновление резервных копий программ и данных операционной системы;
- постоянный контроль изменений в конфигурационных данных и политике безопасности операционной системы. Информацию об этих изменениях часто дублируют на неэлектронные носители информации, чтобы нарушителю, преодолевшему защиту операционной системы, было труднее замаскировать свои несанкционированные действия[60].

[60] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

В конкретных конфигурациях операционных систем могут потребоваться и другие административные меры защиты информации [42].

Адекватная политика безопасности

Задача выбора и поддержания адекватной политики безопасности является важнейшей и одной из сложнейших задач, стоящих перед администратором операционной системы. Если принятая в операционной системе политика безопасности неадекватна, это может приводить к фактам несанкционированного доступа пользователя-нарушителя к ресурсам защищаемой системы, а также к снижению надежности ее функционирования.

Не всякая адекватная политика безопасности применима на практике. В общем случае верно следующее утверждение: чем лучше операционная система защищена, тем труднее с ней работать пользователям и администраторам. Это обусловлено следующими факторами[61].

1. Система защиты, не обладающая интеллектом, не всегда способна определить, является ли некоторое действие пользователя злонамеренным. Поэтому система защиты либо не пресекает некоторые виды несанкционированного доступа, либо запрещает некоторые вполне легальные действия пользователей. Чем выше защищенность системы, тем шире класс тех легальных действий пользователей, которые рассматриваются подсистемой защиты как несанкционированные. Если, например, некоторому пользователю запрещено создавать файлы на жестком диске компьютера, то этот пользователь не сможет запустить ни одну программу, для нормального функционирования которой требуется создавать временные файлы. С точки зрения рассматриваемой политики безопасности создание временного файла является несанкционированным действием и в том, что оно пресекается, нет ошибки. Просто в данной политике безопасности класс несанкционированных действий настолько широк, что это препятствует нормальной работе пользователей с операционной системой.

---

[61] *Н.В. Макарова, В.Б. Волков. Информатика. «ООО» Издательство «Питер», 2011.*

2. Любая система, в которой предусмотрены функции защиты информации, требует от администраторов определенных усилий, направленных на поддержание адекватной политики безопасности. Чем больше в операционной системе защитных функций, тем больше времени и средств нужно тратить на поддержание защиты.

3. Подсистема защиты операционной системы, как и любой другой программный пакет, потребляет аппаратные ресурсы компьютера. Чем сложнее устроены защитные функции операционной системы, тем больше процессорного времени, оперативной памяти и других аппаратных ресурсов затрачивается на поддержание функционирования подсистемы защиты и тем меньше ресурсов остается на долю прикладных программ. В отдельных случаях подсистема защиты операционной системы может потреблять более половины аппаратных ресурсов компьютера.

4. Поддержание слишком жесткой политики безопасности может негативно сказаться на надежности функционирования операционной системы. Если, например, в Windows запретить псевдопользователю SYSTEM, от имени которого выполняются системные процессы, доступ к исполняемым файлам системных процессов, операционная система не сможет загрузиться. В данном случае чрезмерно жесткая политика безопасности приводит к моментальному краху операционной системы, в других случаях подобная политика безопасности может приводить к трудно выявляемым ошибкам и сбоям в процессе функционирования операционной системы, что еще более опасно.

Таким образом, при определении адекватной политики безопасности не следует пытаться достигнуть максимально возможного уровня защищенности операционной системы. Оптимальная адекватная политика безопасности - такая политика безопасности, которая не только не позволяет нарушителям выполнять несанкционированные действия, но и не приводит к вышеописанным негативным последствиям.

Не существует единой адекватной политики безопасности на все случаи жизни. То, какая политика безопасности будет адекватной, определяется не только архитектурой операционной системы, но и ее конфигурацией, ассортиментом установленного программного обеспечения и т.д. Политика безопасности, адекватная для некоторой операционной системы, скорее всего, будет неадекватна для другого экземпляра той же операционной системы. Большинство современных операционных систем достаточно универсальны и могут применяться для решения самых разных задач. Одна и та же операционная система может использоваться для обеспечения функционирования автоматизированной банковской системы, web-сервера, системы электронного документооборота. Очевидно, что угрозы безопасности для всех трех указанных применений будут различны и адекватная политика безопасности в каждом из трех случаев будет своя.

Формирование и поддержание адекватной политики безопасности операционной системы в общем случае можно разделить на следующие этапы [58].

1. *Анализ угроз*. Администратор операционной системы рассматривает возможные угрозы безопасности данного экземпляра операционной системы. Среди возможных угроз выделяются наиболее опасные, защите от которых нужно уделять максимум сил и средств.

2. *Формирование требований к политике безопасности.* На этом этапе администратор определяет, какие средства и методы будут применяться для защиты от тех или иных угроз. Например, защиту от несанкционированного доступа к некоторому объекту операционной системы можно решать либо средствами разграничения доступа, либо криптографическими средствами, либо используя некоторую комбинацию этих средств, либо используя какие-то иные средства. На данном этапе администратор должен сделать подобный выбор для каждой угрозы безопасности операционной системы, выбирая оптимальные средства защиты от каждой угрозы. Одновременно администратор анализирует возможные побочные эффекты различных

вариантов политики безопасности, оценивая, в какой мере в каждом варианте политики безопасности будут проявляться побочные негативные факторы. Как правило, администратору приходится идти на компромисс, смиряясь либо с недостаточной защищенностью операционной системы от отдельных угроз, либо с определенными трудностями пользователей при работе с системой. Результатом данного этапа является набор требований наподобие: «В операционной системе должно быть предусмотрено дискреционное разграничение доступа с минимизацией полномочий пользователей и частичной реализацией правил изолированной программной среды[62]».

3. *Формальное определение политики безопасности*. Данный этап заключается в том, что администратор четко определяет, как конкретно должны выполняться требования, сформулированные на предыдущем этапе. Администратор решает, можно ли добиться выполнения этих требований только встроенными средствами операционной системы или необходима установка дополнительных пакетов защиты. В последнем случае производится выбор необходимого программного обеспечения. На данном этапе формулируются необходимые требования к конфигурации операционной системы, а также требования к конфигурации дополнительных пакетов защиты, если установка таких пакетов необходима. Кроме того, на данном этапе администратор должен предусмотреть порядок внесения необходимых изменений в политику безопасности в чрезвычайных ситуациях, например, при обнаружении факта несанкционированного входа в систему пользователя-нарушителя. Результатом данного этапа является развернутый перечень настроек конфигурации операционной системы и дополнительных пакетов защиты с указанием того, в каких ситуациях какие настройки должны быть выставлены.

---

[62] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

4. *Претворение в жизнь политики безопасности*. К началу этого этапа у администратора операционной системы имеется четкое представление о том, какой должна быть адекватная политика безопасности. Задачей этапа является приведение конфигурации операционной системы и дополнительных пакетов защиты в соответствие с политикой безопасности, формально определенной на предыдущем этапе.

5. *Поддержание и коррекция политики безопасности*. На данном этапе операционная система функционирует в соответствии с политикой безопасности, определенной на третьем этапе. Задачей администратора является контроль над соблюдением политики безопасности и внесение в нее необходимых изменений по мере появления изменений в функционировании операционной системы. Например, если в операционной системе устанавливается новый программный продукт, может потребоваться коррекция политика безопасности таким образом, чтобы этот программный продукт мог нормально функционировать.

Стандарты безопасности операционных систем

Анализ угроз, с которого начинается формирование политики безопасности, является весьма трудоемкой и трудно формализуемой процедурой. Как правило, угрозы, от которых предполагается защищать компьютерную систему или сеть, очень разнородны, сравнивать их между собой и выделять среди них наиболее опасные обычно крайне затруднительно. Иногда эту проблему пытаются решать путем количественного выражения элементарных рисков в некоторых условных единицах с использованием формул наподобие:

*Риск = (стоимость ресурса * вероятность угрозы) / величина уязвимости*

Практическая реализация данного подхода в конкретных операционных системах сталкивается с рядом трудностей. Наиболее серьезная проблема количественного анализа рисков заключается в том, что для исходных числовых данных, используемых в количественном анализе рисков, часто

затруднительно обосновать погрешность присвоения тем или иным качественным характеристикам конкретных числовых значений. Например, погрешность оценки вероятности угрозы может быть корректно вычислена только для тех угроз, которые реализуются регулярно. Если же попытки реализации некоторой угрозы в исследуемых операционных системах ни разу не регистрировались, вероятность данной угрозы, как правило, можно оценить лишь с точностью до порядка. Соответственно, риск данной угрозы тоже может быть вычислен лишь с точностью до порядка. Это может поставить под сомнение обоснованность окончательных выводов, сделанных в результате проведенного анализа.

К сожалению, часто наблюдаются ситуации, когда эксперты, выполняющие анализ рисков той или иной операционной системы, совсем не уделяют внимания оценкам погрешностей используемых количественных показателей, в результате чего анализ рисков вырождается в «жонглирование цифрами», позволяющее получить любой желаемый результат, подобрав исходные данные соответствующим образом[63].

Альтернативный подход к управлению безопасности основан на том, чтобы привести политику безопасности защищаемой системы в соответствие с тем или иным набором стандартов безопасности или иных нормативных документов. Основным преимуществом такого подхода является то, что он позволяет существенно сократить затраты на разработку политики безопасности, сведя к минимуму анализ рисков для защищаемой системы. Фактически, анализ рисков в данном случае сводится к обоснованию выбора стандартов безопасности, используемых в качестве основы для планирования политики безопасности операционной системы.

Если защищаемая операционная система имеет типовую конфигурацию и хорошо описывается существующими стандартами безопасности,

---

[63] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

применение данного подхода к управлению безопасностью является вполне оправданным. С другой стороны, известны случаи бездумного применения к управлению безопасностью конкретных систем заведомо неподходящих стандартов безопасности.

В последнее время заметной становится тенденция к сближению двух рассмотренных подходов. Стандарты информационной безопасности становятся все более подробными и детализированными, с каждым годом все больше практически значимых ситуаций оказываются описанными в тех или иных стандартах. Большое влияние на роль и место стандартов безопасности в процессе управления безопасностью конкретных компьютерных систем оказал состоявшийся в последнее десятилетие переход от линейных шкал классов защищенности к более гибкой системе профилей защиты. Если раньше стандарты информационной безопасности позволяли удовлетворительно описать требования к безопасности лишь для наиболее типовых конфигураций операционных систем, то теперь профиль защиты может быть построен для практически любой конфигурации операционной системы, исключая лишь самые экзотические. При этом для конкретной операционной системы выбор и обоснование выбора профиля защиты выполняется путем анализа рисков, соответствующих тем или иным профилям защиты.

Управление доступом

Объектом доступа *(или просто объектом)* мы будем называть любой элемент операционной системы, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен. Ключевым словом в данном определении является слово «*произвольно*». Если правила, ограничивающие доступ субъектов к некоторому элементу операционной системы, определены жестко и не допускают изменения с течением времени, этот элемент операционной системы мы не будем считать объектом. Другими словами, возможность доступа к объектам операционной системы

определяется не только архитектурой операционной системы, но и текущей политикой безопасности.

Методом доступах, объекту называется операция, определенная для некоторого объекта. Например, для файлов могут быть определены методы доступа «чтение», «запись» и «добавление» *(дописывание информации в конец файла)*.

Субъектом доступа *(или просто субъектом)* мы будем называть любую сущность, способную инициировать выполнение операций над объектами *(обращаться к объектам по некоторым методам доступа)*. Например, пользователи являются субъектами доступа[64].

Обычно к субъектам доступа относят не только пользователей, работающих в системе, но и порожденные ими процессы. Данный подход является оправданным и, более того, единственно верным, во всех случаях, когда в область рассмотрения включаются программные закладки, функционирующие автономно и преследующие свои собственные задачи, не совпадающие с целями пользователя, работающего в системе. Однако мы будем *(за редкими исключениями)* рассматривать только *«чистые»* операционные системы, не зараженные вредоносным программным обеспечением.

Таким образом, в данном разделе везде, где явно не оговорено противное, субъектом доступа мы будем считать не процесс *(или поток процесса-сервера)*, выполняющий некоторую операцию, а пользователя, от имени которого этот процесс *(или поток)* выполняется.

Итак, *объект доступа* - это то, к чему осуществляется доступ, субъект доступа - это тот, кто осуществляет доступ, и метод доступа - это то, как осуществляется доступ.

---

[64] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

Для объекта доступа может быть определен владелец - субъект, несущий ответственность за конфиденциальность содержащейся в объекте информации *(если эта информация конфиденциальна)*, а также за целостность и доступность объекта. Обычно владельцем объекта автоматически назначается субъект, создавший данный объект, в дальнейшем владелец объекта может быть изменен с использованием соответствующего метода доступа к объекту. Владелец объекта не может быть лишен некоторых прав на доступ к этому объекту, на владельца, как правило, возлагается ответственность за корректное ограничение прав доступа к данному объекту других субъектов.

Правом доступа к объекту мы будем называть право на выполнение доступа к объекту по некоторому методу или группе методов. В последнем случае право доступа дает субъекту возможность осуществлять доступ к объекту по любому методу из данной группы. Говорят, что субъект имеет некоторое право на доступ к объекту *(или «субъект имеет право доступа к объекту» или «субъект имеет право на объект»)*, если он имеет возможность осуществлять доступ к объекту по соответствующему методу или группе методов. Например, если пользователь имеет возможность читать файл, говорят, что он имеет право на чтение этого файла [58].

Говорят, что субъект имеет некоторую привилегию, если он имеет возможность выполнять в операционной системе некоторые действия, не выражаемые или трудно выражаемые в терминах доступа субъекта к объектам. Например, в операционной системе Windows поддерживаются привилегии перезагружать компьютер и перенастраивать часы компьютера. Как частный случай, привилегией является возможность применения некоторого права доступа или группы прав доступа ко без исключения объектам операционной системы, поддерживающим соответствующие методы доступа. Например, если субъект операционной системы Windows имеет привилегию отладки, он имеет право доступа ко всем объектам типа «процесс» и «поток» по группе методов, используемых отладчиками при

отладке программ *(фактически, по всем поддерживаемым операционной системой методам доступа)*.

Полномочиями субъекта доступа называется совокупность всех предоставленных ему прав и привилегий.

Управлением доступом субъектов к объектам называется совокупность правил, определяющая для каждой тройки субъект-объект-право, разрешена ли реализация данного права данным субъектом в отношении данного объекта. При дискреционном управлении доступом возможность доступа определяется для каждой тройки субъект-объект-право априорно, при мандатном управлении доступом ситуация несколько сложнее.

Мы будем называть субъекта доступа *суперпользователем*, если он имеет возможность игнорировать правила управления доступом к объектам.

Правила управления доступом, действующие в защищаемой компьютерной системе, устанавливаются администраторами системы при определении текущей политики безопасности. За соблюдением этих правил субъектами доступа следит монитор ссылок или монитор безопасности объектов - часть подсистемы защиты компьютерной системы.

Правила управления доступом должны удовлетворять следующим очевидным требованиям.

- Правила управления доступом, принятые в компьютерной системе, должны соответствовать аналогичным правилам, принятым в организации, в которой эксплуатируется данная система. Другими словами, если, согласно правилам организации, доступ пользователя к некоторой информации считается несанкционированным, то в операционной системе этот доступ тоже должен быть ему запрещен. Под несанкционированным доступом здесь подразумевается не только несанкционированное чтение информации, но и несанкционированное изменение, копирование или уничтожение информации.
- Правила управления доступа должны не допускать *(или, по крайней мере, затруднять)* разрушающие воздействия субъектов доступа, не

обладающих соответствующими полномочиями, на операционную систему, выражающиеся в несанкционированном изменении, удалении или другом воздействии на объекты, критически важные для обеспечения нормального функционирования системы.

- Любой объект системы должен иметь владельца. Присутствие в системе ничейных объектов - объектов, не имеющих владельца, должно быть недопустимо.
- Присутствие в системе недоступных объектов - объектов, к которым не может обратиться ни один субъект доступа ни по одному методу доступа, должно быть недопустимо. Недоступные объекты фактически бесполезно растрачивают аппаратные ресурсы компьютера.
- Утечка конфиденциальной информации из защищаемой системы должна быть недопустима. Поскольку реализовать выполнение данного требования программно-аппаратными средствами весьма сложно, оно предъявляется лишь в редких случаях. Как правило, предотвращение утечки конфиденциальной информации из защищаемой системы обеспечивается одними только организационными мерами[65].

Управление доступом в Windows

Объекты доступа

В операционных системах семейства Microsoft Windows все объекты операционной системы являются объектами доступа. Другими словами, доступ субъектов к любому объекту операционной системы может быть произвольно ограничен. Атрибуты защиты объекта Windows входят в число обязательных атрибутов, объект, не имеющий атрибутов защиты, физически не может существовать. Даже те объекты, которые не могут иметь атрибуты защиты из-за внутренних особенностей реализации *(например, файлы, физически размещенные на файловой системе FAT, не могут иметь*

[65] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

атрибуты защиты, поскольку те не поддерживаются файловой системой), при открытии получают временный набор атрибутов защиты «объект общедоступен».

Интересной особенностью Windows по сравнению с другими операционными системами является то, что поддерживаемый набор типов объектов доступа не задан жестко в коде операционной системы, но может расширяться системным программным обеспечением, в том числе и разработанным третьими фирмами.

При загрузке операционной системы все поддерживаемые типы объектов регистрируются путем создания в директории дерева объектов ObjectTypes специальных объектов типа «тип объекта», каждый из которых соответствует одному из поддерживаемых типов объектов. Любая программа, имеющая право создавать объекты в директории ObjectTypes, может регистрировать в операционной системе нестандартные типы объектов, которые начиная с момента регистрации обрабатываются Windows наравне со стандартными типами.

В Windows 7 SP1 определено 42 стандартных типа объектов, большинство из которых используются внутри операционной системы и недоступны прикладным программам. Как правило, прикладные программы Windows работают только с объектами следующих типов:

- файловые объекты: файлы, дисковые директории, устройства, именованные каналы и т. п.;
- ключи реестра;
- секции разделяемой памяти;
- процессы;
- потоки;
- события;
- мьютексы;
- семафоры;
- порты;

- маркеры доступа;
- рабочие столы;
- оконные станции;
- пакетные задания;
- директории дерева объектов;
- символические связи *(линки)* дерева объектов.

Субъекты доступа

Операционная система Windows поддерживает следующие типы субъектов доступа:

1. Пользователи, включая псевдопользователей. К псевдопользователям в Windows относятся следующие субъекты доступа:

- SYSTEM - операционная система локального компьютера. Данный псевдопользователь всегда входит в группу Administrators и всегда имеет все привилегии;
- LOCAL SERVICE - псевдопользователь, от имени которого выполняются локальные *(несетевые)* сервисы;
- NETWORK SERVICE - псевдопользователь, от имени которого выполняются сетевые сервисы;
- ANONYMOUS - «бесправный» псевдопользователь, от имени которого выполняются сетевые запросы, сделанные в рамках нуль-сессии *(null session);*
- *(имя_компьютера)* $ - псевдопользователи, соответствующие компьютерам, входящим в домен. Эти псевдопользователи используются при взаимной аутентификации компьютеров в лесу доменов, кроме того эти псевдопользователи используются для делегирования полномочий псевдо пользователя SYSTEM одного компьютера на другие компьютеры леса доменов.

2. Группы пользователей. В Windows группы пользователей могут пересекаться, т.е. каждый пользователь Windows может входить в потенциально неограниченное количество групп. Среди всех групп, в которые

входит пользователь, выделяется одна первичная группа, которая используется исключительно для совместимости со стандартом POSIX, как та самая единственная группа, в которую должен входить любой пользователь POSIX-совместимых систем. К политике безопасности операционной системы первичная группа не имеет никакого отношения[66].

3. Специальные *(временные)* группы. В отличие от обычных групп членство пользователя в таких группах определяется не администратором, а самой операционной системой в зависимости от способа взаимодействия пользователя с системой. К специальным группам относятся:

- INTERACTIVE - пользователи, работающие с системой локально *(обычно не более одного)*;
- NETWORK - пользователи, работающих с системой через сеть;
- DIALJJP - пользователи, работающих с системой по модему;
- BATCH - пользователи и псевдопользователи, от имени которых запущены пакетные задания *(batch jobs)*;
- SERVICE - пользователи и псевдопользователи, от имени которых выполняются сервисы *(службы)*;
- TERMINAL SERVER USER - пользователи, работающие с системой через терминальную сессию.

4. Относительные субъекты. Эти субъекты определяются относительно объекта, для которого определяются права доступа.

Существуют следующие относительные субъекты [58]:

- CREATOR.OWNER - владелец объекта;
- CREATOR.GROUP - первичная группа владельца объекта.

Относительные субъекты используются, если нужно описать права доступа пользователей к объектам по принципу «что кому принадлежит, то ему и доступно».

---

[66] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

Для идентификации субъектов доступа в Windows используется особый тип идентификатора, называемый SID *(security id)*. Субъекты доступа SYSTEM, LOCAL SERVICE, NETWORK SERVICE, ANONYMOUS, Everyone *(группа, в которую входят все пользователи, возможно, за исключением псевдопользователя ANONYMOUS)*, INTERACTIVE, NETWORK, DIAL_UP, BATCH, SERVICE, TERMINAL SERVER USER, CREATOR_OWNER и CREATOR_GROUP имеют стандартные идентификаторы, общие для всех экземпляров операционной системы. Идентификаторы остальных субъекты доступа уникальны в пределах всей вселенной.

Методы и права доступа

Операционная система Windows поддерживает до 22 методов доступа субъектов к объектам каждого типа *(за исключением объектов активного каталога)*. Шесть методов доступа представляют собой стандартные методы, поддерживаемые для объектов всех типов:

- удаление объекта;
- получение атрибутов защиты объекта;
- изменение списка доступа объекта;
- изменение владельца объекта;
- получение и изменение параметров аудита в отношении объекта;
- ожидание объекта.

Для каждого типа объекта поддерживается до 16 специфичных методов доступа. Следующая таблица описывает специфичные методы доступа, определенные для некоторых типов объектов.

Объект	Методы
Файл	чтение запись добавление информации в конец выполнение получение атрибутов

	изменение атрибутов получение расширенных атрибутов изменение расширенных атрибутов
Дисковая директория	просмотр создание нового файла создание поддиректории проход *(traverse)* удаление файла или поддиректории получение атрибутов изменение атрибутов получение расширенных атрибутов изменение расширенных атрибутов
Ключ реестра	чтение значений изменение значений создание подключа перечисление подключей требование оповещения при доступе к ключу другого потока создание символической связи
Процесс	завершение создание нового потока изменение атрибутов страниц адресного пространства чтение адресного пространства запись в адресное пространство дублирование хэндлов получение приоритета изменение приоритета получение информации о процессе изменение квоты

Поток	завершение приостановка/возобновление получение контекста изменение контекста получение приоритета изменение приоритета назначение маркера доступа
Диспетчер сервисов	подключение получение статуса списка сервисов перечисление сервисов создание нового сервиса блокирование списка сервисов
Сервис	запуск останов приостановка/возобновление получение текущего состояния обновление текущего состояния перечисление зависимых сервисов получение конфигурации изменение конфигурации метод доступа, специфичный для данного сервиса
Рабочий стол	чтение элементов рабочего стола изменение элементов рабочего стола создание окна создание меню установка фильтра *(hook setting)* запись макрокоманды *(journal recording)* воспроизведение макрокоманды *(journal playback)* перечисление *(используется функцией EnumDesktops)*

	отображение рабочего стола на экране
Оконная станция	чтение содержимого экрана закрытие получение атрибутов4 изменение атрибутов обращение к карману *(clipboard)* обращение к таблице атомов создание нового рабочего стола перечисление рабочих столов перечисление самой оконной станции *(используется функцией EnumWindowStations)*
Секция	получение информации о текущем состоянии отображение для чтения отображение для записи отображение для выполнения изменение размера
Маркер доступа	чтение получение информации о подсистеме, создавшей маркер доступа включение/выключение групп включение/выключение привилегий изменение атрибутов защиты по умолчанию изменение идентификатора сессии назначение процессу назначение потоку копирование
Событие	получение состояния изменение состояния
Семафор	получение состояния

	изменение состояния
Мьютекс	получение состояния изменение состояния
1. Контекст потока в Windows - аппаратно-зависимая структура данных, в которой сохраняются значения регистров приостановленного или прерванного потока. 2. Все 128 нестандартных операций управления, специфичных для конкретного сервиса, рассматриваются подсистемой управления доступом как единый метод доступа. 3. Элементами рабочего стола Windows являются окна, контексты устройств 4. *(DC)*, шрифты и т.д. Атрибутами оконной станции являются цветовые настройки, используемые обои и хранитель экрана и т.д.	

(табл. 4.18.1). Специфичные методы объектов

Следующие методы доступа требуют наличия у субъекта доступа специальных привилегий:

- создание нового сервиса;
- блокирование списка сервисов;
- запуск сервиса;
- останов сервиса;
- приостановка/возобновление сервиса;
- назначение процессу маркера доступа;
- получение или изменение параметров аудита в отношении объекта.

Каждому специфичному методу доступа, поддерживаемому в Windows, соответствует право на его осуществление. Эти права доступа называются специфичными, поскольку они специфичны для каждого типа объектов. Для каждого типа объектов может поддерживаться до шестнадцати специфичных прав доступа.

Каждому стандартному методу доступа, за исключением метода «получение и изменение параметров аудита в отношении объекта», также

соответствует право доступа, дающее возможность реализации соответствующего метода доступа. Такие права доступа называются стандартными.

Заметим, что для некоторых объектов стандартные и специфичные права доступа реализованы не вполне корректно. Например, при попытке получения атрибутов защиты объекта типа «процесс» проверяется не стандартное право «получение атрибутов защиты», а специфичное право «получение информации о процессе». В Windows 2000 при попытке изменения списка доступа файла проверяется не только стандартное право «изменение списка доступа», но и специфичное право «изменение расширенных атрибутов файла». Видимо, эти странности обусловлены ошибками программистов. В пользу этого предположения говорит то, что странность реализации изменения атрибутов защиты файлов имеет место лишь в Windows 2000, но не в более поздних версиях Windows.

Также Windows поддерживает так называемые общие *(generic)*, или отображаемые *(mapped)* права доступа. Поддерживаются четыре отображаемых права доступа:

- чтение *(GENERICJREAD)*;
- запись *(GENERICLWRITE)*;
- выполнение *(GENERICJEXECUTE)*;
- все действия *(GENERIC_ALL)*.

Каждое из отображаемых прав доступа представляет собой некоторую комбинацию стандартных и специфичных прав доступа. Другими словами, отображаемое право доступа дает возможность на осуществление некоторого набора методов доступа к объекту. Отображаемые права могут быть предоставлены для доступа к объекту любого типа, однако конкретное содержание отображаемого права доступа зависит от типа объекта.

Следует иметь в виду, что порядок отображения отображаемого права доступа в набор стандартных и специфичных прав не обязательно совпадает с интуитивным смыслом общего права доступа.

Например, следующие специфичные права:

- подключение к сервисам - для объекта «диспетчер сервисов»;
- реализация специфичных для конкретного сервиса методов доступа - для объектов типа «сервис»; почему-то не включены в отображаемое право GENERIC_READ.

Но чаще всего порядок отображения отображаемых прав все же совпадает с интуитивно ожидаемым.

Отображаемые права доступа позволяют пользователю устанавливать права доступа к объекту, ничего не зная о специфике объектов данного типа. Например, если пользователь желает, чтобы все пользователи могли читать некоторый файл, он просто предоставляет группе пользователей Everyone отображаемое право на чтение файла. При этом пользователь не обязан отдельно предоставлять группе Everyone права на получение различных атрибутов файла, поскольку все эти права автоматически предоставляются группе Everyone при отображение отображаемого права доступа «чтение объекта». Пользователь может даже не знать, что чтение информации, содержащейся в файле и чтение атрибутов файла реализуются разными методами доступа.

Последним классом прав доступа, поддерживаемых Windows, являются виртуальные права доступа. Виртуальные права доступа не могут быть предоставлены субъекту, но могут быть им запрошены. Поддерживаются два виртуальных права доступа:

- MAXIMUMJ_LLOWED;
- ACCESS_SYSTEM_SECURITY.

Запрашивая виртуальное право MAXIMUM YELLOWED на доступ к объекту, субъект тем самым требует открытия объекта с максимально доступными ему правами. Это виртуальное право позволяет субъекту открыть объект с максимально доступными правами, не производя детального анализа того, какие именно права доступны данному субъекту по отношению к

данному объекту. Операционная система сама проводит такой анализ в процессе проверки прав доступа субъекта к объекту.

Виртуальное право ACCESS_SYSTEM_SECURITY - это право на получение и изменение параметров аудита по данному объекту. Возможность доступа к объектам по этому методу полностью регулируется соответствующей привилегией субъекта доступа. Субъект, обладающий этой привилегией, может обращаться по данному методу доступа к любому объекту операционной системы, а субъект, не обладающий этой привилегией, не может применять данный метод доступа ни к одному объекту. Таким образом, субъект, имеющий доступ к параметрам аудита некоторого объекта, имеет доступ к параметрам аудита любого объекта операционной системы. Разрешить или запретить доступ конкретного субъекта к конкретному объекту по методу «доступ к параметрам аудита по объекту» в Windows невозможно, и поэтому данное право доступа является виртуальным[67].

Аутентификация в Windows

В Windows задачи идентификации, аутентификации и авторизации пользователей решаются специальной подсистемой аутентификации. Подсистема аутентификации Windows делится на три уровня - верхний, средний и нижний. Средний уровень подсистемы аутентификации пользуется услугами нижнего уровня и предоставляет услуги верхнему [58].

Верхний уровень подсистемы аутентификации Windows включает в себя процесс аутентификации winlogon.exe и так называемые провайдеры аутентификации — заменяемые библиотеки, реализующие большую часть высокоуровневых функций процесса аутентификации.

Процесс Winlogon представляет собой обычный процесс, выполняющийся от имени псевдопользователя SYSTEM. Данный процесс автоматически запускается при старте операционной системы и остается

---

[67] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

активным до выключения питания или перезагрузки. При аварийном завершении Winlogon происходит аварийное завершение работы всей операционной системы *(синий экран)*. Таким образом, подменить Winlogon в процессе функционирования операционной системы практически невозможно.

При входе пользователя в систему с локального или удаленного терминала провайдер, обслуживающий данный терминал, получает от пользователя его имя и пароль. В Windows 2003 и более ранних версиях по умолчанию использовался единственный провайдер аутентификации - библиотека *msgina.dll*, которая осуществляет все взаимодействие между локальным пользователем и процессом аутентификации. Начиная с Windows Vista, в Windows реализован более сложный механизм взаимодействия провайдеров аутентификации и процесса Winlogon, основанный на COM-интерфейсах и позволяющий одновременно использовать несколько различных провайдеров аутентификации.

Вход локального пользователя в систему обычно выполняется в Windows следующим образом.

1. Провайдер аутентификации получает от пользователя идентификационную и аутентификационную информацию. В стандартной конфигурации операционной системы в качестве идентификационной информации используется текстовое имя, а в качестве аутентификационной информации - текстовый пароль. Также возможно применение для аутентификации внешних носителей ключевой информации или биометрических характеристик пользователя.

2. Провайдер аутентификации генерирует запрос на аутентификацию, передавая необходимые данные на средний уровень подсистемы аутентификации с помощью системного вызова LsaLogonUser или одной из более высокоуровневых программных оберток этого системного вызова. Если аутентификация прошла успешно, создается маркер доступа пользователя.

3. Если маркер доступа пользователя создан успешно, провайдер аутентификации осуществляет авторизацию пользователя, запуская процесс userinit.exe от имени аутентифицированного пользователя. Для этого используется системный вызов CreateProcessAsUser, который отличается от вызова CreateProcess только тем, что запускаемому процессу назначается маркер доступа, отличный от маркера доступа процесса-родителя. В данном случае процессу userinit назначается только что созданный маркер доступа авторизуемого пользователя.

4. Процесс userinit загружает индивидуальные настройки пользователя из его профиля, запускает программу-оболочку пользователя *(чаще всего это Проводник Windows)* и после этого завершает работу.

В средний уровень подсистемы аутентификации Windows входит локальный распорядитель безопасности *(local security authority, LSA)* и так называемые пакеты аутентификации - заменяемые библиотеки, реализующие большую часть низкоуровневых функций аутентификации.

Локальный распорядитель безопасности представляет собой сервисный процесс lsass.exe, выполняющийся от имени псевдопользователя SYSTEM. Аварийное завершение LSA приводит к аварийному завершению работы всей операционной системы. Так же, как и Winlogon, LSA передоверяет большинство своих функций заменяемым библиотекам. Стандартная схема аутентификации Windows NT обслуживалась пакетом аутентификации MSV 1.0 *(msvl_0.dll)*, а начиная с Windows 2000, стандартным является пакет аутентификации Kerberos.

Пакет аутентификации осуществляет аутентификацию пользователя в процессе обработки системного вызова LsaLogonUser. Аутентификация производится следующим образом [58].

1. Пакет аутентификации получает от верхнего уровня подсистемы аутентификации имя и пароль пользователя и генерирует образ пароля.

2. Используя услуги нижнего уровня подсистемы аутентификации, пакет аутентификации получает информацию, необходимую для проверки

пароля, и проверяет пароль. Проверка пароля может вестись как путем простого сравнения хеш-образа введенного пароля с эталонным хеш-образом *(протоколы LanManager, NTLM)*, так и путем более сложных криптографических процедур *(Kerberos).*

3. Если введенный пароль признан корректным, LSA получает от нижнего уровня подсистемы аутентификации информацию о том, может ли данный пользователь начинать в данный момент работу с данной рабочей станцией *(не устарел ли пароль, не заблокирован ли бюджет пользователя и т.д.)*.

4. В случае положительного результата проверки LSA формирует маркер доступа пользователя, получая необходимую информацию от нижнего уровня подсистемы аутентификации.

5. LSA передает сформированный маркер доступа верхнему уровню подсистемы аутентификации.

Нижний уровень подсистемы аутентификации Windows отвечает за хранение в системе учетной информации о пользователях, в том числе и эталонных образов паролей. При аутентификации пользователя нижний уровень подсистемы аутентификации передает среднему уровню эталонный образ пароля пользователя, а при авторизации - список групп и привилегий пользователя.

Аутентификация при удаленном входе в систему осуществляется в целом по той же схеме за исключением того, что на верхнем уровне вместо процесса Winlogon может выступать произвольная пара *клиент + сервер*. Существует специальный интерфейс SSPI *(Security Support Provider Interface),* обеспечивающий взаимодействие приложений Windows с LSA в ходе аутентификации. В Windows поддерживается пять стандартных провайдеров сетевой аутентификации[68].

---

[68] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

NTLM *(NT Lan Manager, поддерживается начиная с Windows NT 4.0)*

Данный провайдер является наиболее универсальным, он может применяться практически в любой ситуации, когда необходимо осуществить удаленную аутентификацию. Алгоритм сетевого взаимодействия выглядит в общих чертах следующим образом.

1. Клиент направляет серверу имя пользователя в открытом виде *(в NTLM идентификационная информация пользователя не считается секретом)*.
2. Сервер генерирует случайное число от 0 до 65535 и высылает его клиенту.
3. Клиент зашифровывает это число, используя в качестве ключа хеш-функцию пароля пользователя и высылает результат шифрования серверу. В качестве алгоритма шифрования используется модификация алгоритма DES.
4. Сервер проводит аналогичные вычисления и сравнивает результат с полученным от клиента. Если результаты совпали, аутентификация признается успешной, в противном случае - неуспешной. В домене Windows сервер может передоверить данный шаг алгоритма контроллеру домена [58].

Kerberos *(поддерживается, начиная с Windows 2000).*

Протокол аутентификации Kerberos весьма сложен, и детальное его рассмотрение выходит за рамки настоящего пособия. Отметим лишь основные его достоинства и недостатки.

Основным достоинством протокола Kerberos является его чрезвычайно высокая стойкость. Даже перехватив весь трафик информационного взаимодействия всех участников процесса аутентификации, получить несанкционированный доступ к ресурсам любого из участников информационного обмена практически невозможно. Особенно повышают защищенность Kerberos жесткие ограничения, которые данный протокол устанавливает на время аутентификации. Большинство данных, которые могут быть перехвачены нарушителем, устаревают спустя считанные минуты, некоторые данные могут сохранять актуальность несколько часов. В любом

случае, современная вычислительная техника, включая суперкомпьютеры, не позволяет осуществлять взлом используемых криптографических алгоритмов за приемлемое время[69].

Основным недостатком Kerberos является то, что аутентификация по этому протоколу требует некоторой подготовительной работы и не может быть выполнена произвольной парой клиент + сервер. Как минимум, клиент и сервер должны выбрать сервера - посредника, которому они оба доверяют и который заранее осведомлен о некоторых характеристиках клиента и сервера. Поэтому протокол Kerberos может эффективно применяться только в централизованно управляемых локальных сетях с априорно известными топологией и структурой. Существуют модификации Kerberos для работы в Internet и даже для локальной аутентификации, но это, фактически, профанация - в этих режимах Kerberos не имеет никаких преимуществ по сравнению с более примитивными протоколами типа NTLM, но вычислительная сложность криптографических преобразований Kerberos существенно выше.

Negotiate *(поддерживается, начиная с Windows 2000)*.

Этот провайдер обеспечивает автоматический выбор провайдера между NTLM и Kerberos. В современных версиях Windows Negotiate выбирает NTLM лишь в тех случаях, когда использование Kerberos невозможно по техническим причинам. Как правило, приложения обращаются не к NTLM и не к Kerberos, а именно к Negotiate[58].

Digest *(поддерживается, начиная с Windows XP)*.

Данный протокол аутентификации специально предназначен для web-приложений. Подробно спецификации протокола изложены в RFC 2617. Функционально Digest похож на NTLM, для криптографических

---

[69] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

преобразований в Digest может использоваться поточный шифр RC4 с длиной ключа 40, 56 или 128 бит, а также DES либо Triple DES.

Schannel *(поддерживается, начиная с Windows NT 4.0 SP4)*.

Этот провайдер поддерживает протоколы сетевой аутентификации TLS 1.0 и SSL 3.0, а также устаревший протокол PCT 1.0. К криптографическим преобразованиям, используемым Schannel, относятся RC2, RC4, DES, Triple DES, RSA, DHE, MD5, SHA.

Помимо перечисленных стандартных провайдеров, Windows может работать и с нестандартными провайдерами, созданными вне Microsoft. Интерфейсы, используемые провайдерами аутентификации, практически полностью документированы.

Начиная с Windows 2000, Windows поддерживает специальный унифицированный интерфейс, обслуживающий внешние носители ключей аутентификации.

Подсистема аутентификации Windows обладает достаточно большой гибкостью и позволяет администраторам операционной системы настраивать различные параметры аутентификации как для отдельных пользователей системы, так и для всех пользователей в совокупности.

Администраторы Windows могут вводить следующие ограничения на пароли пользователей [58]:

- минимальный и максимальный срок действия пароля;
- минимальную допустимую длину пароля;
- минимальное допустимое количество смен пароля до первого повторения;
- должна ли при смене пароля пользователем проводиться проверка качества нового пароля;
- разрешать ли хранение в системе образов паролей, допускающих обратное расшифрование *(обычно это запрещено, но может потребоваться для некоторых сетевых сервисов)*;

- максимально допустимое количество неудачных попыток входа в систему;
- срок, по истечении которого счетчик неудачных попыток входа в систему обнуляется;
- срок, на который пользователю запрещается вход в систему в случае превышения максимально допустимого количества неудачных попыток входа в систему *(может быть неограниченным, в этом случае запрет на вход пользователя в систему может быть снят только администратором)*;
- могут ли пользователи самостоятельно менять пароль в случае истечения максимального срока его действия, или они должны уведомлять администратора о случившемся;
- могут ли использоваться пустые пароли при сетевой аутентификации;
- какие протоколы аутентификации могут использоваться программами, выполняющимися в данной системе;
- должно ли выдаваться пользователю, осуществляющему локальный вход в систему, имя пользователя, осуществлявшего локальный вход в систему в предыдущий раз;
- обязан ли пользователь нажимать *Ctrl-Alt-Del* перед вводом имени и пароля;
- какое сообщение должно выдаваться пользователю перед входом в систему;
- за какое время до истечения срока действия пароля пользователь начинает получать предупреждения от операционной системы;
- обязательно ли использование внешних носителей ключа при локальной аутентификации;
- как операционная система должна реагировать на извлечение внешнего носителя аутентификационной информации из соответствующего устройства *(варианты: никак не реагировать, заблокировать консоль, завершить сеанс работы пользователя с операционной системой)*;

• через какое время неактивное сетевое соединение должно принудительно разрываться;

• должен ли принудительно завершаться сеанс работы пользователя с операционной системой по истечении разрешенного интервала времени;

• разрешено ли использовать при генерации образа пароля устаревшую хеш-функцию Lan Manager, обладающую низкой криптографической стойкостью;

• должен ли список зарегистрированных пользователей и групп считаться конфиденциальным.

Механизм автоматической блокировки *(lock out)* пользователя при превышении максимально допустимого количества неудачных попыток входа в систему не распространяется на пользователя Administrator.

Для каждого конкретного пользователя могут быть установлены следующие флаги [58]:

• пользователь обязан сменить пароль при ближайшем входе в систему - обычно применяется для только что зарегистрированных пользователей;

• пользователь не может менять свой пароль - обычно применяется для «групповых» пользователей *(например, Guest)*;

• на пользователя не распространяется ограничение максимального срока действия пароля - обычно применяется в совокупности с предыдущим требованием;

• пользователь не может работать в системе - применяется для временного блокирования учетной записи пользователя *(например, на период отпуска или болезни пользователя)*.

Для пользователей домена могут быть введены следующие дополнительные требования к процедурам идентификации, аутентификации и авторизации[70]:

- время работы пользователя с операционной системой может быть ограничено, в этом случае вход пользователя в систему разрешается только в отведенные для этого часы;
- количество компьютеров, с которых пользователь может входить в домен, может быть ограничено, администратор может явно перечислить компьютеры, с которых разрешен вход пользователя в домен;
- может быть установлена автоматическая блокировка учетной записи пользователя по истечении определенного времени;
- может быть указана программа или скрипт, автоматически выполняемая при входе пользователя в систему;
- может быть ограничена продолжительность терминальных сессий пользователя *(подключений к терминальному серверу с удаленных компьютеров через Remote Desktop или другую подобную программу)*;
- может быть включена функция удаленного контроля *(«подсматривания»)* администратора за действиями пользователя в ходе работы с терминальным сервером. В зависимости от настроек данной функции, вмешательство администратора в сессию пользователя может происходить либо только с разрешения пользователя, либо без разрешения, незаметно для пользователя. Вмешательство администратора может быть ограничено просмотром пользовательского терминала либо ничем не ограничено - в этом случае администратор может управлять клавиатурой и мышью вместе с пользователем;
- могут быть установлены особые правила использования пользователем удаленного подключения к домену через модем или VPN.

---

[70] *А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.*

Помимо вышеперечисленных требований и ограничений, при идентификации и аутентификации пользователя также осуществляется проверка одной из следующих пяти так называемых привилегий входа *(привилегии входа, строго говоря, не являются привилегиями, поскольку никогда не добавляются в маркер доступа пользователя и, следовательно, не учитываются монитором безопасности объектов операционной системы)*:

- входить в систему интерактивно;
- входить в систему через сеть;
- входить в систему через терминальный сервер;
- запускать сервис от своего имени;
- запускать пакетное задание *(batch job)* от своего имени.

То, какая «привилегия» должна проверяться, определяется провайдером при вызове функции LogonUser. Например, если четвертый параметр этой функции равен LOGON32_LOGON_SERVICE, это означает, что пользователь входит в систему в качестве сервиса, т. е. запускает сервис от своего имени, и должна быть проверена «привилегия» запускать сервисы от своего имени.

Начиная с Windows 2000, для каждой привилегии входа поддерживается два списка - белый и черный. Чтобы субъект доступа получил некоторую привилегию входа, он должен быть прямо или косвенно упомянут в соответствующем белом списке и ни прямо, ни косвенно не упомянут в соответствующем черном списке.

В лесу доменов Windows все вышеперечисленные параметры интегрированы в групповую политику дерева доменов, что позволяет при необходимости централизованно управлять параметрами аутентификации всех компьютеров определенных подразделений корпоративной сети либо всей корпоративной сети в целом.

Выше была изложена стандартная схема идентификации и аутентификации пользователя в Windows, которая применяется при использовании стандартных провайдеров и пакетов аутентификации. Однако поскольку и провайдеры, и пакеты аутентификации являются заменяемыми

компонентами подсистемы аутентификации, администратор операционной системы может, установив нестандартный провайдер или пакет аутентификации, реализовать в Windows любую другую схему аутентификации. Для этого необходимо всего лишь разместить в системной директории Windows необходимые библиотеки и внести изменения в соответствующие ключи реестра.

Вопросы для самоконтроля

1. Что называется, защищенной операционной системой?
2. Какие подходы к построению защищенных операционных систем вы знаете?
3. Какие административные меры защиты вы знаете?
4. Какую политика безопасности называют адекватной?
5. Почему неограниченный рост защищенности операционной системы неизбежно приводит к снижению ее эксплуатационных качеств?
6. К каким негативным последствиям может привести поддержание чрезмерно высокого уровня защищенности системы?
7. Каковы основные этапы процесса формирования и поддержания адекватной политики безопасности операционной системы?
8. Когда заканчивается поддержание и коррекция адекватной политики безопасности?
9. С какими проблемами сталкиваются попытки количественного анализа рисков для тех или иных операционных систем?
10. Каковы роль и место стандартов безопасности в деле управления безопасностью операционной системы?
11. Что такое идентификация, аутентификация, авторизация?
12. Какие три основные схемы аутентификации вы знаете?
13. Каково важнейшее преимущество парольной аутентификации по сравнению с другими схемами?

14. Как должен храниться в операционной системе эталонный образ пароля, предназначенный для проверки пароля в ходе аутентификации?

15. Какие пароли являются самыми распространенными в мире?

16. Зачем нужно ограничивать сроки действия паролей?

17. Какие ограничения обычно накладываются на содержание паролей?

18. Каково важнейшее преимущество схемы аутентификации, основанной на внешних электронных носителях аутентификационных данных?

19. Почему при генерации ключей для внешних электронных носителей аутентификационных данных нельзя применять стандартные алгоритмы программной генерации псевдослучайных последовательностей?

20. Какие тесты можно применять для оценки качества случайной последовательности?

21. Какие методы получения истинно случайных последовательностей с помощью программных генераторов вы знаете?

22. Перечислите основные достоинства и недостатки протокола аутентификации Kerberos.

23. Какие ограничения на пароли пользователей могут применяться в Windows?

24. В каких ситуациях пользователь Windows обязан нажимать *Ctrl-Alt-Del* перед каждым вводом пароля на вход в систему?

25. Какие индивидуальные параметры аутентификации могут быть установлены для конкретного пользователя Windows?

26. Какие привилегии входа поддерживаются в Windows?

27. Как можно построить в Windows нестандартную схему аутентификации пользователя?

С О Д Е Р Ж А Н И Е

C O N T E N T

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Постановление Президента Республики Узбекистан от 14 мая 2018 года № ПП-3724. «О мерах по ускоренному развитию электронной коммерции»

2. Закон Республики Узбекистан от 11.12.2003 г. N 560-II. Об Информатизации.

3. Закон Республики Узбекистан от 11.12.2003 г. N 562-II. Об Электронной цифровой подписи

4. Ш.М. Мирзиёев. «Мы все вместе построим свободное, демократическое и процветающее государство Узбекистан». *Выступление на торжественной церемонии вступления в должность Президента Республики Узбекистан на совместном заседании палат Олий Мажлиса.* Мирзиёев Ш.М. - Ташкент: Ўзбекистон, 2016. - 56 с.

5. Ш.М. Мирзиёев. "Критический анализ, жесткая дисциплина и персональная ответственность должны стать повседневной нормой в деятельности каждого руководителя". *В книге приведен доклад Президента Республики Узбекистан Шавката Мирзиёева на состоявшемся 14 января текущего года расширенном заседании Кабинета Министров, посвященном итогам социально-экономического развития страны в 2016 году и важнейшим приоритетным направлениям экономической программы на 2017 год.* Ташкент: Ўзбекистон, 2017. - 104 с.

6. Ш.М. Мирзиёев. Обеспечение верховенства закона и интересов человека – гарантия развития страны и благополучия народа. *Доклад Президента Республики Узбекистан Шавката Мирзиёева на торжественном собрании, посвященном 24-й годовщине принятия Конституции Республики Узбекистан.* Ташкент: Ўзбекистон, 2017. - 48 с.

7. Ш.М. Мирзиёев. Свободное, демократическое и процветающее государство Узбекистан мы построим вместе с нашим мужественным и благородным народом. *Выступление Шавката Мирзиёева на торжественной церемонии вступления в должность Президента Республики*

Узбекистан на совместном заседании палат Олий Мажлиса. Ташкент: Ўзбекистон, 2017. - 488 с.

8. Указ Президента Республики Узбекистан. О стратегии действий по дальнейшему развитию Республики Узбекистан. Президент Республики Узбекистан Ш. МИРЗИЁЕВ. г. Ташкент, 7 февраля 2017 г., № УП-4947.

9. The InfoSec Handbook: An Introduction to Information Security 2014th Edition by Umesh Hodeghatta Rao.

10. Jaydip Sen. Cryptography and Security in Computing. InTech (March 07, 2012), 242 pages. eBook PDF files.

11. Darren Death. The Information Security Handbook. Packt Publishing - ebooks Account *(December 8, 2017)*. Paperback 330 pages, eBook PDF

12. John R. Vacca. Computer and Information Security Handbook, Third Edition 3rd Edition. Morgan Kaufmann Pub; 3 edition *(June 15, 2017)*. 1280 pages

13. Micki Krause, Harold F. Tipton. Handbook of Information Security Management. eBook Online, HTML, PDF files. 1080 pages.

14. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. CRC Press, 1999.-816 p.

15. А.А. Александров, М.П. Сычев. Организационно-правовое обеспечение информационной безопасности. - М.: Издательство МГТУ имени Н.Э. Баумана, 2018. - 291 с.

16. А.П. Алферов, и другие. Основы криптографии. Москва “Гелиос АРВ” 2002.

17. П.Н. Башлы. Информационная безопасность. Ростов-на-Дону «ФЕНИКС» 2006.

18. А. Бабаш, Е. Баранова, Д. Ларин. "Информационная безопасность. История защиты информации в России" *(2015)*

19. Е. Баранова, А. Бабаш. "Информационная безопасность и защита информации" 3-е изд. *(2016)*

20. В.В. Бондарев. "Введение в информационную безопасность автоматизированных систем" *(2016).*

21. А. Бирюков. "Информационная безопасность: защита и нападение" 2-е изд. *(2017)*

22. А.В. Бабаш, Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2016. - 136 с.

23. А.М. Блинов. Информационная безопасность. Учебное пособие. Часть 1./ Издательство: СПГУ, 2010. - 98с.

24. П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб, пос. для вузов / -М.: Радио и связь. - 1999.-168 с.

25. Ю.В. Вайнштейн и другие. Основы информационной безопасности. Красноярск 2007.

26. Ю.А. Гатчин, Е.В. Климова. Основы информационной безопасности. Санкт-Петербург. СПбГУ ИТМО, 2009 - 84 с.

27. В.А. Галатенко. Основы информационной безопасности. Интернет-Университет Информационных Технологий, www.intuit.ru, 2006

28. В.В. Гафнер. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2017. - 324 с.

29. Ю.Ю. Громов. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2017. - 384 с.

30. А.А. Гладких, В.Е. Дементьев. Базовые принципы информационной безопасности вычислительных систем./ Издательство: УлГТУ, 2009. - 168 с.

31. Л.Л. Ефимова. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2016. - 239 с.

32. С.В. Запечников. Информационная безопасность открытых систем. В 2-х т. Т.1 - Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. - М.: ГЛТ, 2017. - 536 с.

33. С.В. Запечников. Информационная безопасность открытых систем. В 2-х т. Т.2 - Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ, 2018. - 558 с.

34. В.И. Завгородний. Комплексная защита информации в компьютерных системах. Москва. Логос-2001

35. С.В. Запечников, и другие. Информационная безопасность открытых систем. Москва «Горячая линия-Телеком», 2006.

36. М.А. Иванов. Криптографические методы защиты информации в компьютерных системах и сетях. "КУДИЦ-ОБРАЗ" Москва 2001

37. В.П. Леонтьев. Безопасность в сети интернет. Москва ОЛМА Медиа Групп 2008.

38. А.А. Малюк. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. - М.: ГЛТ, 2016. - 280 с.

39. В.П. Мельников и другие. Информационная безопасность и защита информации. Москва Издательский центр «Академия», 2006

40. Т.С. Мельникова. Информационная безопасность. Саратов. СГСЭУ-2013.

41. Р.В. Мещеряков. Информационная безопасность и защита информации в сетях ЭВМ. Издательство Томского политехнического университета-2008.

42. Н.В. Макарова, В.Б. Волков. Информатика. «ООО» Издательство «Питер», 2011.

43. С.А. Нестеров. Информационная безопасность и защита информации. Санкт-Петербург Издательство Политехнического университета 2009

44. С.А. Нестеров. "Основы информационной безопасности" *(2016)*

45. Т.Л. Партыка. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2016. - 432 с.

46. С.В. Петров. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2016. - 296 с.

47. А.В. Пролетарский и другие. Технологии защиты информации в компьютерных сетях. ООО ИНТУИТ РУ. - 2016. - 369 с.

48. Проскурин Г.В. Криптография. Методы защиты информации в телекоммуникационных сетях //Connect! Мир связи. -1999. - №6-С.124-126.

49. Т.А. Пулко. Введение в информационную безопасность. Минск БГУИР-2016.

50. Ю. Родичев. "Нормативная база и стандарты в области информационной безопасности" (2017)

51. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. -М.: Радио и связь - 1999, 328 с.

52. В.А. Семененко. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2017. - 277 с.

53. Н. Скабцов. Аудит безопасности информационных систем. - СПб.: Питер, 2018. - 272 с.

54. А.Ф. Чипига. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2017. - 336 с.

55. В.Ф. Шаньгин. Защита информации и информационная безопасность. Часть I. Основы информационной безопасности. Симметричные криптосистемы: Учеб. пос. для вузов. М: МИЭТ -1999-140 с.

56. В.Ф. Шаньгин. Защита информации и информационная безопасность. Часть II. Асимметричные криптосистемы. Идентификация, аутентификация, электронная цифровая подпись и управление ключами: Учеб. пос. для вузов,-М.: МИЭТ, - 2000. -124 с.

57. В.Ф. Шаньгин. Информационная безопасность компьютерных систем и сетей. Москва ИД «ФОРУМ» - ИНФРА-М 2011.

58. А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. Безопасность операционных систем: учебное пособие / – М.: "Издательство Машиностроение-1", 2007 – 220 с.

ИНТЕРНЕТ-РЕСУРСЫ

1. Базовый стандарт организации беспроводных локальных сетей IEEE 802.11. http://standards.ieee.org/reading/ieee/std/Ianman/802.1 l-1999.pdf

2. Беляев А. В. Методы и средства защиты информации, http://www.citforum.ru/internet/infsecure/its2000_01.shtml

3. Касперский Е. Компьютерные вирусы, http://www.kaspersky.ru

4. Коротыгин С. Развитие технологии беспроводных сетей: стандарт IEEE 802.11. http://www.ixbt.com/comm/wlan.shtml.

5. Кузнецов С. Защита файлов в операционной системе UNIX. http://www.citforum.ru/database/articles/art_8.shtml.

6. Олифер Я.А., Олифер В.Г Сетевые операционные системы, Центр Информационных Технологий, http: //citforum. Ru / operating_systems /sos/ contents. shtml.

7. Семейство стандартов IEEE 802.11. HTTP: //www. wireless.ru /wireless/ wrl_base80211

8. Скородумов Б.И. Стандарты для безопасности электронной коммерции в сети Интернет, http://www.stcarb.comcor.ru

9. Advanced Encryption Standard *(AES)* Development Effort. February 2001 //csrc.nist.gov/CryptoToolkit/aes/index2.html

10. Daemen J., Rijmen V. AES Proposal: Rijndael. Document version 2. September 1999 I j www.esat.kuleuven.ac.be/~rijmen/rijndael

11. Dierks T., Allen C. RFC 2246: The TLS Protocol Version 1.0. January 1999 //www.ietf.org/rfc/rfc2246.txt

12. FIPS Publication 197. Announcing the Advanced Encryption Standard *(AES)*. November, 2001 //csrc.nist.gov/publications/fips/ fipsl97/fips-197 .pdf.

Список использованных сокращений

АС	Автоматизированная система
ACL	Access Control List – список
АИС	Автоматизированные
АЛУ	Арифметико-логическое устройство
АТС	Автоматическая телефонная станция
БД	База данных
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
ГПСЧ	Генератор псевдослучайных чисел
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОК	Открытый ключ
ОС	Операционная система
ОО	Объект оценки
ПО	Программное обеспечение
ПБ	Программное безопасность
СЗИ	Система защиты информации
СК	Секретный ключ
СУИБ	Системы управления информационной безопасностью
СУБД	Система управления базами данных
ЭЦП	Электронная цифровая подпись
SPI	Security Parameter Index – индекс параметров защиты
DES	Data encryption standard
DOS	Denied of Service – отказ в обслуживании
VPN	Виртуальная частная сеть

Г Л О С С А Р И Й

Название термина на русском языке	The terminology of the English language	Объяснение термина
Абонентское шифрование *(информации)*	*Subscriber encryption (information)*	Способ шифрования, при котором за шифрование данных осуществляется в системе абонента - получателя.
Абонентское шифрование *(оконечное)*	*Subscriber encryption (terminal)*	Защита информации, передаваемой средствами телекоммуникаций криптографическими методами, непосредственно между отправителем и получателем.
Абстрактное представление данных	*Abstract representation of data*	Принцип определения типа данных через операции, которые могут, выполняться над объектами данного типа. При этом вводятся следующие ограничения: значения объектов могут модифицироваться и наблюдаться только путем использования этих операций
Автоматизированная информационная система, ***АИС***	*Automated information system (AIS)*	Совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений.
Автоматический контроль *(встроенный контроль)*	*Automatic check (builtin check)*	Контроль, выполняемый автоматически аппаратными средствами.
Авторизация	*Authorization*	Предоставление доступа пользователю, программе или процессу.
Авторизация данных	*Data authorization*	Определение и установление степени приватности данных в базе данных.
Авторизация программы	*Program authorization*	Установление ограничения на доступ к системной или пользовательской программе со стороны других программ и пользователей.
Авторское право	*Copyright*	Совокупность правовых норм (раздел гражданского права), которые регулируют отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнения, постановок, передач организаций эфирного или кабельного вещания.
Администратор базы данных	*Data administrator*	Специальное должностное лицо *(группа лиц)*, имеющий полное представление о базе данных и отвечающее за ее ведение, использование и развитие. Входит в состав администрации банка данных.

Администратор доступа	*Access administrator*	Одно из должностных лиц в составе администрации банка данных, отвечающее за организацию доступа пользователей к базам данных.
Администратор защиты	*Security administrator*	Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.
Администратор системы *(системный администратор)*	*System administrator*	Лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии
Администратор службы безопасности	*The administrator of the security service*	Человек (или группа людей), имеющий полное представление об одной или нескольких системах обеспечения безопасности и контролирующий проектирование и их использование.
Администрация системы	*System administration*	Пользователь сети, деятельность которого связана с управлением системами.
Активная угроза	*Active threat*	Угроза преднамеренного несанкционированного изменения состояния системы.
Активность защиты	*Protection activity*	Принцип защиты, выражающийся в целенаправленном навязывании техническим разведкам ложного представления об объекте в соответствии с замыслом защиты, а также подавление возможностей технической разведки.
Акустическая защита выделенного помещения	*Acoustic protection of a dedicated room*	Процесс реализации запланированного комплекса организационно - технических мероприятий по предотвращению утечки речевой секретной или конфиденциальной информации за пределы выделенного помещения путем прямого проникновения звука через ограждающие конструкции.
Алгоритм	*algorithm*	Упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов
Алгоритм шифрования	*Encryption algorithm*	Набор математических правил, определяющих содержание и последовательность операций, зависящих от ключевой переменной (ключ шифрования), по преобразованию исходной формы представления информации (открытый текст) к виду, обладающему секретом обратного преобразования *(зашифрованный текст).*
Анализ риска	*Risk analysis*	Процесс изучения характеристик и слабых сторон системы, проводимый с использованием вероятностных расчетов, с целью определения ожидаемого ущерба в случае возникновения неблагоприятных событий. Задача анализа риска состоит в определении степени приемлемости того или иного риска в работе системы.
Антивирус	*Antivirus*	Программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус

		удалить не, удается, то зараженная программа уничтожается.
Аппаратная защита	*Hardware security*	Использование аппаратных средств, например, регистров границ или замков и ключей для защиты данных в ЭВМ
Аппаратное средство защиты информации	*Hardware means of information security*	Специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.
Асимметричный шифр	*Asymmetric cipher*	Шифр, в котором ключ шифрования не совпадает с ключом дешифрирования.
Атака	*Attack*	Нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой.
Аутентификация	*Authenticate*	Проверка идентификации пользователя (проверка подлинности), устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.
Безопасная операционная система	*Secure operating system*	Операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой.
Безопасность	*Safety (security)*	Свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение.
Безопасность автоматизированной информационной системы	*Automated information system security*	Совокупность мер управления и контроля, защищающая APIS от отказа в обслуживании и несанкционированного (умышленного или случайного) раскрытия, модификации или разрушения АИС и данных.
Безопасность информации	*Information security*	Состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение.
Безопасность информации в ИС	*The security of the information in the IP*	Защищенность информации и оборудования ИС от факторов, представляющих угрозу для: конфиденциальности (обеспечение санкционированного доступа); целостности; доступности.
Безопасность информационной сети	*Network security*	Меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.

Безопасность информационной системы	*Information system security*	Свойство информационной системы противостоять попыткам несанкционированного доступа. Совокупность элементов, необходимых для обеспечения адекватной защиты компьютерной системы; включает аппаратные и / или программные функции, характеристики и средства; операционные и учетные процедуры, средства управления доступом на центральном компьютере, удаленных компьютерах и телекоммуникационных средствах; административные мероприятия, физические конструкции и устройства; управление персоналом и коммуникациями.
Безопасность компьютерных систем	*Computer security*	Свойство компьютерных систем противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, и навязыванию ложной информации.
Безопасность связи	*Communication security*	Свойство систем связи противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, навязыванию ложной информации.
Безопасность, информационная общества	*Security, information security*	То же, что и "безопасность, информационная личности" применительно к организованному коллективу людей и к обществу в целом.
Биометрические данные	*Biometric data*	Средства аутентификации, представляющие собой такие личные отличительные признаки пользователя как тембр голоса, форма кисти руки, отпечатки пальцев и т.д., оригиналы которых в цифровом виде хранятся в памяти ЭВМ.
Бит *(двоичный код)*	*Bit*	Минимальная единица количества информации в ЭВМ, равная одному двоичному разряду.
Бит защиты	*Protection bit*	Двоичный разряд в ключе памяти, устанавливающий защиту соответствующего блока памяти от записи либо от выборки и записи.
Блокирование информации	*The blocking of information*	Утрата информацией при ее обработке техническими средствами свойства доступности, выражающаяся в затруднении или прекращении санкционированного доступа к ней для проведения санкционированных операций по ознакомлению, документированию, модификации или уничтожению.
Брандмауэр	*Firewall*	Метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами.
Браузер	*Web browser*	Клиентская программа для работы в WWW.
Взвешенный код	*Weighted code*	Блочный код, в котором каждой позиции символа в закодированном слове присваивается определенный вес.

Восстанавливаемая система	*Recovery system*	Система, допускающая ремонт в процессе выполнения своих функций.
Восстановление	*Recovery (regeneration)*	Возврат к исходному значению или к нормальному функционированию. 2) Процесс, с помощью которого станция передачи данных разрешает конфликт или исправляет ошибки, возникающие при/передаче данных.
Встроенный дешифратор	*Onchip decoder*	Дешифратор, расположенный на одном и том же кристалле с запоминающей матрицей.
Вторичный индекс	*Secondary index*	Индекс для вторичных ключей
Гамма шифра	*Gamma of cipher*	Псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для за шифрования открытой информации и рас шифрования зашифрованной.
Гаммирование	*Gamming*	Процесс наложения по определенному закону гаммы шифра на открытые данные.
Гарантия защиты	*Security accredidation*	Наличие сертификата соответствия для технического средства обработки информации или аттестата на объект информатики, подтверждающих, что безопасность обрабатываемой информации соответствует требованиям стандартов и других нормативных документов.
Главный пароль	*Master password*	Корневое слово, являющееся общим для определенного набора паролей. 2) Пароль, предназначенный для защиты каталога паролей.
Государственная тайна	*State secret*	Сведения, охраняемые государством, разглашение которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала страны или повлечь другие тяжкие последствия для ее обороноспособности, государственной безопасности, экономических и политических интересов. К государственной тайне относится секретная информация с грифами "особой важности" и "совершенно секретно".
Дескриптор	*Descriptor*	Описатель, элемент информационной структуры объекта, указывающий, в каком виде запоминается та или иная информация (например, в массиве записи или файле). Обратившись к дескриптору, программа получает возможность интерпретировать характеризуемые им данные.
Дешифратор *(декодер)*	*Decjder*	Логическая схема, преобразующая n разрядное входное двоичное слово (код, шифр) в единичный сигнал на одном из 2n выходов этой схемы. Обратную функцию выполняет шифратор.
Дешифратор адреса	*Address decoder*	Преобразователь адреса в управляющие сигналы, направляемые запоминающему устройству.
Дешифрование	*Decipherement*	Операция, обратная шифрованию и связанная с восстановлением исходного текста из зашифрованного.

Диагностика	*Diagnostics*	Контроль, проверка и прогнозирование состояния объектов. Цель технической диагностики обнаружение неисправностей и выявление элементов, ненормальное функционирование которых является причиной возникновения неисправностей.
Диагностика ошибок	*Error diagnostics*	Поиск места ошибки в программе, установление характера и причин возникновения ошибки и определение мер по ее устранению. При обнаружении ошибки выдается диагностическое сообщение.
Доверительность	*Trusted funcionality*	Свойство соответствия безопасности некоторым критериям.
Домен безопасности	*Secyrity domain*	Ограниченная группа объектов и субъектов безопасности, к которым применяется одна методика безопасности со стороны одного и того же администратора безопасности.
Достоверность	*Validity, adequacy*	Свойство информации быть правильно воспринятой; вероятность отсутствия ошибок.
Доступ	*Access*	Предоставление данных системе обработки данных или получение их из нее путем выполнения операций поиска, чтения и *(или)* записи данных.
Доступ к информации	*Access to information*	Процесс ознакомления с информацией, ее документирование, модификация или уничтожение, осуществляемые с использованием штатных технических средств.
Зависание системы	*System quiescing*	Останов *(замораживание)* мультипрограммной системы путем подавления ввода новых заданий.
Законодательство о защите данных	*Data protection legislation*	Законодательство, принятое или принимаемое во всех странах для защиты персональных данных, обрабатываемых компьютерами. Цель законодательства заключается в контроле и предотвращении неправильного использования информации в случае, когда персональные данные хранятся в компьютере.
Закрытая информация	*Private information*	Информация, которая по тем или иным соображениям представляет тайну и распространение которой возможно лишь с согласия органов, уполномоченных контролировать вопросы, связанные е этой информацией.
Зашифрованные данные	*Cipher data*	Информация, хранящаяся в памяти ЭВМ в зашифрованном виде, т.е. данные, к которым применен способ криптографической защиты.
Зашифрованный текст	*Ciphertext*	Результат за шифрования исходного открытого текста, осуществляемого с целью сокрытия его смысла.
Защита	*Protection, security, lock out*	Средство для ограничения доступа или использования всей или части вычислительной системы; юридические, организационные и

		технические, в том числе программные, меры предотвращения несанкционированного доступа к аппаратуре, программам и данным.
Защита данных	*Data protection*	Охрана данных от несанкционированного, умышленного или случайного их раскрытия, модификации или уничтожения
Защита информации	*Information protection*	Включает в себя комплекс мероприятий, направленных на обеспечение информационной безопасности. На практике под этим понимается поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.
Защита от записи	*Writeprotect*	Способ защиты информации на диске и / или в оперативной памяти, заключающийся в установке ключей защиты или в заклеивании метки считывания на диске, что предотвращает запись новых данных и сохраняет имеющиеся от разрушения.
Защита от несанкционированного доступа	*Protection from unauthorized access*	Предотвращение или существенное затруднение несанкционированного доступа к программам и данным путем использования аппаратных, программных и криптографических методов и средств защиты, а также проведение организационных мероприятий. Наиболее распространенным программным методом защиты является система паролей.
Защита паролем	*Password protection*	Способ защиты данных, при котором для получения доступа к ним необходимо ввести пароль.
Защита системы	*System security*	Совокупность мер, предпринимаемых для исключения несанкционированного доступа к программам и данным системы или случайного вмешательства в ее работу.
Злоумышленник	*Intruder*	Лицо или организация, заинтересованные в получении несанкционированного доступа к программам или данным, предпринимающие попытку такого доступа или совершившие его.
Идентификатор	*Identifier*	Средство идентификации доступа, представляющее собой отличительный признак субъекта или объекта доступа. Основным средством идентификации доступа для пользователей является пароль.
Идентификатор доступа	*Access identifier*	Уникальный признак субъекта или объекта доступа.
Идентификация	*Identification*	Присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Имитация	*Imitation*	Составная часть технической дезинформации, осуществляемая путем искусственного

		воспроизведения ложных объектов и технических демаскирующих признаков.
Имитация экрана	*Screen mimic*	Маскировка экрана, обычно связана с высвечиванием ничего не подозревающему пользователю ложного экрана опроса для перехвата его имени и пароля.
Информатизация	*Informatization*	Организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.
Информационная безопасность	*Information security*	Это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры
Информационная система	*Information system*	Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.
Информационные процессы	*Information process*	Процессы сбора, обработки, накопления, хранения, поиска и распространения информации.
Информация	*Information*	Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
Канал утечки информации	*Covert channel*	Канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.
Категория защиты	*Security classification*	Классификация доступности информации, например, "секретная информация" или "медицинская информация только для врачей".
Ключ *(шифрования)*	*Encryption key*	Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.
Ключ	*Key*	Совокупность знаков, используемая для идентификации записей в файле и быстрого доступа к ней.
Компьютерный вирус	*Computer virus*	Программа, которая обладает следующими свойствами: возможностью копирования себя в другие файлы, диски, ЭВМ; возможностью выполнения без явного вызова; возможностью осуществления несанкционированного доступа к

		информации; возможностью маскировки от попыток обнаружения.
Конфиденциальная информация	*Sensitive information*	Информация, требующая защиты.
Конфиденциальность	*Confidentiality*	Некоторый класс данных, получение либо использование которых неавторизованными для этого лица ми может стать причиной серьезного ущерба для организации.
Криптоанализ	*Criptoanalysis*	Изучение системы защиты сообщений и/или исследование ее входных и выходных сообщений с целью выделить скрытые переменные или истинные данные, включая исходный текст.
Криптографическая защита	*Cryptosecurity (criptographical security)*	Защита информации путем осуществления ее криптографического преобразования.
Криптографическая система	*Cryptosystem*	Совокупность технических и /или программных средств, организационных методов, обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей.
Криптографический ключ	*Cryptology key*	Последовательность символов, обеспечивающая возможность шифрования и дешифрования.
Криптография	*Cryptography*	Принципы, средства и методы преобразования информации к непонятному виду, а также восстановления информации к виду, пригодному для восприятия.
Лицензия	*License*	Разрешение на право продажи или предоставления услуг.
Маска	*Mask*	Местный предмет или защитное сооружение, предназначенное для скрытия (маскировки) объекта защиты от визуально-оптических и фотографических средств технической разведки, а также от всех видов локации *(пеленгации).* Маски подразделяются на естественные *(лес, кустарник, строения, неровности рельефа и т.д.)* и искусственные *(инженерные сооружения, системы).*
Нумерационное кодирование	*Enumerative coding*	Представление последовательности сообщений источника последовательностью целых чисел.
Объект безопасности	*Security object*	Пассивная системная составляющая, к которой применяется методика безопасности.
Объект защиты	*Object of protection*	Обобщающий термин для всех форм существования информации, требующих защиты от технических разведок. По своему составу объекты защиты могут быть единичными и групповыми.
Пароль	*Password*	Средство идентификации доступа, представляющее собой кодовое слово в буквенной, цифровой или буквенно-цифровой форме, которое вводится в ЭВМ перед началом диалога с нею с

		клавиатуры терминала или при помощи идентификационной /кодовой/ карты.
Патент	*Patent*	Гарантия со стороны правительства, данная изобретателю или его доверенному лицу и дающая привилегию в виде исключительного права на реализацию, использование или продажу изобретения в течение определенного срока
Политика безопасности	*Security policy*	Набор законов, правил и практического опыта, на основе которых строится управление, защита и распределение критичной информации.
Правовая форма защиты информации	*Legal form of protection of the information*	Защита информации, базирующаяся на применении статей конституции и законов государства, положений гражданского и уголовного кодексов и других нормативно-правовых документов в области информатики, информационных отношений и защиты информации. Правовая форма защиты информации регламентирует права и обязанности субъектов информационных отношений, правовой статус органов, технических средств и способов защиты информации и является базой для создания морально-этических норм в области защиты информации.
Риск	*Risk*	Возможность проведения захватчиком успешной атаки в отношении конкретной слабой стороны системы.
Самоконтроль	*Selfchecking*	Способность системы автоматически контролировать процесс своего функционирования и определенным образом реагировать на возникновение отказов.
Санкционирование	*Authorization*	Предоставление права пользования услугами системы, например, права доступа к данным.
Скрытый канал	*Covert channel*	Путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким способом, который нарушает системную политику безопасности.
Служба безопасности	*Security service*	Совокупность должностных лиц и технических средств, обеспечивающая защиту систем связи и передаваемых данных.
Угроза безопасности информации	*The threat to information security*	Потенциальная возможность нарушения основных качественных характеристик *(свойств)* информации при ее обработке техническими средствами: секретности /конфиденциальности/, целостности, доступности.
Управление доступом	*Access control*	Определение и ограничение доступа пользователей, программ и процессов к данным, программам и устройствам вычислительной системы.
Управление информационной безопасностью	*Information security management*	Способ обеспечения информационной безопасности путем использования механизмов обеспечения ЗИ.

Утечка информации	*Information loss*	Неконтролируемое распространение информации, которое привело (может привести) к ее несанкционированному получению.
Уязвимость	*Vulnerability*	Свойство системы, которое может привести к нарушению ее защиты при наличии угрозы. Уязвимость может возникать случайно из-за неадекватного проектирования или неполной отладки или может быть результатом злого умысла.
Цифровая подпись	*Digital signature*	Дополнительная информация, предоставляемая источником для обеспечения аутентификации. Последовательность данных, добавляемая к блоку данных или к результату его криптографического преобразования, которая позволяет получателю данных проверить источник и целостность блока данных, а также защиту от подлога или подделки.
Человек	*Person*	Форма существования информации, обусловленная свойством человека накапливать и хранить в своем сознании *(памяти*) смысловую информацию, а при необходимости выдавать ее другому человеку или техническому устройству. Выдача человеком информации происходит устно при разговоре, письменно в виде документа или путем передачи изделий различного назначения.
Шифр	*Cipher*	Совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключа.
Шифрование *(информации)*	*Ncryption (information)*	Процесс за шифрования или рас шифрования информации.
Шифрование с открытым ключом	*Public key cryptography*	Криптографический метод, в котором используются раздельные ключи для шифрования и дешифрования.
Экспертиза системы защиты информации	*Examination of information security system*	Оценка соответствия представленных проектных материалов по защите информации *(на объекте)* поставленной цели, требованиям стандартов и других нормативных документов.
Экспертная система	*Expert system*	Комплекс программных средств, в основу которого положена интерпретация правил, аккумулирующих знания экспертов по определенной специальности.
Эффективность защиты информации	*information techmical protection efficiency*	Степень соответствия достигнутого уровня защищенности информации поставленной цели.
Ядро защиты	*Security kernel*	Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.