

**ЎЗБЕКИСТОН АЛОҚА ВА
АХБОРОТЛАШТИРИШ
АГЕНТЛИГИ**

**ТОШКЕНТ АХБОРОТ
ТЕХНОЛОГИЯЛАРИ
УНИВЕРСИТЕТИ**

**Ганиев Салим Каримович, Каримов Мажид Маликович,
Ташев Комил Ахматович**

АХБОРОТ ХАВФСИЗЛИГИ

(Ахборот-коммуникацион тизимлар хавфсизлиги)

**Техника фанлари доктори, профессор С.С. Қосимов
умумий таҳрири остида**

Ўзбекистон Республикаси

*Олий ва ўрта махсус таълим вазирлиги томонидан
техника олий ўқув юртлари бакалавриат босқичи
талабалари учун ўқув қўланма сифатида тавсия
этилган*

Ганиев Салим Каримович, Каримов Мажид Маликович, Ташев Комил Ахматович. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма Т., «Алоқасҳи», 2008, 382 бет.

Ушбу қўлланма компьютер тармоқлари ва корпоратив ахборот тизимларини яратишда ва ишлатишда ахборотни химоялашнинг долзарб муаммоларига бағишланган. Компьютер тармоқлари ва тизимларига таҳдид хиллари ҳамда локал ва корпоратив тармоқларни Internet-атакалардан химоялаш усуллари ва воситалари муҳокама этилади. Электрон бизнес ва электрон тижоратда ахборот хавфсизлигини таъминлаш муаммосига алоҳида эътибор берилади. Ахборот хавфсизлиги концепцияси таърифланади ва тармоқларда хавфсизлик сиёсати аниқланади.

Маълумотларни химоялаш технологияси, тармоқ хавфсизлигининг базавий технологияси, сукилиб киришларни ва тармоқ хавфсизлигини бошқариш таҳлилланади. Хусусан, ахборотни замонавий криптографик химоялаш воситаларининг принциплари, алгоритмлари ва протоколлари кўрилади; тармоқлараро экранларнинг турли хиллари тавсифланади ва уларни ишлатиш бўйича тавсиялар берилади; Internet хилидаги глобал очик тармоқларнинг очик коммуникациялари орқали криптохимояланган виртуал туннелларни шакллантириш усуллари ва воситалари муҳокама этилади; корхона ахборот ресурсларидан масофадан хавфсиз фойдаланишни таъминлаш масалалари кўрилади: маълумотларни узатиш тармоғида ахборотни химоялаш масалалари ва уларни ечиш йўллари тавсифланади: симсиз тармоқ концепцияси, симсиз тармоқ хавфсизлигига таҳдидлар, симсиз тармоқ хавфсизлиги муаммоси баён этилади; тармоқ хавфсизлигини бошқариш усуллари ва воситалари таҳлилланади.

Хавф-хатарларни таҳлиллаш ва бошқариш асосида корхона ахборот хавфсизлиги тизимини куриш методологияси таърифланади.

Қўлланма олий ўқув юртлари талабаларига, ахборот технологиялари, компьютер тизимлари соҳасида фаолият кўрсатувчиларга мўлжалланган.

Данное пособие посвящено актуальным проблемам защиты информации при создании и использовании компьютерных сетей и корпоративных информационных систем. Обсуждаются виды атак на компьютерные сети и системы, а также методы и средства защиты локальных и корпоративных сетей от удаленных Internet-атак. Особое внимание уделяется проблемам обеспечения информационной безопасности электронного бизнеса и электронной коммерции. Формулируется концепция информационной безопасности и определяется политика безопасности в сетях.

Анализируются технологии защиты данных, базовые технологии сетевой безопасности, обнаружения вторжений и управления сетевой безопасностью. В частности, рассматриваются принципы, алгоритмы и протоколы современных криптографических средств защиты информации; описываются различные типы межсетевых экранов и даются рекомендации по их использованию; обсуждаются методы и средства формирования криптозащищенных виртуальных туннелей через открытые коммуникации глобальных открытых сетей типа Internet; рассматриваются вопросы обеспечения удаленного доступа к информационным ресурсам предприятия; описываются задачи защиты информации в сетях передачи данных и пути их решения; излагаются концепция беспроводной сети, угрозы на безопасность беспроводной сети, проблемы безопасности беспроводной сети; анализируются методы и системы управления сетевой безопасностью.

На основе анализа и управления рисками, формулируется методология построения системы информационной безопасности предприятия.

Пособие рассчитано на студентов высших учебных заведений, а также лицам, занимающимся в области информационной технологий и компьютерных систем.

The given manual is devoted to actual problems of protection of the information at creation and use of computer networks and corporate information systems. Kinds of attacks to computer networks and systems, and also methods and means of protection of local and corporate networks from the removed Internet-attacks are discussed. The special attention is given problems of maintenance of information safety of electronic business and electronic commerce. The concept of information safety is formulated and the politics of safety in networks is determined.

Technologies of protection of data, base technologies of network safety, detection of intrusions and managements of network safety are analyzed. In particular, principles, algorithms and reports of modern cryptographic means of protection of the information are considered; various types of gateway screens are described and recommendations on their use are given; methods and means of formation cryptoprotection virtual tunnels through the open communications of the global open networks of type Internet are discussed; questions of maintenance of the removed access to information resources of the enterprise are considered; problems of protection of the information in networks of data transmission and a way of their decision are described; the concept of a wireless network, threat on safety of a wireless network, a problem of safety of a wireless

network are stated; methods and control systems of network safety are analyzed.

On the basis of the analysis and management of risks, the methodology of construction of system of information safety of the enterprise is formulated.

The manual is calculated on students of higher educational institutions, and also to the persons who are engaged in the field of information technologies and computer systems.

Тақризчилар: **акад. Бекмуратов Т.Ф.** – Замонавий ахборот технологиялари ИТМ, «Алгоритм-инжиниринг» ИТИ етакчи илмий ходими, т.ф.д., проф;
проф. Орипов М.М. – Мирзо Улуғбек номи Ўзбекистон Миллий университети «Информатика ва татбикий дастурлаш» кафедраси мудири, физика-математика фанлари доктори.

ISBN 978-9943-326-20-0

© «ALOQACHI», 2008

МУҚАДДИМА	14
<i>I боб. АХБОРОТ ХАВФСИЗЛИГИГА ТАҲДИДЛАР</i>	
1.1. Ахборот урушлар ва киберхужумлар	17
1.2. Ахборот-коммуникацион тизимлар ва тармоқларда таҳдидлар ва заифликлар	22
1.3. Компьютер жиноятчилигининг таҳлили	25
1.4. Тармоқдаги ахборотга бўладиган намунавий ҳужумлар ..	28
1.5. Ахборот хавфсизлигини бузувчининг модели	32
1.6. Internet – хизматлар ва электрон бизнес тизимларида хавфсизлик-муаммолари	36
<i>II боб. АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ АСОСИЙ ЙЎЛЛАРИ</i>	
2.1. Ахборотни ҳимоялаш концепцияси	43
2.2. Ахборот ҳимоясининг стратегияси ва архитектураси	46
2.3. Ахборот хавфсизлигининг сиёсати	48
2.4. Ахборот-коммуникацион тизимлар ва тармоқлар хавфсизлигига қўйиладиган талаблар	53
<i>III боб. АХБОРОТ ХАВФСИЗЛИГИНИНГ ҲУҚУҚИЙ ВА ТАШКИЛИЙ ТАЪМИНОТИ</i>	
3.1. Ахборот хавфсизлиги соҳасида ҳуқуқий бошқариш	59
3.2. Ахборот хавфсизлигининг ташкилий-маъмурий таъминоти	61
3.3. Ахборот хавфсизлиги бўйича стандартлар ва спецификациялар	65
<i>IV боб. АХБОРОТНИ ҲИМОЯЛАШНИНГ КРИПТОГРАФИК УСУЛЛАРИ</i>	
4.1. Криптографиянинг асосий коидалари ва таърифлари	71
4.2. Симметрик шифрлаш тизими	74
4.3. Асимметрик шифрлаш тизимлари	89
4.4. Шифрлаш стандартлари	92
4.5. Хэшлаш функцияси	99
4.6. Электрон рақамли имзо	102
4.7. Криптографик калитларни бошқариш	107
<i>V боб. ИНДЕНТИФИКАЦИЯ ВА АУТЕНТИФИКАЦИЯ</i>	
5.1. Асосий тушунчалар ва туркумланиши	115
5.2. Пароллар асосида аутентификациялаш	120
5.3. Сертификатлар асосида аутентификациялаш	125
5.4. Қатъий аутентификациялаш	128

5.5. Фойдаланувчиларни биометрик идентификациялаш ва аутентификациялаш	147
VI боб. ТАРМОҚЛАРАРО ЭКРАН ТЕХНОЛОГИЯСИ	
6.1. Тармоқлараро экранларнинг ишлаш хусусиятлари	153
6.2. Тармоқлараро экранларнинг асосий компонентлари	163
6.3. Тармоқлараро экранлар асосидаги тармоқ химоясининг схемалари	174
VII боб. ҲИМОЯЛАНГАН ВИРТУАЛ ХУСУСИЙ ТАРМОҚЛАР	
7.1. Ҳимояланган виртуал хусусий тармоқларни куриш концепцияси	185
7.2. Ҳимояланган виртуал хусусий тармоқларнинг туркумланиши	193
7.3. Ҳимояланган корпоратив тармоқларни куриш учун VPN ечимлар	203
7.4. Канал ва сеанс сатҳларда химояланган виртуал каналларни куриш	220
7.5. IPSec протоколлар стекини химояланган виртуал хусусий тармоқлар куришда ишлатилиши	245
VIII боб. ОЧИҚ КАЛИТЛАРНИ БОШҚАРИШ ИНФРАТУЗИЛМАСИ РКІ	
8.1. РКІнинг ишлаш принципи	255
8.2. Очiq калитларни бошқариш инфратузилмасининг мантиқий тузилмаси ва компонентлари	265
IX боб. АХБОРОТ-КОММУНИКАЦИОН ТИЗИМЛАРДА СУҚИЛИБ КИРИШЛАРНИ АНИҚЛАШ	
9.1. Хавфсизликни адаптив бошқариш концепцияси	271
9.2. Ҳимояланишни таҳлиллаш	275
9.3. Хужумларни аниқлаш	279
9.4. Компьютер вируслари ва вирусдан химояланиш муаммолари	288
9.5. Вирусга қарши дастурлар	297
9.6. Вирусга қарши химоя тизимини куриш	305
X боб. МАЪЛУМОТЛАРНИ УЗАТИШ ТАРМОҒИДА АХБОРОТНИ ҲИМОЯЛАШ	
10.1. Маълумотларни узатиш тармоқларида ахборот химоясини таъминлаш	309
10.2. Алоқа каналларида маълумотларни химоялаш усуллари	312

**XI боб. СИМСИЗ АЛОҚА ТИЗИМЛАРИДА АХБОРОТ
ҲИМОЯСИ**

11.1. Симсиз тармоқ концепцияси ва тузилмаси	317
11.2. Симсиз тармоқлар хавфсизлигига таҳдидлар	327
11.3. Симсиз тармоқлар хавфсизлиги протоколлари	337
11.4. Симсиз қурилмалар хавфсизлиги муаммолари	342

**XII боб. ХАВФСИЗЛИКНИ БОШҚАРИШ ВА ҲИМОЯ
ТИЗИМИНИ ҚУРИШ**

12.1. Бошқаришнинг функционал масалалари	347
12.2. Хавфсизлик воситаларини бошқариш архитектураси ...	351
12.3. Ахборот тизимларининг аудити ва мониторинги.....	356
12.4. Хавф-хатарларни таҳлиллаш ва бошқариш	363
12.5. Ахборот хавфсизлиги тизимини қуриш методологияси..	368
ФЙДАЛАНИЛГАН АДАБИЁТЛАР	375
ҚИСҚАРТИРИЛГАН СЎЗЛАР	378

ПРЕДИСЛОВИЕ	14
<i>I глава. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</i>	
1.1. Информационные войны и кибератаки	17
1.2. Угрозы и уязвимости в информационно-коммуни- кационных системах и сетях	22
1.3. Анализ компьютерной преступности	25
1.4. Типовые атаки на информацию в сети	28
1.5. Модель нарушителя информационной безопасности	32
1.6 Проблемы безопасности в Internet-услугах и системах электронного бизнеса	36
<i>II глава. ОСНОВНЫЕ ПУТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</i>	
2.1. Концепция защиты информации	43
2.2. Стратегия и архитектура защиты информации	46
2.3. Политика безопасности информации	48
2.4. Условия безопасности информационно- коммуникационных систем и сетей	53
<i>III глава. ПРАВОВОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ</i>	
3.1. Правовое управление в сфере информационной безопасности	59
3.2. Организационно-административное обеспечение информационной безопасности	61
3.3. Стандарты и спецификации по информационной безопасности	65
<i>IV глава. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ</i>	
4.1. Основные правила и определения криптографии	71
4.2. Симметричные системы шифрования	76
4.3. Асимметричные системы шифрования	89
4.4. Стандарты шифрования	92
4.5. Функция хэширования	99
4.6. Электронная цифровая подпись	102
4.7. Управление криптографическими ключами	107
<i>V глава. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ</i>	
5.1. Основные понятия и классификация	115
5.2. Аутентификация на основе паролей	120
5.3. Аутентификация на основе сертификатов	125

5.4. Строгая аутентификация	128
5.5. Биометрическая идентификация и аутентификация пользователей	147
<i>VI глава. ТЕХНОЛОГИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ</i>	
6.1. Особенности функционирования межсетевых экранов	153
6.2. Основные компоненты межсетевых экранов	163
6.3. Схема защиты сети на базе межсетевых экранов	174
<i>VII глава. ЗАЩИЩЕННЫЕ ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ</i>	
7.1. Концепция построения защищенных виртуальных частных сетей	185
7.2. Классификация защищенных виртуальных частных сетей	193
7.3. Решения для построения защищенных виртуальных частных сетей VPN.....	203
7.4. Построение защищенных виртуальных частных сетей в канальном и сеансовом уровнях.....	220
7.5. Использование стека IPSec протокола при построении защищенных виртуальных частных сетей	245
<i>VIII глава. ИНФРАСТРУКТУРА УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ РКІ</i>	
8.1. Принцип функционирования РКІ.....	255
8.2. Логическая структура и компоненты инфраструктуры управления открытыми ключами.....	265
<i>IX глава. ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ</i>	
9.1. Концепция адаптивного управления безопасностью ...	271
9.2. Анализ защищенности	275
9.3. Обнаружение атак.....	279
9.4. Компьютерные вирусы и проблемы антивирусной защиты.....	288
9.5. Антивирусные программы.....	297
9.6. Построение системы антивирусной защиты	305
<i>X глава. ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ</i>	
10.1. Обеспечение защиты информации в сетях передачи данных	309
10.2. Методы защиты данных в каналах связи	312

*XI глава. ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ
БЕСПРОВОДНОЙ СВЯЗИ*

11.1. Концепция и структура беспроводной сети.....	317
11.2. Угрозы безопасности беспроводной сети.....	327
11.3. Протоколы безопасности беспроводной сети.....	337
11.4. Проблемы безопасности беспроводных устройств.....	342

*XII глава. УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ И
ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ*

12.1. Функциональные задачи управления.....	347
12.2. Архитектура управления средствами безопасности...	351
12.3. Аудит и мониторинг информационных систем	356
12.4. Анализ и управление рисками	363
12.5. Методология построения системы информационной безопасности.....	368
ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА	375
СПИСОК СОКРАЩЕНИЙ	378

CONTENTS

INTRODUCTION	14
<i>I chapter. THREATS OF INFORMATION SAFETY</i>	
1.1. Information wars and cyberattacks	17
1.2. Threats and vulnerability in information-communication systems and networks	22
1.3. The analysis of computer criminality	25
1.4. Typical attacks to the information in a network.....	28
1.5. Model of the infringer of information safety	32
1.6 Problems of safety in Internet-services and systems of electronic business.	36
<i>II chapter. THE BASIC WAYS OF MAINTENANCE OF INFORMATION SAFETY</i>	
2.1. The concept of protection of the information	43
2.2. Strategy and architecture of protection of the information	46
2.3. Politics of safety of the information.....	48
2.4. Conditions of safety of information-communication systems and networks	53
<i>III chapter. LEGAL AND ORGANIZATIONAL SAFETY OF THE INFORMATION</i>	
3.1. Legal management in sphere of information safety.....	59
3.2. Organizational-administrative maintenance of information safety	61
3.3. Standards and specifications on information safety	65
<i>IV chapter. CRYPTOGRAPHIC METHODS OF PROTECTION OF THE INFORMATION</i>	
4.1. Basic rules and definitions of cryptography.....	71
4.2. Symmetric systems of enciphering.....	74
4.3. Asymmetric systems of enciphering.....	89
4.4. Standards of enciphering	92
4.5. Function of hashing.....	99
4.6. The electronic digital signature.....	102
4.7. Management of cryptographic keys.....	107
<i>V chapter. IDENTIFICATION AND AUTHENTICATION</i>	
5.1. The basic concepts and classification.....	115
5.2. Authentication on the basis of passwords.....	120
5.3. Authentication on the basis of certificates.....	125
5.4. Strong authentication	128
5.5. Biometric identification and authentication users.....	147

<i>VI chapter. TECHNOLOGY OF GATEWAY SCREENS</i>	
6.1. Features of functioning of gateway screens.....	153
6.2. The basic components of gateway screens.....	163
6.3. The scheme of protection of a network on the basis of gateway screens	174
<i>VII chapter. PROTECTED VIRTUAL PRIVATE NETWORKS</i>	
7.1. The concept of construction of the protected virtual private networks.....	185
7.2. Classification of the protected virtual private networks...	193
7.3. Decisions for construction of protected virtual private networks VPN.....	203
7.4. Construction of the protected virtual private networks in channel and session levels.....	220
7.5. Use of stack IPsec of the report at construction of the protected virtual private networks	245
<i>VIII chapter. INFRASTRUCTURE OF MANAGEMENT OF THE PUBLIC KEYS PKI</i>	
8.1. Principle of functioning PKI	255
8.2. Logic structure and components of an infrastructure of management of the public keys.....	265
<i>IX chapter. DETECTION OF INTRUSIONS IN INFORMATION-COMMUNICATION SYSTEMS</i>	
9.1. The concept of adaptive management of safety	271
9.2. The analysis of security	275
9.3. Detection of attacks	279
9.4. Computer viruses and problems of anti-virus protection.....	288
9.5. Anti-virus programs	297
9.6. Construction of system of anti-virus protection.....	305
<i>X chapter. PROTECTION OF THE INFORMATION IN NETWORKS OF DATA TRANSMISSION</i>	
10.1. Maintenance of protection of the information in networks of data transmission	309
10.2. Methods of protection of data-in liaison channels.....	312
<i>XI chapter. PROTECTION OF THE INFORMATION IN SYSTEMS OF WIRELESS COMMUNICATION</i>	
11.1. The concept and structure of a wireless network	317
11.2. Threats of safety of a wireless network	327
11.3. Protocols of safety of a wireless network.....	337
11.4. Problems of safety of wireless devices.....	342

XII chapter. MANAGEMENT OF SAFETY AND

CONSTRUCTION SYSTEMS OF PROTECTION

12.1. Functional tasks of management	347
12.2. Architecture of management of means of safety.....	351
12.3. Audit and monitoring of information systems	356
12.4. The analysis and management of risks	363
12.5. Methodology of construction of system of information safety	368
THE USED LITERATURE	375
THE LIST OF REDUCTIONS	378

Илдам кадамлар билан ривожланаётган компьютер ахборот технологиялари ҳаётимизда сезиларли ўзгаришларга сабаб бўлмоқда. «Ахборот» тушунчаси сотиб олиш, сотиш, бирор нарсага алмашиш ва ҳ. мумкин бўлган махсус товарни белгилашда тез-тез ишлатила бошланди. Бунда ахборотнинг нархи кўпинча у жойлашган компьютер тизими нархидан юз ва минг марта юкори бўлади. Демак, ахборотни рухсатсиз фойдаланишдан, атайин ўзгартириш-дан, йўқ қилишдан ва бошқа жиноий ҳаракатлардан химоялаш заруриятининг пайдо бўлиши табиийдир.

Ахборотни химоялаш муаммоси компьютер тизимлари ва тармоқлари соҳасида фаолият кўрсатувчи мутахассислар ҳамда замонавий компьютер воситаларидан фойдаланувчилар эътиборини жалб этмоқда. Айни пайтда компьютер фани ва амалиётининг ушбу долзарб муаммоси Давлат тилида ёзилган илмий-техник ва ўқув адабиётларда етарлича ўз аксини топмаган.

Ўқувчи эътиборига ҳавола этилаётган китоб ахборот-коммуникацион тизимлар хавфсизлигига бағишланган ва 12 та бобдан иборат.

Китобнинг I бобида ахборот хавфсизлигининг ҳозирги ҳолатига баҳо берилади. Компьютер жиноятчилиги таҳлил этилиб, тармок ахборотига бўладиган намунавий ҳужум усуллари келтирилади ҳамда ахборот хавфсизлигини бузувчининг модели тавсифланади. Шунингдек, бу бобда Internet – хизматлари ва электрон бизнес тизимларида хавфсизлик муаммолари кўрилган.

Ахборот хавфсизлигининг асосий тушунчалари, хавфсизликни таъминлашнинг амалда текширилган принциплари ҳамда хавфсизлик сиёсатини яратиш жараёни тавсифи китобнинг II бобида келтирилган. Шу билан бирга ахборот-коммуникацион тизимлар ва тармоқлар хавфсизлигига қўйиладиган талаблар ва ахборот хавфсизлигини таъминловчи чоралар хусусида сўз юритилган.

Ахборот хавфсизлигининг ҳукукий ва ташкилий таъминоти, хавфсизликнинг халқаро ва миллий ҳукукий меъёрлари китобнинг III бобида баён этилган.

Китобнинг IV боби ахборотни ҳимоялашнинг криптографик усулларига бағишланган бўлиб, маълумотларни шифрлашнинг блокли симметрик алгоритмлари, жумладан, АҚШнинг янги стандарти AES таҳлил этилган ва миллий стандартимиз ёритиб ўтилган. Замонавий асимметрик криптоотизимлар муҳокама этилиб, ҳэшлаш функцияларининг асосий хусусиятлари ва ишлатилиш соҳалари аниқланган. Рақамли имзони генерациялаш ва текшириш муолажалари кўрилган. Калитларни бошқариш – калитларни тақсимлаш жараёнига алоҳида эътибор қилинган.

Тизимнинг фойдаланувчилар билан ўзаро алоқасидаги асосий жараёнлар – фойдаланувчи ҳаракатини аутентификациялаш, авторизациялаш ва маъмурлаш, кўп ва бир маротабали пароллар ҳамда рақамли сертификатлар асосидаги аутентификациялаш хусусиятларининг таҳлили китобнинг V бобида ёритилган. Фойдаланувчини идентификациялаш ва аутентификациялашнинг намунавий схемалари кўрилган. Симметрик ва асимметрик криптоалгоритмларга асосланган катъий аутентификациялашга алоҳида эътибор берилган. Аутентификациялашнинг Kerberos протоколи муҳокама этилган. Биометрик идентификациялаш ва аутентификациялаш воситалари тавсифланган.

Тармоқлараро экранларнинг функциялари таҳлили, уларнинг OSI моделининг турли сатҳларида ишлаши хусусиятлари муҳокамаси, тармоқларо экранлар асосида тармокни ҳимоялаш схемалари, шахсий ва тақсимланган тармок экранларининг ишлатилиши VI бобда кўрилган.

Ҳимояланган виртуал хусусий тармоқларни қуриш концепцияси ва уларнинг асосий хусусияти – туннеллаш, виртуал ҳимояланган каналларни қуриш вариантлари таҳлили, ҳимояланган виртуал хусусий тармоқларнинг қатор аломатлари бўйича туркумлиниши, VPN технологиянинг корпоратив ахборот тизимлари ва тармоқларида қўлланилишининг техник ва иқтисодий афзалликлари, OSI очик тизимлар ўзаро алоқа эталон моделининг канал ва сеанс сатҳларида ҳимояланган виртуал каналлар қурилишининг муаммолари муҳокамаси, IPSec протоколлар стекининг архитектура-си, уларнинг ҳимояланган хусусий тармоқлар қуришда ишлатилиши масалалари китобнинг VII бобидан ўрин олган.

Китобнинг VIII бобда очик калитларни бошқариш инфратузилмаси PKI кўрилган. Очик калитларнинг рақамли сертификатларини ишлатиш зарурияги асосланган. PKI нинг ишлаш принциплари муҳокама этилган. Сертификациялашнинг базавий моделлари, PKI нинг мантикий тузилмаси ва компонентлари келтирилган.

Ахборот хавфсизлигини адаптив бошқаришнинг долзарб муаммолари, корпоратив тармоқ хавфсизлигини адаптив бошқариш концепцияси тавсифи, химояланишни таҳлиллашнинг технологиялари ва воситалари батафсил муҳокама этилиб, тармоқ ахборотини таҳлиллаш усуллари, ҳужумларни аниқлаш тизимларининг компонентлари ва архитектураси китобнинг IX бобида ўз аксини топган. Шу билан бир қаторда компьютер вирусларидан химояланишнинг долзарб муаммолари ҳам ушбу бобдан ўрин олган. Компьютер вирусларининг туркумланиши келтирилган, вирус ҳаёт цикли босқичлари таҳлилланган, вируслар ва бошқа зарар келтирувчи дастурларнинг асосий тарқалиш каналлари кўрилган. Вирусга қарши дастурларнинг асосийлари муҳокама этилиб, вирусга қарши химоя тизимини қуриш масаласи ёритилган.

Маълумотларни узатиш тармоғида ахборотни химоялаш муаммоси, маълумотларни узатиш тармоғи компонентларига ва архитектурасига реал таъсир этувчи функционал, архитектуравий ва бошқариш (маъмурий) талаблари ҳамда алоқа каналларида маълумотларни химоялаш усуллариининг муҳокамаси X бобда ёритиб ўтилган.

Симсиз алоқа тизимларида ахборот химоясининг долзарб масалаларига бағишланган муаммолар XI бобда келтирилган бўлиб, унда симсиз тармоқ концепцияси ва тузилмаси кўрилган. Симсиз тармоқ хавфсизлигига таҳдидлар батафсил таҳлил этилиб, симсиз тармоқ хавфсизлиги протоколлари муҳокама этилган. Симсиз қурилмалар хавфсизлиги муаммолари ҳам ушбу бобдан ўрин олган.

Китобнинг XII боби тармоқ хавфсизлиги воситаларини бошқариш усулларига бағишланган. Ахборот тизимларини бошқаришнинг кенг тарқалган методологияси ITIL тавсифланган. Корхона миқёсида ахборотни химоялаш тизимини бошқариш масаласи таърифланган. Хавфсизликни марказлаштирилган бошқаришнинг глобал ва локал хавфсизлик сиёсатига асосланган истикболли архитектурасига алоҳида эътибор берилган. Ахборот тизимлари хавфсизлигининг аудити ва мониторинги кўрилган. Хавфхатарларни таҳлиллаш ва бошқариш муаммоси ҳамда тармоқ хавфсизлик тизимини қуриш методологияси тавсифланган.

Кўлланмани тайёрлашда яқиндан ёрдам берган (VII ва XI боблар) техника фанлари номзоди А.А. Ғаниева, тақризчиларга ҳамда ўқув кўлланма ҳақидаги барча фикр мулоҳазалари учун ҳурматли китобхонларга муаллифлар ўз миннатдорчиликларини изҳор этадилар.

МУАЛЛИФЛАР

1.1. Ахборот урушлар ва киберхужумлар

Хавфсизлик – ҳар куни биз тўқнашадиган ҳаётимизнинг жиҳати: эшикни кулфлаймиз, қимматбаҳо нарсаларни бегона кўзлардан беркитамиз ва ҳамённи дуч келган жойда қолдирмаймиз. Бу «рақамли дунёга» ҳам расм бўлиши шарт, чунки ҳар бир фойдаланувчининг компьюттери қароқчи ҳужуми объекти бўлиши мумкин.

Тижорат ташкилотлари хавфсизликни таъминлаш ўзининг биринчи галдаги вазифаси эмас, балки уни таъминлашга сарф этиладиган харажатларни муқаррар бало деб ҳисоблаб келганлар. Қандайдир даражада бу «оқилона иш»: ниҳоят, усиз ҳам иш бажаришда тўсиклар тўлиб-тошиб ётибдику?! Аммо фирманинг барча корпоратив биноларига кеча-кундуз киришга рухсат беришга журъат этувчи ақли жойида «саноат капитанлари»ни кўрганмисиз? Албатта, йўк! Ҳатто кичкина компания биносининг кириш йўлида сизни қоровул ёки киришни чегараловчи ва назоратловчи тизими қарши олади. Ахборотни ҳимоялаш эса ҳали кўнгилдагидек эмас. Ахборотни қандай йўқотиш мумкинлигини ва бу қандай оқибатларга олиб келишини барча ҳам тушунавермайди.

Йирик ўйинчилар яхшигина сабоқ олдилар: хакерлар Yahoo.com, Amazon.com каби компанияларга ва ҳатто космик тадқиқот агентлиги NASAга қатта зарар етказдилар. Хавфсизлик хизмати бозорининг энг йирик номбандаларидан бири RSA Security, ҳар қандай таҳдидга қарши чора борлиги хусусидаги ўйламасдан қилган баёнотидан бир неча кундан кейин, ҳужумга дучор бўлди [33].

Одатда, одамлардан ёки предметлардан чиқадиган ва зарар етказадиган таҳдидлар қуйидаги синфларга бўлинади: *ички ёки ташқи* ва *тузилмаган* (маълум объектга қарши) ёки *тузилмаган* («қимга Худо беради» қабилда манзилланувчи). Масалан, компьютар вируслари «ташқи тузилмаган таҳдидлар» сифатида туркумланади ва тамомила оддий ҳисобланади. Қизиғи

шундаки, фойдаланувчилар ўзининг компьютерини муайян нишон деб ҳисобламайдилар, улар ўзларини яхшигина химоялангандек сезадилар. Керакли химоя даражаси аксарият ҳолларда ишингизнинг ҳолатига боғлиқ. Агар ташкилотингиз ёки компаниянгиз қандайдир тазйик нишони бўлса, агар сиз миллий энергетик ресурсларни тақсимловчи ёки миллий алоқа тармоқларига хизмат килувчи давлат инфратузилмаси таркибида бўлсангиз, оддий террористлар бомбаларини ва пистолетларини четга қўйиб, турлигуман дастурий воситалар ёрдамида ташкилотингизга электрон хужумни амалга ошириш масаласини кўрадилар. Иккинчи томондан, савдо-сотик ва маркетинг бўйича оддий ташкилот хусусида сўз борса, фақат мижозлар рўйхатини ўғриловчи хизматчиларингиз тўғрисида, калбаки кредит карточкалари бўйича товар олувчи фирибгарлар, тармоғингизга прејскурантлардан фойдаланиш мақсадида кирувчи рақиблар, Web-сайтнингизни таъмағирлик мақсадида бузувчилар ва шунга ўхшашлар тўғрисида кайғуришингизга тўғри келади.

Аммо, ваҳимага ўрин йўқ. Биринчи навбатда кундалик эҳтиёж чоралари кўрилиши лозим. Ахборотга эга бўлишнинг энг оммабоп усули оддий ўғрилик. Сиз иш столингизда кечага мўмайгина пулни колдириб кетмайсизу. Нима учун боқувчингиз-шахсий компьютер хавфсизлигини таъминлашга озгина вақт сарф килмайсиз? Бу нафақат аппарат воситаларига, балки маълумотларга ҳам тааллуқли. Маълумотларни ўғирлатиш ёки йўқотиш катта, баъзида, тузатиб бўлмайдиган зарар келтиради.

Маълумки, тизим маъмурлари барча махфий материаллардан фойдаланиш имконига эга ва, одатда, компания фойдасидан ўз улушларига эга эмаслар. Шу сабабли худди улар ташкилот хавфсизлигига таҳдид сола олувчилар ичида энг каттаси ҳисобланадилар. Таъкидлаш лозимки, компания ишга кирувчиларни синчиклаб текширади. Худди шундай, хавфсизлик хизматини таъминловчиларга, айниқса, маслаҳат бериш, режалаштириш ва муъмурашнинг тавсия этувчиларга диққат билан қараш лозим.

Цивилизация ривожининг замонавий босқичида ахборот нафақат жамоат ва давлат институтлари фаолиятида, балки ҳар бир инсон ҳаётида ҳал қилувчи ролни ўйнайди. Кўз олдимизда жамиятнинг ахборотлашиши шиддат билан ва кўпинча олдиндан билиб бўлмайдиган тарзда ривожланмоқда. Биз эса унинг ижтимоий, сиёсий, иктисодий ва бошқа оқибатларини тушуниб етишга бошлай-

миз, холос. Жамиятимизнинг ахборотлашиши ягона дунё ахборот маконининг яратилишига олиб келадик, бу макон доирасида ахборотни йиғиш, ишлаш, сақлаш ва субъектлар – инсонлар, ташкилотлар, давлатлар ўртасида алмашиш амалга оширилади.

Равшанки, сиёсий, иқтисодий, илмий-техникавий ва бошқа ахборотларни тезликда алмашиш имконияти, жамият ҳаётининг барча соҳаларида ва айниқса, ишлаб чиқаришда ва бошқаришда янги технологияларнинг қўлланилиши сўзсиз фойдалидир. Аммо, саноатнинг тезликда рифожланиши Ер экологиясига таҳдид сола бошлади, ядро физикаси соҳасидаги ютуқлар ядро уруши хавфини туғдирди. Ахборотлаштириш ҳам жиддий муаммолар манбаига айланиши мумкин.

Урушлар доимо бўлган. Вакт ўтиши билан урушни олиб бориш бутун бир фанга айланди. Ҳар қандай фандагидек урушда ўзининг тарихи, ўзининг қондаси, машҳур намоёндалари, ўзининг методологияси пайдо бўлди.

Замонавий уруш ғояси жуда илдамлаб кетди. Энди унинг макони – бутун ер шари. Уруш локал қарокчи ҳужумидан бир неча давлатларни вайрон қилувчи глобал муаммога айланди.

Турли мамлакатларнинг ҳарбий доктриналарида электрон қурол ривожини режалари ва махсус вазифаларга мўлжалланган дастурий таъминот тўғрисида эслатишлар кўзга ташланмоқда. Турли разведка манбаларидан келатган ахборотнинг таҳлили натижасида ҳулоса қилиш мумкинки, баъзи бир давлатларнинг раҳбарлари ҳужумкор кибер-дастурларни яратишни молияламоқдалар.

Ахборот урушига оддий воситалар ёрдамида ҳарбий ҳаракатлар самара бермайдиган ҳолларга нисбатан стратегик альтернатива сифатида қаралмоқда.

Ҳарбийлар томонидан киритилган *ахборот уруши* атамаси реал, қирғинли ва емирувчи ҳарбий ҳаракатлар билан боғлиқ шифқатсиз ва хавfli фаолиятни англатади. Бу урушнинг алоҳида қирралари-штаб уруши, электрон уруши, психологик амаллар ва ҳ.

Ҳар қандай уруш, ахборот уруши шу жумладан, замонавий қурол ёрдамида олиб борилади. Ахборот қуроли ёрдамида, уруш олиб борилувчи барча қуроллардан фарқли ўларок, эълон қилинмаган ва кўпинча дунёга кўринмайдиган урушларни олиб бориш мумкин (олиб боришмоқда ҳам). Бу қуролнинг таъсир объектлари – иқтисодий, сиёсий, ижтимоий ва ҳ. каби жамият ва дав-

лат институтлари. Маълумотларни узатиш тармоқларининг келажак жанрлар майдонига айланиши аллақачон эътироф этилган.

Ахборот курули хужумда ва мудофаада «электрон тезлик» билан ишлатилиши мумкин. У энг илғор технологияларга асосланган бўлиб, ҳарбий низоларни дастлабки босқичида ҳал этилишини таъминлайди ҳамда умуммақсад кучларнинг қўлланилишини истисно қилади. Ахборот курули қўлланишининг стратегияси хужумкор характерга эга. Аммо хусусий заифлик нуқтаи назари мавжуд, айниқса фуқаролик секторида. Шу сабабли бундай курулдан ва ахборот терроризмидан химояланиш муаммоси ҳозирда биринчи ўринга чиққан. Фойдаланувчиларига дунё тармоқларида ишлашни таъминловчи мамлакатларнинг миллий ахборот ресурсларининг заифлиги – ҳар икки томонга хавfli нарса.

Ахборот курули деганда ахборот массивларини йўқотиш, бузиш ёки ўғирлаш воситалари, химоялаш тизимини йўқотиш, қонуний фойдаланувчилар фаолиятини чегаралаш асбоб-ускуналар ва бутун компьютер тизими ишлаши тартибини бузиш воситалари тушунилади.

Ҳозирда хужумкор ахборот курули сифатида қуйидагиларни кўрсатиш мумкин:

– *компьютер вируслари* – кўпайиш, дастурларда ўрнашиш, алоқа линиялари, маълумотларни узатиш тармоқлари бўйича узатилиш, бошқариш тизимларни ишдан чиқариш ва шунга ўхшаш қобилиятларга эга;

– *манتيқий бомбалар* – сигнал бўйича ёки ўрнатилган вақтда ҳаракатга келтириш мақсадида ҳарбий ёки фуқаро инфратузилмаларига ўрнатиловчи дастурланган курилмалар;

– *телекоммуникация тармоқларида ахборот алмашинувини бостириш воситалари*, давлат ва ҳарбий бошқарув каналларида ахборотни сохталаштириш;

– *тестли дастурларни бетарафлаштириш воситалари*;

– объект дастурий таъминотига айғокчилар томонидан атайин киритилувчи турли хил *хатоликлар*.

Универсаллик. махфийлик, дастурий-аппарат амалга оширилишининг ҳар хиллиги, таъсирининг кескинлиги, қўлланилишининг вақти ва жойини танлаш имконияти, ниҳоят, фойдалилиги ахборот курулини ҳаддан ташқари хавfli қилади. Бу курулни, масалан, интеллектуал мулкни химоялаш воситасига ўхшатиб никоблаш мумкин. Ундан ташқари, у ҳатто уруш эълон қилмасдан

хужум ҳаракатларини автоном тарзда олиб бориш имконини беради.

Замонавий жамиятда ахборот куролини ишлатиш ҳарбий стратегияси фуқаро сектори билан узвий боғланган. Ахборот куролининг, унинг таъсири шакли ва усулларининг пайдо бўлиши ва қўлланиши хусусиятларининг турли-туманлилиги ундан химояланишнинг мураккаб масалаларини вужудга келтирди.

Ахборот куроли қўлланилишини олдини олиш ёки қўлланиши оқибатларини бартараф қилиш учун қуйидаги чораларни кўриш лозим:

- ахборот ресурсларининг физик асосини ташкил этувчи моддий-техник объектларни химоялаш;
- маълумотлар базалари ва банкларининг меъёрий ва муттасил ишлашини таъминлаш;
- ахборотдан рухсатсиз фойдаланишдан, уни бузилишидан ёки йўқ қилинишидан химоялаш;
- ахборот сифатини сақлаш (ўз вақтидалиги, аниқлиги, тўлаллиги ва фойдаланувчанлиги).

Давлатнинг дунё очик тармоғига уланишининг иқтисодий ва илмий-техник сиёсатини ахборот хавфсизлиги орқали кўриш лозим. Бу очик, фуқароларнинг ахборотга ва интеллектуал мулкга эга бўлиш қонуний ҳуқуқини сақлашга мўлжалланган сиёсат мамлакат ҳудудида тармок асбоб-ускуналарини унга ахборот куроли элементларининг қиришидан сақлашни кўзда тутиш лозим. Бу муаммо ҳозирда, чет эл ахборот технологияларини оммавий сотиб олинаётган пайтда ўта муҳимдир.

Маълумки, дунё ахборот маконига уланмасдан мамлакат иқтисодини ривожлантириб бўлмайди. Internet тармоғи томонидан таъминланган ахборот ва ҳисоблаш ресурсларидан оператив фойдаланишни давлатчиликни, фуқаролик жамияти институтларини мустаҳкамлаш, ижтимоий инфратузилмаларининг ривожланиш шартлари сифатида талқин этиш мумкин.

Аммо мамлакатнинг ҳалқаро телекоммуникация тизимида ва ахборот алашинувида иштирокининг ахборот хавфсизлиги муаммосини комплекс ҳал қилмасдан мумкин эмаслигини аниқ тасаввур этиш лозим. Айниқса, хусусий ахборот ресурсларини химоялаш муаммоси ахборот ва телекоммуникация технологиялар соҳасида ривожланган мамлакатлардан технологик орқада қолаётган мамлакатлар учун жиддий ҳисобланади.

Ахборот қуролини ишлаб чиқишни ва уни ишлатишни кимёвий ва бактериологик қурол каби тақиклаш эҳтимолдан узок. Худди шу каби кўпгина мамлакатларнинг ягона глобал ахборот маконини шакллантириш бўйича уринишларини чегаралаб бўлмайди.

Тизим маъмури учун химоянинг мақбул даражасини таъминлашнинг ягона усули-ахборотга эга бўлиши, чунки ҳозирча ахборот ҳужумига энг тез реакция берадиган инсон ҳисобланади. Демак, ахборотни химоялаш маъмурларининг ўқитишга ва профессионал ўсишига сарф-харажат ахборот ҳужумларига қарши турувчи энг самарали восита ҳисобланади.

1.2. Ахборот-коммуникацион тизимлар ва тармоқларда таҳдидлар ва заифликлар

Тармоқ технологиялари ривожининг бошланғич босқичида вируслар ва компьютер ҳужумларининг бошқа турлари таъсиридаги зарар кам эди. чунки у даврда дунё иктисодининг ахборот технологияларига боғлиқлиги катта эмас эди. Ҳозирда, ҳужумлар сонининг доимо ўсиши ҳамда бизнеснинг ахборотдан фойдаланиш ва алмашишнинг электрон воситаларига боғлиқлиги шароитида машина вақтининг йўқолишига олиб келувчи ҳатто озгина ҳужумдан келган зарар жуда катта рақамлар орқали ҳисобланади. Мисол тариқасида келтириш мумкинки, фақат 2003 йилнинг биринчи чорагида дунё микёсидаги йўқотишлар 2002 йилдаги барча йўқотишлар йиғиндисининг 50 %ини ташкил этган ёки бўлмаса 2006 йилнинг ўзида Россия Федерациясида 14 мингдан ортиқ компьютер жиноятчилиги ҳолатлари қайд этилган [24, 34, 35]. Корпоратив тармоқларда ишланадиган ахборот, айниқса, заиф бўлади. Ҳозирда руҳсатсиз фойдаланишга ёки ахборотни модификациялашга, ёлғон ахборотнинг муомалага кириши имконининг жиддий ошишига қуйидагилар сабаб бўлади:

- компьютерда ишланадиган, узатиладиган ва сақланадиган ахборот ҳажмининг ошиши;
- маълумотлар базасида муҳимлик ва махфийлик даражаси турли бўлган ахборотларнинг тўпланиши;
- маълумотлар базасида сақланаётган ахборотдан ва ҳисоблаш тармоқ ресурсларидан фойдаланувчилар доирасининг кенгайиши;
- масофадаги ишчи жойлар сонининг ошиши;

– фойдаланувчиларни боғлаш учун Internet глобал тармоғини ва алоканинг турли каналларини кенг ишлатиш;

– фойдалувчилар компьютерлари ўртасида ахборот алмашинувининг автоматлаштирилиши.

Ахборот хавфсизлигига таҳдид деганда ахборотнинг бузилиши ёки йўқотилиши хавфига олиб келувчи химояланувчи объектга қарши қилинган ҳаракатлар тушунилади. Олдиндан шуни айтиш мумкинки, сўз барча ахборот хусусида эмас, балки унинг фақат, мулк эгаси фикрича, тижорат кийматида эга бўлган қисми хусусида кетаяпти.

Замонавий корпоратив тармоқлар ва тизимлар дучор бўладиган кенг тарқалган таҳдидларни таҳлиллаймиз. Ҳисобга олиш лозимки, хавфсизликка таҳдид манбалари корпоратив ахборот тизимининг ичида (ички манба) ва унинг ташқарисида (ташки манба) бўлиши мумкин. Бундай ажратиш тўғри, чунки битта таҳдид учун (масалан, ўғирлаш) ташки ва ички манбаларга қарши ҳаракат усуллари турлича бўлади. Бўлиши мумкин бўлган таҳдидларни ҳамда корпоратив ахборот тизимининг заиф жойларини билиш хавфсизликни таъминловчи энг самарали воситаларни танлаш учун зарур ҳисобланади.

Тез-тез бўладиган ва хавфли (зарар ўлчами нуктаи назаридан) таҳдидларга фойдаланувчиларнинг, операторларнинг, маъмурларнинг ва корпоратив ахборот тизимларига хизмат кўрсатувчи бошқа шахсларнинг атайин қилмаган хатоликлари қиради. Баъзида бундай хатоликлар (нотўғри қиритилган маълумотлар, дастурдаги хатоликлар сабаб бўлган тизимнинг тўхташи ёки бузилиши) тўғридан тўғри зарарга олиб келади. Баъзида улар нияти бузук одамлар фойдаланиши мумкин бўлган нозик жойларни пайдо бўлишига сабаб бўлади. Глобал ахборот тармоғида ишлаш ушбу омилнинг етарлича долзарб қилади. Бунда зарар манбаи ташкилотнинг фойдаланувчиси ҳам, тармоқ фойдаланувчиси ҳам бўлиши мумкин, охиргиси айниқса хавфли.

Зарар ўлчами бўйича иккинчи ўринни ўғирлашлар ва сохта-лаштиришлар эгаллайди. Текширилган ҳолатларнинг аксариятида ишлаш режимлари ва химоялаш чоралари билан аъло даражада та-ниш бўлган ташкилот штатидаги ходимлар айбдор бўлиб чиқдилар. Глобал тармоқлар билан боғланган қувватли ахборот каналининг мавжудлигида, унинг ишлаши устидан етарлича назорат йўқлиги бундай фаолиятга қўшимча имкон яратади.

Хафа бўлган ходимлар (хатто собиклари) ташкилотдаги тартиб билан таниш ва жуда самара билан зиён етказишлари мумкин. Ходим ишдан бўшаганида унинг ахборот ресурсларидан фойдаланиш ҳукуки бекор қилиниши назоратга олиниши шарт.

Ҳозирда ташки коммуникация орқали рухсатсиз фойдаланишга атайин қилинган уринишлар бўлиши мумкин бўлган барча бузилишларнинг 10 %ини ташкил этади. Бу катталик анчагина бўлиб туюлмаса ҳам, Internetда ишлаш тажрибаси кўрсатадики, қарийб ҳар бир Internet-сервер кунига бир неча марта суқилиб кириш уринишларига дучор бўлар экан. Хавф-хатарлар тахлил қилинганда ташкилот корпоратив ёки локал тармоғи компьютерларининг хужумларга қарши туриши ёки бўлмаганида ахборот хавфсизлиги бузилиши фактларини қайд этиш учун етарлича химоялан-маганлигини ҳисобга олиш зарур. Масалан, ахборот тизимларини химоялаш Агентлигининг (АҚШ) тестлари кўрсатадики, 88 % компьютерлар ахборот хавфсизлиги нуқтан назаридан нозик жойларга эаки, улар рухсатсиз фойда таниш учун фаол ишлатишлари мумкин. Ташкилот ахборот тузилмасидан масофадан фойдаланиш ҳоллари алоҳида кўрилиши лозим.

Ҳимоя сиёсатини тузишдан аввал ташкилотда компьютер муҳити дучор бўладиган хавф-хатар баҳоланиши ва зарур чоралар кўрилиши зарур. Равшанки, химояга таҳдидни назоратлаш ва зарур чораларни кўриш учун ташкилотнинг сарф-харажати ташкилотда активлар ва ресурсларни химоялаш бўйича ҳеч қандай чоралар кўрилмаганида қутиладиган йўқотишлардан ошиб кетмаслиги шарт.

Умуман олганда, ташкилотнинг компьютер муҳити икки хил хавф-хатарга дучор бўлади:

1. Маълумотларни йўқотилиши ёки ўзгартирилиши.
2. Сервиснинг тўхтатилиши.

Таҳдидларнинг манбаларини аниқлаш осон эмас. Улар нияти бузук одамларнинг бостириб киришидан то компьютер вирусларигача турланиши мумкин.

Бунда инсон хатоликлари хавфсизликка жиддий таҳдид ҳисобланади. 1.1-расмда корпоратив ахборот тизимида хавфсизликнинг бузилиш манбалари бўйича статистик маълумотларни тас-вирловчи секторли диаграмма келтирилган.

**Физик
хавфсизлик
муаммолари**



1.1-расм. Хавфсизликнинг бузилиш манбалари.

1.1.-расмда келтирилган статистик маълумотлар ташкилот маъмуриятига ва ходимларига корпоратив тармоқ ва тизими хавфсизлигига таҳдидларни самарали камайтириш учун ҳаракатларни қаерга йўналтиришлари зарурлигини айтиб бериши мумкин. Албатта, физик хавфсизлик муаммолари билан шуғулланиш ва инсон хатоликларининг хавфсизликка салбий таъсирини камайтириш бўйича чоралар кўрилиши зарур. Шу билан бир қаторда корпоратив тармоқ ва тизимга ҳам ташқаридан, ҳам ичкаридан бўладиган ҳужумларни олдини олиш бўйича тармоқ хавфсизлиги масаласини ечишга жиддий эътиборни қаратиш зарур.

1.3. Компьютер жиноятчилигининг таҳлили

Компьютер жиноятчилиги статистикаси таҳлил этилса қайғули манзарага эга бўламиз. Компьютер жиноятчилиги етказган зарарни наркотик моддалар ва куролларнинг ноқонуний айланишидан олинган фойдага қиёслаш мумкин. Фақат АҚШда «электрон жиноятчилар» етказган ҳар йилги зарар қарийб 100 млрд. долларни ташкил этар экан.

Якин келажакда жиний фаолиятнинг бу тури даромадлиги, пул маблағларининг айланиши ва унда иштирок этувчи одамлар сони бўйича якин вақтларгача ноқонуний фаолият орасида даромадлиги билан биринчи ўринни эгаллаган ноқонуний бизнеснинг уч туридан ўзиб кетиш эҳтимоллиги катта. Бу ноқонуний бизнеслар-наркотик моддалар, қурол ва кам учрайдиган ёввойи ҳайвонлар билан савдо қилиш.

Давлат ва хусусий компаниялар фаолиятининг социологик тадқиқи маълумотларига қараганда XXI асрнинг биринчи йилларида иқтисодий соҳадаги жиноятчилик банк ва бошқа тизимларнинг ахборот-коммуникацион комплексларига бўлиши мумкин бўлган ғаразли иқтисодий ҳаракатларга қаратилган бўлади.

Кредит-молия соҳасидаги компьютер жиноятчилигининг сони муттасил ўсиб бормоқда. Масалан, онлайн магазинларида 25 %гача қаллоблик тўлов амаллари қайд этилган. Шунга қарамасдан Ғарб давлатларида электрон тижоратнинг-юқори даромадли замонавий бизнеснинг фаол ривожланиши кўзга ташланмоқда. Маълумки, бу соҳа ривожланиши билан параллел равишда «виртуал» қаллобларнинг ҳам даромади ошади. Қаллоблар энди яқка ҳолда ҳаракат қилмайдилар, улар пухталиқ билан тайёрланган, яхши техник ва дастурий қуролланган жиний гуруҳлар билан, банк хизматчиларининг ўзлари иштирокида ишлайдилар.

Хавфсизлик соҳасидаги мутахассисларнинг кўрсатишича бундай жиноятчиларнинг улуши 70 %ни ташкил этади. «Виртуал» ўғри ўзининг ҳамкасби-оддий босқинчига нисбатан кўп топади. Ундан ташқари, «виртуал» жиноятчилар уйдан чиқмасдан ҳаракат қиладилар. Фойдаланишнинг электрон воситаларини ишлатиб қилинган ўғрилиқ зарарининг ўртача кўрсаткичи фақат АКШда банкни қуролли босқинчиликдан келган зарарнинг ўртача статистик зараридан 6–7 марга катта.

Банк хизмати ва молия амаллари соҳасидаги турли хил қаллоблик натижасида йўқотишлар 1989 йили 800 млн. доллардан 1997 йили – 100 млрд. долларга етган. Бу кўрсаткичлар ўсаяпти, аслида юқорида келтирилган маълумотлардан бир тартибга ошиши мумкин. Чунки кўп йўқотишлар аниқланмайди ёки эълон қилинмайди. ўзига хос «индамаслик сиёсати»ни тизим маъмурларининг ўзининг тармоғидан рухсатсиз фойдаланганлик тафсилоти-

ни, бу ноҳуш ҳодисанинг такрорланишидан кўриб ва ўзининг химоя усулини ошкор этмаслик важида муҳокама этишни хоҳламасликлари билан тушуниш мумкин.

Компьютер ишлатиладиган инсон фаолиятининг бошқа соҳаларида ҳам вазиёт яхши эмас. Йилдан-йилга ҳуқуқни муҳофаза қилувчи органларига компьютер жиноятчилиги хусусидаги муурожаатлар ошиб бормоқда.

Барча мутахассислар вирусларнинг тарқалиши билан бир қаторда ташқи ҳужумларнинг кескин ошганлигини эътироф этмоқдалар. Кўриниб турибдики, компьютер жиноятчилиги натижасида зарар қатъий ортмоқда. Аммо компьютер жиноятчилиги кўпинча «виртуал» қаллоблар томонидан амалга оширилади дейиш ҳақиқатга тўғри келмайди. Ҳозирча компьютер тармоқларига сукилиб кириш хавфи ҳар бири ўзининг усулига эга бўлган ҳакерлар, кракерлар ва компьютер қароқчилари томонидан келмоқда.

Ҳакерлар, бошқа компьютер қароқчиларидан фарқли ҳолда, баъзида, олдиндан, мақтаниш мақсадида компьютер эгаларига уларнинг тизимига кириш ниятлари борлигини билдириб қўядилар. Муваффақиятлари хусусида Internet сайтларида хабар берадилар. Бунда ҳакер мусобақалашув ниятида қирган компьютерларига зарар етказмайди.

Кракерлар (stacker) – электрон «ўғрилар» манфаат мақсадида дастурларни бузишга ихтисослашганлар. Бунинг учун улар Internet тармоғи бўйича тарқатилувчи бузишнинг тайёр дастурларидан фойдаланадилар.

Компьютер қароқчилари – рақобат қилувчи фирмалар ва ҳатто ажнабий махсус хизматлари буюртмаси бўйича ахборотни ўғирловчи фирма ва компанияларнинг юқори малакали мутахассислари. Ундан ташқари, улар бегона банк счётидан пул маблағларини ўғирлаш билан ҳам шуғулланадилар.

Баъзи «мутахассислар» жиддий гуруҳ ташкил қиладилар, чунки бундай криминал бизнес ўта даромадлидир. Бу эса тез орада, «виртуал» жиноятнинг зарари жиноят бизнесининг анъанавий ҳи-лидаги зарардан бир тартибга (агар кўп бўлмаса) ошишига сабаб бўлади. Ҳозирча бундай таҳдидни бетарафлаштиришнинг самарали усуллари мавжуд эмас.

1.4. Тармоқдаги ахборотга бўладиган намунавий ҳужумлар

Барча ҳужумлар Internet ишлаши принципларининг қандайдир чегараланган сонига асосланганлиги сабабли масофадан бўладиган намунавий ҳужумларни ажратиш ва уларга қарши қандайдир комплекс чораларни тавсия этиш мумкин. Бу чоралар, ҳақиқатан, тармоқ хавфсизлигини таъминлайди.

Internet протоколларининг мукамал эмаслиги сабабали тармоқдаги ахборотга масофадан бўладиган асосий намунавий ҳужумлар куйидагилар:

- тармоқ трафигини таҳлиллаш;
- тармоқнинг ёлғон объектини киритиш;
- ёлғон маршрутни киритиш;
- хизмат килишдан воз кечишга ундайдиган ҳужумлар.

Тармоқ трафигини таҳлиллаш. Сервердан Internet тармоғи базавий протоколлари FTP (File Transfer Protocol) ва TELNET (виртуал терминал протоколи) бўйича фойдаланиш учун фойдаланувчи *идентификация* ва *аутентификация* муолажаларини ўтиши лозим. Фойдаланувчини идентификациялашда ахборот сифатида унинг идентификатори (исми) ишлатилса, аутентификациялаш учун *парол* ишлатилади. FTP ва TELNET протоколларининг хусусияти шундаки, фойдаланувчиларнинг паролни ва идентификатори тармоқ орқали очик, шифрланмаган кўринишда узатилади. Демак, Internet хостларидан фойдаланиш учун фойдаланувчининг исми ва паролни билиш кифоя.

Ахборот алмашинувида Internetнинг масофадаги иккита узели алмашинув ахборотини *пакетларга* бўлишади. Пакетлар алоқа каналлари орқали узатилади ва шу пайтда ушлаб қолиниши мумкин.

FTP ва TELNET протоколларининг таҳлили кўрсатадики, TELNET паролни символларга ажратади ва паролнинг ҳар бир символни мос пакетга жойлаштириб битталаб узатади, FTP эса, аксинча, паролни бугунлайича битга пакетда узатади. Пароллар шифрланмаганлиги сабабли пакетларнинг махсус сканердастурлари ёрдамида фойдаланувчининг исми ва паролни бўлган пакетни ажратиш олиш мумкин. Худди шу сабабли, ҳозирда оммавий тус олган ICQ дастури ҳам ишончли эмас. ICQнинг протоколлари ва ахборотларни сақлаш, узатиш форматлари маълум ва демак, унинг трафиги ушлаб қолиниши ва очилиши мумкин.

Асосий муаммо алмашинув протоколида. Базавий татбикий протоколларнинг TCP/IP оиласи анча олдин (60-йилларнинг охири ва 80-йилларнинг боши) ишлаб чиқилган ва ундан бери умуман ўзгартирилмаган. Ўтган давр мобайнида тақсимланган гармок хавфсизлигини таъминлашга ёндашиш жиддий ўзгарди. Гармок уланишларини химоялашга ва трафикни шифрлашга имкон берувчи ахборот алмашинувининг турли протоколлари ишлаб чиқилди. Аммо бу протоколлар эскиларининг ўрнини олмади (SSL бундан истисно) ва стандарт мақомига эга бўлмади. Бу протоколларнинг стандарт бўлиши учун эса гармоқдан фойдаланувчиларнинг барчаси уларга ўтишлари лозим. Аммо, Internetда гармоқни марказлашган бошқариш бўлмаганлиги сабабли бу жараён яна кўп йиллар давом этиши мумкин.

Гармоқнинг ёлғон объектини киритиш. Ҳар қандай тақсимланган гармоқда кидириш ва манзиллаш каби «нозик жойлари» мавжуд. Ушбу жараёнлар кечишида гармоқнинг ёлғон объектини (одатда, бу ёлғон хост) киритиш имконияти туғилади. Ёлғон объектнинг киритилиши натижасида манзилатга узатмоқчи бўлган барча ахборот аслида нияти бузук одамга тегади. Тахминан буни тизимингизга, одатда, электрон почтани жўнатишда фойдаланадиган провайдерингиз сервери манзили ёрдамида киришга кимдир уддасидан чиққани каби тасаввур этиш мумкин. Бу ҳолда нияти бузук одам унчалик қийналмасдан электрон хат-хабарингизни эгаллаши, мумкин, сиз эса ҳатто ундан шубҳаланмасдан ўзингиз барча электрон почтангизни жўнатган бўлар эдингиз.

Қандайдир хостга мурожаат этилганида манзилларни махсус ўзгартиришлар амалга оширилади (IP-манзилдан гармоқ адаптери ёки маршрутизаторининг физик манзили аниқланади). Internetда бу муаммони ечишда ARP (Address Resolution Protocol) протоколидан фойдаланилади. Бу қуйдагича амалга оширилади: гармоқ ресурсларига биринчи мурожаат этилганида хост кенг кўламли ARP-сўровни жўнатади. Бу сўровни гармоқнинг берилган сегментидаги барча станциялар қабул қилади. Сўровни қабул қилиб, хост сўров юборган хост хусусидаги ахборотни ўзининг ARP-жадвалига киригади, сўнгра унга ўзининг Ethernet-манзили бўлган ARP-жавобни жўнатади. Агар бу сегментда бундай хост бўлмаса, гармоқнинг бошқа сегментларига мурожаатга имкон берувчи маршрутизаторга мурожаат қилинади. Агар фойдаланувчи ва нияти бузук одам бир сегментда бўлса, ARP-сўровни ушлаб қолиш ва ёлғон ARP-жавобни йўллаш мумкин бўлади. Бу усулнинг таъсири фақат битта

сегмент билан чегараланганлиги тасалли сифатида хизмат қилиши мумкин.

ARP билан бўлган ҳолга ўхшаб DNS-сўровни ушлаб қолиш йўли билан Internet тармоғига ёлғон DNS-серверни киритиш мумкин.

Бу қуйидаги алгоритм бўйича амалга оширилади:

1. DNS-сўровни кутиш.
2. Олинган сўровдан керакли маълумотни чиқариб олиш ва тармоқ бўйича сўров юборган хостга ёлғон DNS-жавобни ҳақиқий DNS-сервер номидан узатиш. Бу жавобда ёлғон DNS-сервернинг IP-манзили кўрсатилган бўлади.

3. Хостдан пакет олинганида пакетнинг IP-сарлавҳасидаги IP-манзилни ёлғон DNS сервернинг IP-манзилига ўзгартириш ва пакетни серверга узатиш (яъни ёлғон DNS-сервер ўзининг номидан сервер билан иш олиб боради).

4. Сервердан пакетни олишда пакетнинг IP-сарлавҳасидаги IP-манзилни ёлғон DNS-сервернинг IP-манзилига ўзгартириш ва пакетни хостга узатиш (ёлғон DNS серверни хост ҳақиқий хисоблайди).

Ёлғон маршрутни киритиш. Маълумки, замонавий глобал тармоқлари бир-бири билан *тармоқ узеллари* ёрдамида уланган тармоқ сегментларининг мажмуидир. Бунда *маршрут* деганда маълумотларни манбадан қабул қилувчига узатишга хизмат қилувчи тармоқ узелларининг кетма-кетлиги тушунилади. Маршрутлар хусусидаги ахборотни алмашишни унификациялаш учун маршрутларни бошқарувчи махсус протоколлар мавжуд. Internet-даги бундай протоколларга янги маршрутлар хусусида хабарлар алмашиш протоколи – ICMP (Internet Control Message Protocol) ва маршрутизаторларни масофадан бошқариш протоколи SNMP (Simple Network Management Protocol) мисол бўла олади. Маршрутни ўзгартириш ҳужум қилувчи ёлғон хостни киритишдан бўлак нарса эмас. Ҳатто, охириги объект ҳақиқий бўлса, ҳам маршрутни ахборот барибир ёлғон хостдан ўтадиган қилиб қуриш мумкин.

Маршрутни ўзгартириш учун ҳужум қилувчи тармоққа тармоқни бошқарувчи қурилмалар (масалан, маршрутизаторлар) номидан берилган тармоқни бошқарувчи протоколлар орқали аниқланган махсус хизматчи хабарларни жўнатиши лозим. Маршрутни муваффақиятли ўзгартириш натижасида ҳужум қилувчи тақсимланган тармоқдаги иккита объект алмашадиган ахборот оқими устидан тўла назоратга эга бўлади, сўнгра ахборотни ушлаб қолиши, таҳлиллаши, модификациялаши ёки оддийгина йўқотиши мумкин. Бошқача айтганда таҳдидларнинг барча турларини амалга ошириш имконияти туғилади.

Хизмат қилишдан воз кечишга ундайдиган тақсимланган хужумлар – DDoS (Distributed Denial of Service) компьютер жиноятчилигининг нисбатан янги хили бўлсада, кўркинчли тезлик билан тарқалмоқда. Бу хужумларнинг ўзи анчагина ёқимсиз бўлгани етмаганидиск, улар бир вақтнинг ўзида масофадан бошқарилувчи юзлаб хужум қилувчи серверлар томонидан бошланиши мумкин.

Хакерлар томонидан ташкил этилган узелларда DDoS хужумлар учун учта инструментал воситани топиш мумкин: trinoo, Tribe FloodNet (TFN) ва TFN2K. Яқинда TFN ва trinooning энг ёқимсиз сифатларини уйғунлаштирган яна биттаси stacheldraht («тикон симлар») пайдо бўлди.

1.2-расмда хизмат қилишдан воз кечишга ундайдиган хужум воситаларининг характеристикалари келтирилган.

Хизмат қилишдан воз кечишга ундайдиган оддий тармок хужумида хакер танлаган тизимига пакетларни жўнатувчи инструментидан фойдаланади. Бу пакетлар нишон тизимининг тўлиб тошиши ва бузилишига сабаб бўлиши керак. Кўпинча бундай пакетларни жўнатувчилар манзили бузиб кўрсатилади. Шу сабабли хужумнинг хақиқий манбасини аниқлаш жуда қийин.



1.2-расм. Хизмат қилишдан воз кечишга ундайдиган хужум воситаларининг характеристикалари.

DDoS хужумларини ташкил этиш битта хакернинг кўлидан келади, аммо бундай хужумнинг эффеќти *агентлар* деб аталувчи хужум қилувчи серверларнинг ишлатилиши ҳисобига анчагина кучаяди. TFNда *серверлар* (server), а тріноода *демонлар* (daemon) деб аталувчи бу агентлар хакер томонидан масофадан бошқарилади.

1.5. Ахборот хавфсизлигини бузувчининг модели

Бўлиши мумкин бўлган тахдидларни олдини олиш учун нафаќат операцион тизимларни, дастурий таъминотни химоялаш ва фойдаланишни назорат қилиш, балки бузувчилар туркумини ва улар фойдаланадиган усулларни аниқлаш лозим.

Сабаблар, маќсадлар ва усулларга боғлиқ ҳолда ахборот хавфсизлигини бузувчиларни тўртга категорияга ажратиш мумкин:

- саргузашт қидирувчилар;
- ғоявий хакерлар;
- хакерлар-профессионаллар;
- ишончсиз ходимлар.

Саргузашт қидирувчи, одатда, ёш, кўпинча талаба ёки юкори синф ўқувчиси ва унда ўйлаб қилинган хужум режаси камдан-кам бўлади. У нишонини тасодифан танлайди, кийинчиликларга дуч келса чекинади. Хавфсизлик тизимида нуксонли жойни топиб, у махфий ахборотни йиғишга тиришади, аммо ҳеч қачон уни яширинча ўзгартиришга уринмайди. Бундай саргузашт қидирувчи муваффаќиятларини фаќат якин дўстлари-касбдошлари билан ўртоқлашади.

Ғояли хакер – бу ҳам саргузашт қидирувчи, аммо мохиррок. У ўзининг эътикоди асосида муайян нишонларни (хостлар ва ресурсларни) танлайди. Унинг яхши кўрган хужум тури Web-сервернинг ахборотини ўзгартириши ёки жуда кам ҳолларда, хужум қили-нувчи ресурслар ишини блокировка қилиш. Саргузашт қиди-рувчиларга нисбатан ғояли хакерлар муваффаќиятларини кенгрок аудиторияда, одатда, ахборотни хакер Web-узелда ёки Usenet анжуманида жойлаштирилган ҳолда эълон қиладилар.

Хакер-профессионал ҳаракатларнинг аниқ режасига эга ва маълум ресурсларни мўлжаллайди. Унинг хужумлари яхши ўйланган ва одатда, бир неча босқичда амалга оширилади. Аввал у

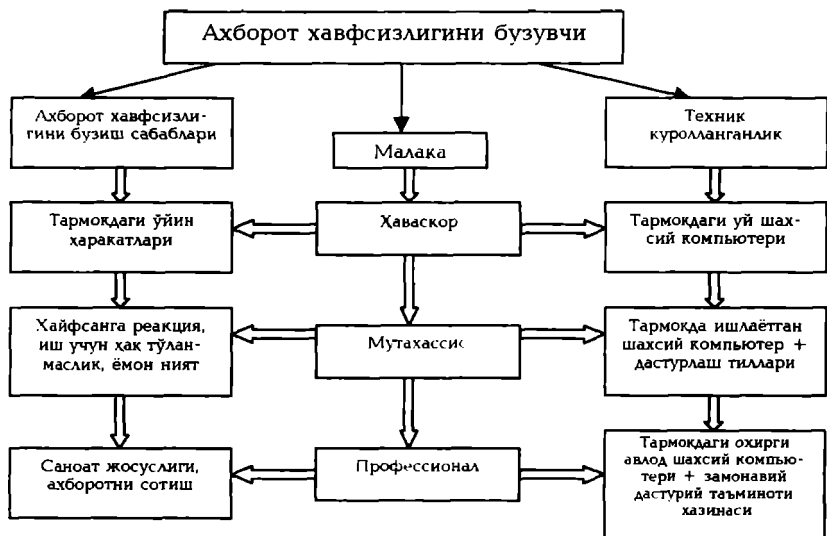
дастлабки ахборотни йиғади (операцион тизим тури, тақдим этиладиган сервислар ва қўлланиладиган химоя чоралари). Сўнгра у йиғилган маълумотларни ҳисобга олган ҳолда хужум режасини тузади ва мос инструментларни танлайди (ёки ҳатто ишлаб чиқади). Кейин, хужумни амалга ошириб, махфий ахборотни олади ва ниҳоят ҳаракатларининг барча изларини йўқ қилади. Бундай хужум қилувчи профессионал, одатда, яхши молияланади ва яқка ёки профессионаллар командасида ишлаши мумкин.

Ишончсиз ходим ўзининг ҳаракатлари билан саноат жосуси етказадиган муаммога тенг (ундан ҳам кўп бўлиши мумкин) муаммони туғдиради. Бунинг устига унинг борлигини аниқлаш мураккаброк. Ундан ташқари, унга тармокнинг ташқи химоясини эмас, балки фақат, одатда, унчалик катъий бўлмаган тармокнинг ички химоясини бартараф қилишига тўғри келади. Аммо, бу ҳолда унинг корпоратив маълумотлардан рухсатсиз фойдаланиши хавфи бошқа ҳар қандай нияти бузук одамникидан юқори бўлади.

Юқорида келтирилган ахборот хавфсизлигини бузувчилар категорияларини уларни малакалари бўйича гуруҳлаш мумкин: ҳаваскор (саргузашт кидирувчи), мутахассис (ғояли хакер, ишончсиз ходим), профессионал (хакер-профессионал). Агар бу гуруҳлар билан хавфсизликнинг бузилиши сабаблари ва ҳар бир гуруҳнинг техник қуролланганлиги таққосланса, ахборот хавфсизлигини бузувчининг умумлаштирилган моделини олиш мумкин (1.3-расм).

Ахборот хавфсизлигини бузувчи, одатда, маълум малакали мутахассис бўлган ҳолда компьютер тизимлари ва тармоқлари хусусан, уларни химоялаш воситалари хусусида барча нарсаларни бишлишга уринади. Шу сабабли бузувчи модели қуйидагиларни аниқлайди:

- бузувчи бўлиши мумкин бўлган шахслар категорияси;
- бузувчининг бўлиши мумкин бўлган нишонлари ва уларнинг муҳимлик ва хавфсизлик даражаси бўйича рутбаланиши;
- унинг малакаси хусусидаги тахминлар; унинг техник қуролланганлигининг баҳоси;
- унинг ҳаракат характери бўйича чеклашлар ва тахминлар.



1.3-расм. Ахборот хавфсизлигини бузувчининг модели.

Тизимдан рухсатсиз фойдаланишга мажбур этиш сабабларининг диапазони етарлича кенг: компьютар билан ўйнаганидаги ҳаяжон кўтаринкилигидан то жирканч менежер устидан ҳокимлик ҳиссиётигача. Бу билан нафакат кўнгил очишни хоҳловчи хаваскорлар, балки профессионал дастурчилар ҳам шуғулланади. Улар паролни танлаш, фараз килиш натижасида ёки бошқа хакерлар билан алмашиш йўли орқали кўлга киритадилар. Уларнинг бир қисми нафакат файлларни кўриб чиқади, балки файлларнинг мазмуни билан кизика бошлади. Бу жиддий таҳдид ҳисобланади, чунки бу ҳолда беозор шўхликни ёмон ният билан қилинган ҳаракатдан ажратиш қийин бўлади.

Яқин вақтгача раҳбарлардан норози хизматчиларнинг ўз мавқеларини сунистеъмол қилган ҳолда тизимни бузишлари, ундан бегоналарнинг фойдаланишларига йўл кўйишлари ёки тизимни иш ҳолатида қаровсиз қолдиришлари ташвишлангирар эди. Бундай ҳаракатларга мажбур этиш сабаблари қуйидагилар:

- ҳайфсанга ёки раҳбар томонидан танбехга реакция;
- иш вақтидан ташқари бажарилган ишга фирма ҳақ тўламаганидан норозилик;

– фирмани қандайдир янги тузилаётган фирмага ракиб сифатида заифлаштириш мақсадида қасос олиш каби ёмон ният.

Раҳбардан норози ходим жамоа фойдаланувчи ҳисоблаш тизимларига энг катта таҳдидлардан бирини туғдиради. Шунинг учун ҳам ҳакерлар билан курашиш агентлиги индивидуал компьютер сохибларига жон деб хизмат кўрсатадилар.

Профессионал ҳакерлар-ҳисоблаш техникасини ва алоқа тизимини жуда яхши биладиган компьютер фанатлари (мутаассиблари) ҳисобланади. Тизимга кириш учун профессионаллар омадга ва фарзга таянмайдилар ва қандайдир тартибни ва тажрибани ишлатадилар. Уларнинг мақсади-химояни аниқлаш ҳамда йўқотиш, ҳисоблаш қурилмасининг имкониятларини ўрганиш ва мақсадига эришиш мумкинлиги тўғрисида қарорга келиш.

Бундай профессионал ҳакерлар категориясига қуйидаги шахслар қиради:

– сиёсий мақсадни кўзловчи жиной гуруҳларга қирувчилар;

– саноат жосуслик мақсадларида ахборотни олишга уринувчилар;

– текин даромадга интилувчи ҳакерлар гуруҳи.

Умуман профессионал ҳакерлар ҳавф-хатарни минималлаштиришга уринадилар. Бунинг учун улар бирга ишлашга фирмада ишлайдиган ёки фирмадан яқинда ишдан бўшатишган ходимларни жалб этадилар, чунки бегона учун банк тизимига киришда ошкор бўлиш ҳавфи жуда катта. Ҳақиқатан, банк ҳисоблаш тизимларининг мураккаблиги ва юқори тезкорлиги, ҳужжатларни юргизиш ва текшириш усулларининг мунтазам такомиллаштирилиши бегона шахс учун хабарларни ушлаб қолиш ёки маълумотларни ўғирлаш мақсадида тизимга ўрнашишига имкон бермайди. Профессионал ҳакерлар учун яна бир қўшимча ҳавотир-тизимдаги бир компонентнинг ўзгариши бошқа бир компонентнинг бузилишига олиб келиши ва хатардан дарак берувчи сигналга сабаб бўлиши мумкин.

Ҳакерлар ҳавф-хатарни қамайтириш мақсадида одатда, молиявий ва оилавий муаммоларга эга бўлган ходимлар билан алоқага қирадилар. Кўпгина одамлар ҳаётида ҳакерлар билан гўкнаш-масликлари мумкин, аммо алкаголга ёки қиморга ружу қўйган ходимлар билмасдан жиной гуруҳ билан боғланган қандайдир бир букмекердан қарздор бўлиб қолишлари мумкин. Бундай ходим қандайдир ўйин-қулги кечасида суҳбатдошининг профессионал

агент эканлигига шубҳа қилмаган ҳолда ортиқча гапириб юбориши мумкин.

1.6. Internet – хизматлар ва электрон бизнес тизимларида хавфсизлик муаммолари

Ҳозирда Internet-хизматининг қуйидаги тижорат шакллари кенг тарқалган:

- Internet-банкинг;
- Internet-трейдинг;
- Internet-суғурта;
- ASP иловаларини ижарага бериш бўйича хизмат кўрсатиш.

Internet-банкинг. Замонавий Internet-технологиялар банкларга хизматларининг бир қисмини янги савияга ўтказишга ва шу орқали янги миқозларни жалб этишга ва уларга хизмат қилиш харажатларини пасайтиришга имкон яратади. Анъанавий банкларнинг аксарияти ўз миқозларига электрон хизмат қилиш ва сўт тўловининг қўшимча шакллари тавсия этади. Фақат Internetда иш юритувчи банклар нисбатан яқинда пайдо бўлди. Улар Web-банклар деб аталади. Энг йирик Web-банклар сирасига First Internet Bank, Net-Bank, CompuBank ва катор бошқа банклар тааллуқли.

Internet-банкинг деганда, одатда, миқозга оддий компьютер ёрдамида стандарт браузерни ишлатиб банк сўтидан Internet орқали тўғридан-тўғри фойдаланиш имкониятининг берилиши тушунилади. Internet-банкинг тизимининг намунали варианты миқозларга банк офисларидаги физик шахсларга (табиийки, нақд пул билан бажариладиган амаллар бундан истисно) тақдим этилувчи банк хизматининг тўлиқ тўпламини ўз ичига олади.

Ҳозирда Internet-банкинг хизмати ҳар бири Internet орқали амалга оширилувчи қуйидаги имкониятларга эга:

- нақд пулсиз ҳисоб-китобларни бажариш;
- коммунал хизматлар учун тўлови;
- Internetдан фойдаланиш учун тўлови;
- уяли ва пейджинг алоқа операторлари сўтларини тўлаш;
- ички ва банклараро ҳужжат асосидаги тўловларни бажариш;
- ўз сўтлари бўйича маблағларни ўтказиш;
- исталган вақт оралиғи учун ўз сўтлари бўйича барча банк амалларини кузатиш.

Internet-банкинг тизимидан фойдаланиш мижозларга қатор имтиёзлар беради:

- фоизли ставкалари нисбатан юкори;
- шахсан банкка бориш зарурияти йўқлиги ҳисобидан мижознинг вақти жиддий тежалади;
- мижоз суткада 24 соат шахсий счётини назоратлаш ва молия бозоридаги вазиятнинг ўзгаришига тездан реакция кўрсатиш имкониятига эга.

Internet-банкинг тизимлари пластик карталар бўйича амалга ошириладиган амалларни кузатишда жуда асқотади-карта ҳисобидан маблағни чиқариш тизимлар томонидан тайёрланган ҳисоблар бўйича кўчирмада дарҳол акслантирилади. Бу мижозга ўз амалларини назоратлашда қулайлик туғдиради.

Internet-трейдинг. Internet-технологиялар фонд бозори учун жуда истикболли. Internet-технологиялар туфайли, дунёда бўш капитални кўйишнинг энг яхши усули сифатида тан олинган кимматбаҳо қоғозларни сотиб олиш, ҳозирда барча хоҳловчилар учун осон. Internet-трейдинг инвесторларни битимларни тузишнинг соддалиги ва онлайн-брокерларнинг хизматига таърифларнинг пастлиги билан ўзига жалб қилади.

Internetнинг замонавий имкониятлари кўчмас мулк билан бўладиган амалларни (сотиб олиш, сотиш, алмаштириш, мерос бўйича бериш, ижарага бериш ва х.) аъъанавий шаклларига нисбатан айтарлича енгиллаштириш ва тезлаштиришга имкон беради. Мижоз уйдан чикмасдан кўчмас мулкни сотиб олиши ва сотиши, мутахассис маслаҳатини олиши мумкин. Бу амалларни бажариш учун компьютери, Internetдан фойдалана олиши ва банкда счёти бўлиши кифоя.

Internet-суғурта. Суғурталаш деганда суғурталанувчи-мижоз (суғурта хизматларини сотиб олувчи) билан суғурталовчи (бундай хизматларни тақдим этувчи) ўртасида шартнома муносабатларини ўрнатиш ва мададлаш тушунилади. Суғурталовчи суғурта дастурини ишлаб чиқади ва аниқлайди, мижозга таклиф этади, агар суғурталанувчи рози бўлса иккала томон шартнома тузади. Мижоз бирданига ва мунтазам тўловларни амалга оширади, суғурталовчи, ўз навбатида, суғурта ҳолат келиши билан суғурталанувчига суғурта шартномаси шартлари бўйича компенсация пулини тўлашга мажбурият олади.

Битимга келишиш жараёнида суғурта полиси деб аталувчи хужжат шакллантирилади. Бу хужжат суғурталовчи ва суғурта компанияси учун юридик хужжат ҳисобланади. Унда суғурта объекти (мол-мулк, одам, масъулият), суғурталанувчи ҳолат, суғурта муддатининг бошланиши ва ниҳояси, суғурта суммаси, суғурта мукофоти каби муҳим томонлари олдиндан айтиб ўтилади.

Ривожланган мамлакатлар суғурта компанияларида суғурта полисларини амалга оширувчи Internet-каналлар мавжуд.

ASP иловаларини ижарага бериш бўйича хизмат кўрсатиш. Янги иктисодиёт ривожининг истикболли йўналишларидан бири ASP (Applications Service Providing) иловаларини ижарага бериш бўйича хизмат кўрсатишдир. Internet ёки хусусий тармоқ орқали фойдаланувчидан узоқдаги серверда жойлашган иловалардан фойдаланишни ASP иловалари амалга оширади.

ASP иловаларининг провайдери ўзининг серверларига иловаларнинг дастурий таъминотини ўрнатади ва улардан миқдорларнинг фойдаланишини таъминлайди. Миқдор компьютерига бундай дастурий таъминотни ўрнатиши, уни янгилashi, захира нусхалashi ва шарт эмас. Барча ишларни ASP провайдери бажаради. Миқдор провайдерга иловалардан фойдалангани учун ижара ҳақини тўлайди.

Компанияларнинг ASP хизматларидан фойдаланишининг сабаби куйидагилар:

- компания эҳтиёж сезган энг янги технологиялардан хавф-хатарсиз, катта харажатсиз ва маъмурий жавобгарсиз фойдаланиш;
- иловалардан тезда фойдаланиш зарурияти;
- агар компанияни илова қандайдир сабабларга тўла қониктирмаса, осонгина воз кечиш имконияти.

Яқин йилларда ASP бозорининг тез ўсиши кутилмоқда. Бу эса, ўз навбатида, барча компанияларга исталган бизнес-иловалардан бир хилда фойдаланишни тақдим этиш орқали, бизнес ривожидан барқарорликни таъминлайди. Аксарият аналитикларнинг фикрича, кейинчалик ASP модели бизнес иловалардан фойдаланиш усулларининг орасида устунлик қилиши мумкин.

Электрон бизнес харидор ва сотувчи орасидаги алоқани ташкил этиш, буюртмани ифодалаш, муҳокама қилиш, ўзгартириш, товарларни ва хизматларни сотиш усулларини ҳамда тўловни амалга ошириш жараёнларини ўзгартириш учун янги технологиялардан фойдаланади. Ҳозирда электрон тижорат ва бизнеснинг аксарият муаммолари ахборот хавфсизлиги билан боғлиқ, яъни хавфсизлик

муаммолари электрон тижорат ва бизнес ривождаги жиддий тўсик ҳисобланади.

Ҳар қандай тижорат компаниясининг бошқа компаниялар билан ёки ушбу компаниянинг бўлимлари орасида алоқа ўрнатилиши зарур. Ҳозирда глобал Internet тармоғи ўзининг узеллари ўртасида ишончли ва арзон ахборот алмашинувини таъминлайди. Очiq глобал Internet тармоғи каналларидан фаол фойдаланувчи электрон бизнеснинг ишлаши жараёнида кўпгина хавф-хатарлар пайдо бўлади.

Internetдан фойдаланиш каналлари компаниянинг ахборот ресурсларидан четдан фойдаланишга имкон бериши мумкин. Коммуникацион, хусусан HTTP – протокол асосидаги дастурлардан эҳтиётсизлик билан фойдаланиш ахборот тизимининг ишга лаёқатлигини бузувчи ва ёки ахборот тизими маълумотларини бузувчи махсус дастур – «троян отларининг» киришига олиб келиши мумкин. Бу хил дастурларнинг ичида вируслар кенг тарқалган. Ўзига хос малакали мутахассислар корпоратив ахборот тармоқларига билинмасдан кириш учун кўпинча умуммаксад тармоқлардан фойдаланадилар.

Электрон кутисининг тез-тез ишлатилиши нияти бузук одамларга электрон бизнес билан шуғулланувчи ташкилот фойдаланувчилари номларини обрўсизлантиришга ёрдам бериши мумкин. Фойдаланувчилар маълумотларини (исмлар, пароллар, PIN – кодлар ва х.) сақловчи тизимининг заиф жойларини кидиришдан тармоқда кенг ишлатилувчи махсус дастурлардан фойдаланиш мумкин.

Internet конфиденциал ахборотни дунёнинг исталган нуктасига юбориши мумкин, аммо у етарлича химояланмаган бўлса, ушлаб қолиниши, нусхалаштирилиши, ўзгартирилиши ҳамда ҳар қандай четдаги фойдаланувчилар – нияти бузук одамлар, рақиблар ва оддий кизикувчилар томонидан ўкилиши мумкин. Масалан, етарлича химояланмаган тўлов топшириғи ёки кредит карточка номерини жўнатаётганда эсда тутиш лозимки, жўнатиш хусусий/шахсий тармоқ орқали амалга оширилмаяпти ва четдаги фойдаланувчилар хабарингизни манипуляция қилиш имкониятига эга. Ундан ташқари хабарингиз алмаштирилиб қўйилиши мумкин: хабарларни худди *B* фойдаланувчидан юборилганидек *A* фойдаланувчидан юбориш усуллари мавжуд. Internet тармоғи махсус пакет, тамомила қонуний пакетлар, сонининг ҳаддан ташқари кўплиги узатишдаги

бузилишлар, тармоқ компонентларининг носозлиги туфайли ишга лаёқат бўлмаслиги мумкин. Бундай ҳоллар «хизмат қилишдан воз кечиш» деб аталади ва электрон тижорат учун энг жиддий таҳдид ҳисобланади. 2.2-жадвалда ахборот хавфсизлиги бузилишининг статистикаси келтирилган [24].

2.2-жадвал

Ахборот хавфсизлиги бузилишининг турлари	Қайд этилганлиги %	Йўқотишлар %
Корпоротив тармоқдан рухсатсиз четдан фойдаланиш	44	25
Хизмат қилишдан воз кечиш	32	28
Узатишда маълумотларни алмаштириш	17	18
Фаол тинглаб кўриш	2	1
Тармоқдан рухсатсиз ички фойдаланиш	97	62
Ахборотдан рухсатсиз ички фойдаланиш	55	32

Ахборот хавфсизлиги электрон бизнес тизимининг энг муҳим элементларидан бири ҳисобланади ва усуллар ва воситаларнинг бутун бир тўплами ёрдамида таъминланиши шарт. Электрон тижорат соҳасидаги савдо кўлами Internet хавфсизлиги масалаларидан ташвишланган харидорлар, сотувчилар ва молия институтларининг бошидан кечирувчи кўркувлари билан чегараланади. Бу кўркувлар, хусусан, қуйидагиларга асосланади:

- конфиденциалликка кафолатнинг йўқлиги-кимдир маълумотларингизни узатилаётганида ушлаб қолиши ва кийматли ахборотни (масалан, кредит карточкангизнинг рақамларини, товар отказиб бериш санаси ва манзил) топишга уриниши мумкин;

- амалда иштирок этувчиларни текшириш даражасининг етарли эмаслиги – транзакция катнашчилари текширилмаганида томонларнинг бири «маскарад» уюштириши мумкинки, унинг оқибати йккинчи томонга анча қимматга тушади. Масалан, харидор сайтга кириб ундаги компаниянинг ҳақиқийлигига шубҳа қилади, шундай

хол ҳам рӯй бериши мумкинки, харидор кредит карточкасининг рақамларини етарлича ваколатга эга бўлмаган шахсга беради;

– сотувчида буюртма берган харидор кредит карточкасининг конуний эгаси эканлигинининг текшириш имкони йўк;

– кредит карточкасининг банк-эмитенти тўловни бажаришга талаб қўйган сотувчини текширишни истаб қолиши мумкин;

– маълумотлар яхлитлигига кафолат йўк – ҳатто маълумотларни жўнатувчи идентификацияланган бўлсада, учинчи томон маълумотларни, улар узатилиши вақтида, ўзгартириш имкониятига эга.

Ахборот хавфсизлигини таъминлаш нуктаи назаридан электрон тижоратнинг намунавий қўлланилишини – Internet орқали маҳсулотга ва хизматларга эга бўлишни кўрайлик. Ушбу жараён куйидаги босқичлар орқали ифодаланиши мумкин.

1. Буюртмачи Web-сервер орқали маҳсулот ёки хизматни танлайди ва мос буюртмани расмийлаштиради.

2. Буюртма магазиннинг буюртмалар маълумотлари банкига киритилади.

3. Буюртма берилган маҳсулот ёки хизматни олиш мумкинлиги маълумотларнинг марказий базаси орқали текширилади.

4. Агар маҳсулотнинг олиниши мумкин бўлмаса, буюртмачи у тўғрида огоҳлантирилади ва маҳсулот ёки хизматга эга бўлиш жараёни тўхтатилади. Маҳсулотга сўров бошка складга (буюртмачи розилигида) йўналтирилиши мумкин.

5. Агар маҳсулот ёки хизмат мавжуд бўлса буюртмачи тўловни тасдиқлайди ва буюртма мос маълумотлар базасига киритилади. Электрон магазин мижозга буюртма тасдиғини юборади. Кўпгина ҳолларда (айникса, эндигина иш бошлаган компанияларда) буюртмалар, таварларнинг борлигини текшириш ва ҳ. учун ягона маълумотлар базаси мавжуд.

6. Мижоз онлайн режимида буюртма ҳақини тўлайди.

7. Товар буюртмачига стқазилади.

Электрон тижорат билан шуғулланадиган компаниялар юкорида келтирилган босқичларда дуч келадиган таҳдидлар куйидагилар:

– электрон магазин Web-сайтининг саҳифасини алмаштириб қўйиш. Бу таҳдидни амалга оширишнинг асосий усули – фойдаланувчи сўровини бошка серверга йўллаш. Бу таҳдид олтинчи

боскичда буюртмачи кредит карточкасининг рақамини киритганда кучаяди;

- ёлгон буюртмалар бериш ва электрон магазин ходимлари томонидан фирибгарлик қилиш. Ҳозирда ички/ташки таҳдидлар муносабати 60/40 %ни ташкил этади;

- электрон тижорат тизимида узатиладиган маълумотларни ушлаб қолиш. Буюртмачининг кредит картаси хусусидаги ахборотни ушлаб қолиш ўзгача хавф-хатарни туғдиради;

- компаниянинг ички тармоғига кириш ва электрон магазин компонентларини обрўсизлантириш;

- «хизмат қилишдан воз кечиш» (denial of service) ҳужумини амалга ошириш ва электрон тижорат ишлашини ёки унинг узелини бузиш.

Ушбу таҳдидлар натижасида компания – электрон битим провайдери – мижозлар ишончини йўқотади, моддий зарар кўради. Баъзи ҳолларда бу компанияларга кредит карточка рақами фош қилинган учун даъво қўзғатилиши мумкин. «Хизмат қилишдан воз кечиш» ҳужуми натижасида электрон магазиннинг ишлаши бузилиши мумкин, унинг ишга лаёқатлилигини тиклашга инсон, вақт ва материал ресурслари талаб этилади.

II боб. АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ АСОСИЙ ЙЎЛЛАРИ

2.1. Ахборотни ҳимоялаш концепцияси

Нияти бузук одамларни ёлғиз фойдаланувчилар эмас, балки корпоратив компьютер тармоқлари кизиктиради. Айнан бундай тармоқларда ахборотнинг йўқолиши, рухсатсиз модификацияланиши жиддий оқибатларга олиб келиши мумкин.

Компьютер тармоқларини ҳимоялаш уйда фойдаланувчи компьютерларни ҳимоялашдан фаркланади (гарчи индивидуал ишчи станцияларни ҳимоялаш-тармоқ ҳимоясининг ажралмас қисми). Чунки, аввало, бундай масала билан саводли мутахассислар шуғулланадилар. Шу билан бирга корпоратив тармоқ хавфсизлиги тизимининг асосини четки фойдаланувчилар учун ишлаш қулайлиги ва техник мутахассисларга қўйиладиган талаблар ўртасида мурасага етишиш ташкил этади.

Компьютер тизимига икки нуқтаи назардан қараш мумкин: унда фақат ишчи станциялардан фойдаланувчиларни кўриш мумкин, ёки фақат тармоқ операцион тизимининг ишлашини ҳисобга олиш мумкин.

Симлар бўйича ўтувчи ахборотли пакетлар мажмуини ҳам компьютер тармоғи дейиш мумкин. Тармоқни ифодалашнинг бир неча сатҳлари мавжуд. Худди шундай тармоқ хавфсизлиги муаммосига турли сатҳларда ёндашиш мумкин. Мас ҳолда ҳар бир сатҳ учун ҳимоялаш усули турлича бўлади. Тизимнинг ишончли ҳимояланиши ҳимояланган сатҳлар сони билан белгиланади.

Биринчи, кўриниб турган ва амалда энг кийин йўл-ҳодимларни тармоқ ҳужумларини кийинлаштирувчи хатти-ҳаракатга ўргатиш. Бу бир қарашда осондай туюлсада, аммо мушкул иш. Internet дан фойдаланишни чегаралаш лозим. Аксарият фойдаланувчилар чегараланишлар сабабини билмайдилар. Шунинг учун тақиклар аниқ ифодаланиши лозим.

Тармоқда ахборотни ҳимоялашнинг зарурий даражасини ишлаб чиқишда ҳодимлар ва раҳбариятнинг ўзаро жавобгарлиги, шахс

ва ташкилот манфаатларига риоя қилиш, ҳуқуқни муҳофаза қилувчи органлар билан ўзаро алоқа ҳисобга олинади. Рақобатли шароитда хизматларнинг катта сонини тақдим этиш ва хизмат қилиш вақтини қисқартириш орқали етакчи ўринни сақлаб қолиш ва янги миқозларни жалб этиш мумкин. Бунга фақат барча амалларни автоматлаштиришнинг зарурий даражасини таъминлаш эвазига эришиш мумкин. Айни замонда ҳисоблаш техникасининг ишлатилиши билан нафақат пайдо бўлган муаммолар ҳал этилади, балки ахборотни бузилиши ва йўқотилиши, тасодифан ва атайин модификацияланиши ҳамда ахборотни бегоналар тарафидан рўқсатсиз олинishi билан боғлиқ янги ноанъанавий таҳдидлар пайдо бўлади.

Компьютер тармоқлари ахборотини химоялашга химоялаш тадбирларининг ягона сиёсатини ҳамда ҳуқуқий, ташкилий-маъмурий ва инженер-техник характерга эга чоралар тизимини ўтказиш орқали эришилади.

Мавжуд ҳолатнинг таҳлили кўрсатадики, ахборотни химоялаш учун қилинадиган тадбирлар даражаси, одатда, автоматлаштириш даражасидан паст. Бундай орқада қолиш жиддий оқибатларга олиб қелиши мумкин.

Автоматлаштирилган комплексларда ахборотнинг заифлигига ҳисоблаш ресурсларининг концентрацияланиши, уларнинг ҳудудий тақсимланганлиги, магнит элтувчиларида маълумотларнинг катта ҳажмини узоқ вақт сақланиши, кўпгина фойдаланувчиларнинг ресурслардан бир вақтда фойдаланиши сабаб бўлади.

Бундай шароитда химоялаш чораларини кўриш заруриятига шубҳа қилмаса бўлади. Аммо қуйидаги қийинчиликлар мавжуд:

- ҳозирги кунда химояланган тизимларнинг ягона назарияси йўқ;

- химоя воситаларини ишлаб чиқарувчилар хусусий масалаларни ечиш учун асосан алоҳида компонентларни тавсия этадилар, химоялаш тизимини шакллантириш ва бу воситаларнинг бирга ишлатилиши масалалари эса истеъмолчи ихтиёрига қолдирилади;

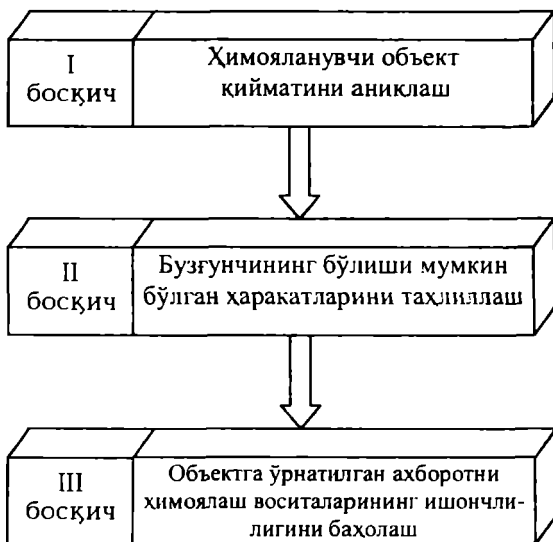
- ишончли химояни таъминлаш учун техник ва ташкилий муаммолари комплексини ҳал этиш ва мос ҳужжатларни ишлаб чиқиш зарур.

Юқорида санаб ўтилган қийинчиликларни бартараф қилиш учун нафақат алоҳида корхона, балки давлат даражасидаги ахборот жараёнларида иштирок этувчилари характерининг координацияси

зарур. Ахборот хавфсизлигини таъминлаш етарлича жиддий масала. Шунинг учун, аввало, ахборот хавфсизлиги концепциясини ишлаб чиқиш зарур. Концепцияда миллий ва корпоратив манфаатлар, ахборот хавфсизлигини таъминлаш принциплари ва мададлаш йўллари аниқланади ва уларни амалга ошириш бўйича масалалар таърифланади.

Концепция – ахборот хавфсизлиги муаммосига расмий қабул қилинган қарашлар тизими ва уни замонавий тенденцияларни ҳисобга олган ҳолда ечиш йўллари. Концепцияда ифодаланган мақсадлар, масалалар ва уларни бўлиши мумкин бўлган ечиш йўллари асосида ахборот хавфсизлигини таъминлашнинг муайян режалари шакллантирилади.

Концепцияни ишлаб чиқишни уч босқичда амалга ошириш тавсия этилади (2.1-расм).



2.1-расм. Ахборот химояси концепциясини ишлаб чиқиш босқичлари.

Биринчи босқичда химоянинг максадли кўрсатмаси, яъни қандай реал бойликлар, ишлаб чиқариш жараёнлари, дастурлар, маълумотлар базаси химояланиши зарурлиги аниқланиши шарт. Ушбу босқичда химояланувчи алоҳида объектларни аҳамияти бўйича табақалаштириш максадга мувофиқ ҳисобланади.

Иккинчи босқичда химояланувчи объектга нисбатан бўлиши мумкин бўлган жиний ҳаракатлар таҳлиланиши лозим. Иқтисодий жосуслик, терроризм, саботаж, бузиш орқали ўтирлаш каби кенг тарқалган жиноятчиликларнинг реал хавф-хатарлик даражасини аниқлаш муҳим ҳисобланади. Сўнгра, нияти бузук одамларнинг химояга муҳтож асосий объектларга нисбатан ҳаракатларининг эҳтимоллигини таҳлиллаш лозим.

Учинчи босқичнинг бош масаласи—вазоятни, хусусан ўзига хос маҳаллий шароитни, ишлаб чиқариш жараёнларини, ўрнатиб қўйилган химоянинг техник воситаларини таҳлиллашдан иборат.

2.2. Ахборот химоясининг стратегияси ва архитектураси

Ахборот хавфсизлиги стратегияси ва химоя тизими архитекту-раси (2.2-расм) ахборот хавфсизлиги концепцияси асосида ишлаб чиқилади.

Ахборот хавфсизлиги бўйича тадбирлар комплексининг асоси-ни ахборот химоясининг стратегияси ташкил этиши лозим. Унда ишончли химоя тизимини куриш учун зарурий максадлар, мезон-лар, принциплар ва муолажалар аниқланади. Яхши ишлаб чиқилган стратегияда нафақат химоя даражаси, раҳналарни кидириш, бренд-мауэрлар ёки ргоху-серверлар ўрнатиладиган жой ва х. ўз аксини топиши лозим, балки ишончли химояни кафолатлаш учун уларни ишлатиш муолажалари ва усуллари ҳам аниқланиши лозим.

Ахборот химояси умумий стратегиясининг муҳим хусусияти хавфсизлик тизимини тақиклашдир. Иккита асосий йўналишни аж-ратиш мумкин:

- химоя воситаларининг таҳлили;
- хужум бўлганини аниқлаш.



2.2-расм. Ахборот хавфсизлигини таъминлаш иерархияси.

Ахборот хавфсизлигини таъминлаш иерархиясидаги иккинчи масала сиёсатни аниқлашдир. Унинг мазмуни энг рационал воситалар ва ресурслар, кўрилаётган масала мақсади ва унга ёндашиш ташкил этади. Ҳимоя сиёсати-умумий ҳужжат бўлиб, унда фойдаланиш қоидалари санаб ўтилади, сиёсатни амалга ошириш йўллари аниқланади ва ҳимоя муҳитининг базавий архитектураси тавсифланади. Бу ҳужжат матннинг бир нечта саҳифаларидан иборат бўлиб, тармоқ физик архитектурасини шакллантиради, ундаги ахборот эса ҳимоя маҳсулотини танлашни аниқлайди.

2.3. Ахборот хавфсизлигининг сиёсати

Ахборот хавфсизлигининг сиёсатини ишлаб чиқишда, аввало, химоя қилинувчи объект ва унинг вазифалари аниқланади. Сўнгра душманнинг бу объектга қизиқиши даражаси, ҳужумнинг эҳтимолли турлари ва кўриладиган зарар баҳоланади. Ниҳоят, мавжуд қарши таъсир воситалари етарли химояни таъминламайдиган объектнинг заиф жойлари аниқланади.

Самарали химоя учун ҳар бир объект мумкин бўлган таҳдидлар ва ҳужум турлари, махсус инструментлар, қуроллар ва портловчи моддаларнинг ишлатилиши эҳтимоллиги нуқтаи назаридан баҳоланиши зарур. Таъкидлаш лозимки, нияти бузук одам учун энг қимматли объект унинг эътиборини тортади ва эҳтимолли нишон бўлиб хизмат қилади ва унга қарши асосий қучлар ишлатилади. Бунда хавфсизлик сиёсатининг ишлаб чиқилишида ечими берилган объектнинг реал химоясини таъминловчи масалалар ҳисобга олиниши лозим.

Қарши таъсир воситалари химоянинг тўлиқ ва эшелонланган концепциясига мос келиши шарт. Бу дегани, қарши таъсир воситаларини марказида химояланувчи объект бўлган концентрик доираларда жойлаштириш лозим. Бу ҳолда душманнинг исталган объектга йўли химоянинг эшелонланган тизимини кесиб ўтади. Мудофаанинг ҳар бир чегараси шундай ташқи қилинадик, кўриклаш ходимининг жавоб чораларини кўришига етарли вақт мобайнида ҳужумчини ушлаб туриш имкони бўлсин.

Сўнги босқичда қарши таъсир воситалари қабул қилинган химоя концепциясига биноан бирлаштирилади. Бутун тизим ҳаёти циклининг бошланғич ва қутилувчи умумий нархини дастлабки баҳолаш амалга оширилади.

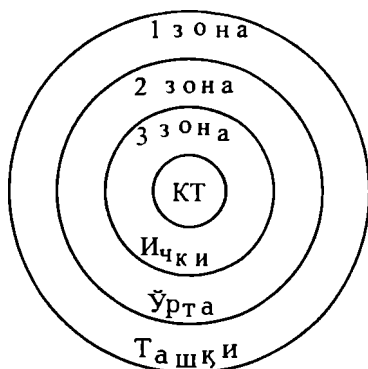
Агар бир бионинг ичида турли химоялаш талабларига эга бўлган объектлар жойлашган бўлса, бино отсек (бўлма)ларга бўлинади. Шу тариқа умумий назоратланувчи макон ичида ички периметрлар ажратилади ва руҳсатсиз фойдаланишдан ички химоя воситалари яратилади. Периметр, одатда, физик тўсиқлар орқали аниқланиб, бу тўсиқлардан ўтиш электрон усул ёки кўриклаш ходимлари томонидан бажарилувчи махсус муолажалар ёрдамида назоратланади.

Умумий чегарага ёки периметрга эга бўлган бинолар гуруҳини химоялашда нафақат алоҳида объект ёки бино, балки унинг жойла-

ниш жойи ҳам ҳисобга олиниши зарур. Кўп сонли бинолари бўлган ер участкалари хавфсизликни таъминлаш бўйича умумий ёки қисман мос келадиган талабларга эга бўлади, баъзи участкалар эса периметр бўйича тўсикка ва ягона йўлакка эга. Умумий периметр ташкил этиб, ҳар бир бинодаги химоя воситаларини камайтириш ва уларни фақат хужум қилиниши эҳтимоли кўпроқ бўлган муҳим объектларга ўрнатиш мумкин. Худди шу тарика участкадаги ҳар бир иморат ёки объект хужумчини ушлаб қолиш имконияти нуқтаи назаридан баҳоланади.

Юқоридаги келтирилган талаблар таҳлили кўрсатадики, уларнинг барчаси ахборотни ишлаш ва узатиш қурилмаларидан ҳуқуқсиз фойдаланиш, ахборот элтувчиларини ўғирлаш ва саботаж имкониятини йўл қўймасликка олиб келади.

Бинолар, иморатлар ва ахборот воситаларининг хавфсизлик тизимини назорат пунктларини бир зонадан иккинчи зонага ўтиш йўлида жойлаштирган ҳолда концентрик ҳалқа кўринишида ташкил этиш мақсадига мувофиқ ҳисобланади (2.3-расм).



1-зона. Компьютер тармоғи (КТ) хавфсизлигининг ташқи зонаси.

Таъминланиши: – физик тўсиклар:

– периметр бўйлаб ўтиш жойлари:

– ҳудудга кириш назоратининг ноавтоматик тизими;

2-зона. КТ хавфсизлигининг ўртадаги зонаси.

Таъминланиши: – эшиклари электрон химояланган назорат пунктлари:

– видеокузатиш;

– бўм бўш зоналарни чиқариб ташлаш;

3-зона. КТ хавфсизлигининг ички зонаси.

Таъминлаш:

– шахсий компьютерга фойдаланиш фақат назорат тизими орқали;

– идентификациялашнинг биометрик тизими.

2.3-расм. Бинодаги компьютер тармоғининг хавфсизлик тизими.

Ахборот хизмати бинолари ва хоналарига киришнинг назорати масаласига келсак, асосий чора-нафақат бино ва хоналарни, балки воситалар комплексини, уларнинг функционал вазифалари бўйича ажратиш ва яққалаш. Бино ва хоналарга киришни назоратловчи автоматик ва ноавтоматик тизимлар ишлатилади. Назорат тизими кундузи ва кечаси кузатиш воситалари билан тўлдирилиши мумкин.

Хавфсизликнинг физик воситаларини танлаш ҳимояланувчи объектнинг муҳимлигини, воситаларга кетадиган харажатни ва назорат тизими ишончлилиги даражасини, ижтимоий жиҳатларни ва инсон нафси бузуклигини олдиндан ўрганишга асосланади. Бармоқ, кафтлар, кўз тўр пардаси, қон томирлари излари ёки нутқни аниқлаш каби биометрик идентификациялаш ишлатилиши мумкин. Шартнома асосида техник воситаларга хизмат кўрсатувчи ходимларни объектга киритишнинг махсус режими кўзда тутилган. Бу шахслар идентификацияланганларидан сўнг объектга кузатувчи ҳамроҳлигида киритилади. Ундан ташқари, уларга аниқ келиш режими, мақоний чегараланиш, келиб-кейтиш вақти, бажарадиган иш характери ўрнатилади.

Нихоят, бино периметри бўйича бостириб киришни аниқловчи турли датчиклар ёрдамида комплекс кузатиш ўрнатилади. Бу датчиклар объектни қўриқлашнинг марказий пости билан боғланган ва бўлиши мумкин бўлган бостириб кириш нукталарини, айниқса ишланмайдиган вақтларда, назорат қилади.

Вақти-вақти билан эшиклар, ромлар, том, вентиляция туйнуклари ва бошқа чиқиш йўлларининг физик ҳимояланиш ишончлилигини текшириб туриш лозим.

Хар бир хонага ичидаги нарсанинг муҳимлилигига боғлиқ фойдаланиш тизимига эга бўлган зона сифатида қаралади. Кириш-чиқиш ҳуқуқи тизими шахс ёки объект муҳимлигига боғлиқ ҳолда селекцияли ва даражалари бўйича рутбаланган бўлиши шарт. Кириш-чиқиш ҳуқуқи тизими марказлашган бўлиши мумкин (рухсатларни бошқариш, жадвал ва календар режаларининг тузилиши, кириш-чиқиш ҳуқуқининг ёзма намуналари ва х.).

Назорат тизимини вақти-вақти билан текшириб туриш ва уни доимо ишга лаёқатли ҳолда сақлаш лозим. Буни ихтисослашган бўлинмалар ва назорат органлари таъминлайди.

Шахсий компьютер ва физикавий ҳимоя воситалари каби ўлчамлари кичик асбоб-ускуналарни кўзда тутиш мумкин.

Юкорида келтирилганларга хулоса килиб, компьютер тармоқларини химоялашда ахборот хавфсизлиги сиёсати қандай аниқланиши хусусида сўз юритамиз. Одатда, кўп сонли фойдаланувчиларга эга бўлган корпоратив компьютер тармоқлари учун махсус «хавфсизлик сиёсати» деб аталувчи, тармоқда ишлашни маълум тартиб ва қоидаларга бўйсундирувчи (регламентловчи) ҳужжат тузилади.

Сиёсат одатда, икки қисмдан иборат бўлади: умумий принциплар ва ишлашнинг муайян қоидалари. Умумий принциплар Internetда хавфсизликка ёндашишни аниқласа, қоидалар нима руҳсат этилишини ва нима руҳсат этилмаслигини белгилайди. Қоидалар муайян муолажалар ва турли қўлланмалар билан тўлдирилиши мумкин.

Одатда, хавфсизлик сиёсати тармоқ асосий сервисларидан (электрон почта, WWW ва х.) фойдаланишни регламентлайди ҳамда тармоқдан фойдаланувчиларни улар қандай фойдаланиш ҳуқуқига эга эканликлари билан таништиради. Бу эса ўз навбатида фойдаланувчиларни аутентификациялаш муолажасини аниқлайди.

Бу ҳужжатга жиддий ёндашиш лозим. Химоянинг бошқа барча стратегияси хавфсизлик сиёсатининг қатъий бажарилиши тахминига асосланган. Хавфсизлик сиёсати фойдаланувчилар томонидан кўпгина маломат орттирилишига сабаб бўлади, чунки унда фойдаланувчига ман этилган нарсалар очиқ-ойдин ёзилган. Аммо хавфсизлик сиёсати расмий ҳужжат, у бир томондан Internet тақдим этувчи сервисларда ишлаш зарурияти, иккинчи томондан мос мутахассис-профессионаллар тарафидан ифодаланган хавфсизлик талаблари асосида тузилади.

Автоматлаштирилган комплекс химояланган ҳисобланади, қачонки барча амаллар объектлар, ресурслар ва муолажаларни бевосита химоясини таъминловчи қатъий аниқланган қоидалар бўйича бажарилса (2.4-расм).

Хавфсизлик

қоидалари



2.4-расм. Ахборот хавфсизлиги сиёсатини таъминлашнинг асосий қоидалари.

Ҳимояга қўйиладиган талабларнинг асосини таҳдидлар рўйхати ташкил этади. Бундай талаблар ўз навбатида ҳимоянинг зарурий вазифалари ва ҳимоя воситаларини аниқлайди.

Демак, компьютер тармоғида ахборотни самарали ҳимоясини таъминлаш учун ҳимоя тизимини лойиҳалаш ва амалга ошириш уч босқичда амалга оширилиши керак.

- хавф-хатарни таҳлиллаш;
- хавфсизлик сиёсатини амалга ошириш;
- хавфсизлик сиёсатини мададлаш.

Биринчи босқичда компьютер тармоғининг заиф элементлари таҳлилланади, таҳдидлар аниқланади ва баҳоланади, ҳимоянинг оптимал воситалари танланади. Хавф-хатарни таҳлиллаш хавфсизлик сиёсатини қабул қилиш билан тугалланади.

Иккинчи босқич – хавфсизлик сиёсатини амалга оширишдаги молиявий харажатларни ҳисоблаш ва бу масалаларни ечиш учун мос воситаларни танлаш билан бошланади. Бунда танланган воситалар ишлашнинг ихтилофли эмаслиги, воситаларни етказиб берувчиларнинг обрўси, ҳимоя механизмлари ва бериладиган қоғозлар хусусидаги тўла ахборот олиш имконияти каби омиллар ҳисобга олинishi зарур. Ундан ташқари, ахборот хавфсизлиги бўйича асосий қоидалар акс эттирилган принциплар ҳисобга олинishi керак.

Учинчи боскич – хавфсизлик сиёсатини мададлаш боскичи энг мухим ҳисобланади. Бу боскичда ўтказиладиган тадбирлар нияти бузук одамларнинг тармокка бостириб киришини доимо назорат қилиб туришни, ахборот объектини ҳимоялаш тизимидаги «рахна»ларни аниқлашни, конфиденциал маълумотлардан рухсатсиз фойдаланиш ҳолларини ҳисобга олишни талаб этади. Тармок хавфсизлиги сиёсатини мададлашда асосий жавобгарлик тизим маъмури бўйнида бўлади. У хавфсизликнинг муайян тизими бузилишининг барча ҳолларига оператив муносабат билдириши, уларни таҳлиллаши ва молиявий воситаларнинг максимал тежалишини ҳисобга олган ҳолда ҳимоянинг зарурий аппарат ва дастурий воситаларидан фойдаланиши шарт.

2.4. Ахборот-коммуникацион тизимлар ва тармоклар хавфсизлигига қўйиладиган талаблар

Қўйида Россия Федерациясида ишлаб чиқилган компьютер тармокларида ахборотни ҳимоялаш соҳасига тааллуқли ҳужжатлар хусусида сўз юритилади. Ҳужжатларда қўйилган талаблар давлат секторида ёки таркибида давлат сири бўлган ахборотни ишловчи тижорат ташкилотларида бажарилиши шарт. Бошқа тижорат тузилмалар учун ҳужжатлар тавсия характерида эга.

Ҳужжатлардан бири ахборотдан рухсатсиз фойдаланишдан ҳимоялаш бўйича талабларни акс эттиради ва «Автоматлаштирилган тизимлар. Ахборотдан рухсатсиз фойдаланишдан ҳимоялаш. Автоматлаштирилган тизимларнинг туркумланиши ва ахборотни ҳимоялаш бўйича талаблар» деб номланади.

Бу ҳужжатда хавфсизликнинг исталган даражасига эришиш бўйича асосланган чораларни ишлаб чиқиш ва қўллаш мақсадида автоматлаштирилган тизимларнинг ахборотни ҳимоялаш нуқтаи назаридан ишлаши шароитлари бўйича туркумланиши келтирилган. Ҳар бир ҳимоялаш бўйича маълум минимал талаблар мажмуи орқали характерланувчи ҳимояланишнинг тўққизта синфи белгиланади (2.1-жадвал).

Компьютер тармоқларининг ҳимояланиш синфлари

Талаблар	Синфлар								
	3 Б	3 А	2 Б	2 А	1 Д	1 Г	1 В	1 Б	1 А
Фойдаланишни бошқариш қисм тизимига									
<i>Идентификациялаш, ҳақиқийлигини текшириш ва субъектлар фойдаланишининг назорати</i>									
– тизимга	х	х	х	х	х	х	х	х	х
– терминалларга, ЭХМга, ЭХМ тармоғи узелларига, алоқа каналларига, ЭХМни ташқи қурилмаларига	–	–	–	х	–	х	х	х	х
– дастурларга	–	–	–	х	–	х	х	х	х
– жилдларга, каталогларга, файлларга, кайдларга	–	–	–	х	–	х	х	х	х
Ахборот оқимларини бошқариш	–	–	–	х	–	–	х	х	х
Рўйхатга ва ҳисобга олиш қисм тизимига									
Рўйхатга ва ҳисобга олиш									
– субъектларнинг тизимга(дан) киришини (чиқишини)	х	х	х	х	х	х	х	х	х
– босма (график) ҳужжатларни беришни	–	х	–	х	–	х	х	х	х
– дастурни ва жараёнларни (топшириқлар, масалалар) ишга туширишни (туғалашни)	–	х	–	х	–	х	х	х	х
– субъект дастурларидан фойдаланишни (ҳимояланувчи файллардан фойдаланиш, уларни яратиш ва йўқотиш, алоқа линиялари ва каналлари орқали узатишни)	–	–	–	х	–	х	х	х	х

- субъект дастурларидан- фойдаланишни (терминал- лардан, ЭХМдан, ЭХМ тармоғи узелларидан, алока каналларидан, ЭХМ ташқи қурилмаларидан, дастурли жилдлардан, кат- логлардан, файллардан, қайдлар ҳошияларидан фойдаланишни)	-	-	-	х	-	х	х	х	х
- фойдаланувчи субъект- лар ваколатларини ўзгартиришларни	-	-	-	-	-	-	х	х	х
- химояланувчи фойдала- ниш объектнинг яратили- шини	-	-	-	х	-	-	х	х	х
Ахборот элтувчиларини ҳисобга олиш	х	х	х	х	х	х	х	х	х
Оператив хотира ва ташқи тўплагичларни тозалаш	-	х	-	х	-	х	х	х	х
Ҳимояни бузишга ури- нишни сигнализацияси	-	-	-	-	-	х	х	х	х
<i>Криптографик қисм тизимига</i>									
Конфиденциал ахборотни шифрлаш	-	-	-	-	-	-	х	х	х
Фойдаланишни турли субъектларига (субъектлар гуруҳига) тегишли ахбо- ротни турли калитларда шифрлаш	-	-	-	-	-	-	-	-	х
Аттестациядан ўтган (сер- тификацияланган) крипто- график воситалардан фой- даланиш	-	-	-	-	-	-	-	х	х
<i>Яхлитликни таъминловчи қисм тизимига</i>									
Дастурий воситалар ва ишланувчи ахборотнинг яхлитлигини таъминлаш	х	х	х	х	х	х	х	х	х
Ҳисоблаш техникаси воси- талари ва ахборот элтув- чиларини қўриқлаш	х	х	х	х	х	х	х	х	х

Ахборот химояси маъмуриятининг (хизматининг) мавжудлиги	–	–	–	х	–	–	х	х	х
Ахборот химояси тизими-ни вақти-вақти билан тестлаш	х	х	х	х	х	х	х	х	х
Ахборот химояси тизими-ни тиклаш воситаларининг мавжудлиги	х	х	х	х	х	х	х	х	х
Сертификацияланган химоя воситаларидан фойдаланиш	–	х	–	х	–	–	х	х	х

Синфлар ахборот ишланиши хусусиятлари билан бир-бирдан фаркланувчи учта гуруҳга бўлинади. Ҳар бир гуруҳ ичида ахборотнинг қийматлигига (конфиденциаллигига) боғлиқ ҳолда химоя бўйича талаблар иерархияси ва демак, химояланиш синфлари сакланади. Ҳар бир гуруҳ кўрсаткичларини, охиригисидан бошлаб кўриб чиқамиз.

Учинчи гуруҳ бир хил конфиденциаллик даражасига эга бўлган элтувчиларда жойлаштирилган барча ахборотдан фойдаланувчи битта фойдаланувчи ишлайдиган тизимлардан иборат. Гуруҳда иккита – 3Б ва 3А синфлари мавжуд.

Иккинчи гуруҳ ҳар хил конфиденциаллик даражасига эга бўлган ишланувчи ва ёки элтувчиларда жойлаштирилган барча ахборотдан фойдаланишга бир хил ҳуқуқли фойдаланувчилари бўлган тизимлардан иборат. Гуруҳда иккита – 2Б ва 2А синфлари мавжуд.

Биринчи гуруҳ кўпчилик фойдаланувчи тизимлардан иборат бўлиб, уларда бир вақтнинг ўзида конфиденциаллик даражаси гурли ахборот ишланади ва ёки сакланади. Гуруҳда бешта – 1Д, 1Г, 1В, 1Б ва 1А синфлари мавжуд.

Умумий ҳолда химоялаш тадбирлари 4 та қисм тизимни ўз ичига олади:

- фойдаланишни бошқариш;
- рўйхатга ва ҳисобга олиш;
- криптографик;
- яхлитликни таъминлаш.

Ҳисоблаш техникаси воситаларини рухсатсиз фойдаланишдан химояланиш кўрсаткичлари «Ҳисоблаш техникаси воситалари. Ахборотни рухсатсиз фойдаланишдан химоялаш. Химоялаш кўрсаткичлари» деб аталувчи ҳужжатда келтирилган. Унда ахборотдан рухсатсиз фойдаланишдан химояланишнинг 7-синфи аниқланган. Энг пастки синф – еттинчи, энг юқори синф – биринчи. Ҳар бир синф химояланиш талабларини олдингисидан мерос қилиб олади. Химоянинг амалга оширилган моделлари ва уларни текшириш ишончлилигига боғлиқ ҳолда синфлар тўртта гуруҳга ажратилади.

Биринчи гуруҳда фақат еттинчи синф бўлади (минимал химояланиш).

Иккинчи гуруҳ танланадиган химоя билан характерланиб олтинчи ва бешинчи синфларни ўз ичига олади. Танланувчи химоя номма-ном айtilган субъектларнинг тизимнинг номма-ном айtilган объектларидан фойдаланишни кўзда тутлади. Бунда ҳар бир «субъект-объект» жуфтлиги учун фойдаланишнинг рухсат этилган турлари аниқланиши шарт. Фойдаланиш назорати ҳар бир объектга ва ҳар бир субъектга қўлланилади.

Учинчи гуруҳ мухтор ҳуқуқли химоя билан характерланиб, тўртинчи, учинчи ва иккинчи синфларни ўз ичига олади. Мухтор ҳуқуқли химоя тизимнинг ҳар бир субъект ва объектига, унинг мос иерархиядаги ўрнини кўрсатувчи туркумлаш белгисини бериш тизимдан фойдаланувчи ёки махсус ажратилган субъект томонидан амалга оширилади. Ушбу ҳуқуқга қирувчи синфлардан талаб қилинадиган нарсасиз-фойдаланишнинг диспетчерини (reference monitor – ҳаволалар монитори) амалга оширилиши. Фойдаланиш назорати барча объектларга нисбатан ҳар қандай субъект томонидан очик ва яширин фойдаланишда амалга оширилиши шарт. Фойдаланишга рухсат бериш фақат танланадиган ва мухтор ҳуқуқли коидаларнинг биргаликда рухсати бўлгандагина амалга оширилиши мумкин.

Тўртинчи гуруҳ тасдиқланган химоя билан характерланиб фақат биринчи синфни ўз ичига олади.

Тизим химояланиш синфини олиши учун қуйидагиларга эга бўлиши лозим:

- тизим бўйича маъмур қўлланмаси;
- фойдаланувчи қўлланмаси;
- тестлаш ва конструкторлик ҳужжатлар.

Юкорида кўриб ўтилганидек, hozирда компьютер жиноятчилиги жуда хам турли-туман. Бу компьютердаги ахборотдан рухсатсиз фойдаланиш, дастурий таъминотга манткий бомбаларни киритиш, компьютер вирусларини ишлаб чиқиш ва таркатиш, компьютер ахборотини ўғирлаш, дастурий-ҳисоб комплексларини ишлаб чиқишда, қуришда ва эксплуатациясида пала-партишлик.

Ахборот хавфсизлигининг бевосита таъминловчи, компьютер жиноятчилигининг олдини олувчи барча чораларни қуйидагиларга ажратиш мумкин:

- ҳуқуқий;
- ташкилий-маъмурий;
- инженер-техник.

Ҳуқуқий чораларга компьютер жиноятчилиги учун жавобгарликни белгиловчи меъёрларни ишлаб чиқиш, дастурчиларнинг муаллифлик ҳуқуқини ҳимоялаш, жиной ва фуқаролик қонун-чилигини ҳамда суд жараёнини такомиллаштириш қиради. Уларга яна компьютер тизимларини яратувчи устидан жамоатчилик назорати масалалари ҳамда, агар компьютер тизимларининг битимга келган мамлакатларнинг ҳарбий, иқтисодий ва ижтимоий жихатларига таъсири бўлса, чеклашлар бўйича мос халқаро шартномаларни қабул қилиш қиради. Фақат охириги йилларда компьютер жиноятчиликларга қарши ҳуқуқий кураш муаммолари бўйича ишлар пайдо бўлди.

Ташкилий-маъмурий чораларга компьютер тизимларини қўриқлаш, ходимларни танлаш, махсус муҳим ишларни бир киши томонидан бажарилиш ҳолларига йўл қўймаслик, марказ ишдан чиққанида унинг ишга лаёқатлигини тиклаш режасининг мавжудлиги, барча фойдаланувчилардан (юкори раҳбарлар ҳам бунга қиради) ҳимояланиш воситаларининг универсаллиги, марказ хавф-сизлигини таъминлашга мутасадди шахсларга жавобгарликни юклаш, марказ жойланадиган жойни танлаш ва ҳ. қиради.

Инженер-техник чораларга компьютер тизимини рухсатсиз фойдаланишдан ҳимоялаш, муҳим компьютер тизимларини резервлаш, ўғирлаш ва диверсиядан ҳимояланишни таъминлаш, резерв электр манбаи, хавфсизликнинг махсус дастурий ва ашпарат воситаларини ишлаб чиқиш ва амалга ошириш ва ҳ. қиради.

III боб. АХБОРОТ ХАВФСИЗЛИГИНИНГ ХУҚУҚИЙ ВА ТАШКИЛИЙ ТАЪМИНОТИ

3.1. Ахборот хавфсизлиги соҳасида ҳуқуқий бошқариш

Ахборот хавфсизлигининг ҳуқуқий таъминоти – ахборотни химоялаш тизимида бажарилиши шарт бўлган қонунлаштирувчи далолатномалар меъёрий-ҳуқуқий ҳужжатлар, қоидалар йўриқномалар, қўлланмалар мажмуи. Ҳозирда ахборот хавфсизлигининг ҳуқуқий таъминоти масаласи ҳам амалий, ҳам қонунчилик жиҳатидан фаол ўрганиб чиқилмоқда.

Компьютер жинойтчиликларини қилиш инструментлари сифатида телекоммуникация ва ҳисоблаш техникаси воситалари, дастурий таъминот ва интеллектуал билим ишлатилади. Компьютер жинойтчиликларини қилиш соҳаси сифатида нафақат компьютерлар, глобал ва корпоратив тармоқлар (Internet/Intranet), балки ахборот технологиясининг замонавий, юқори унумли воситалари ҳамда ахборотнинг қатга ҳажми ишланадиган, масалан, статистик ва молия институтлари, танланади.

Шу сабабли, ҳар қандай ташкилот фаолиятини турли-туман ахборотни олиш учун қўлда ёки ҳисоблаш техникаси воситалари ёрдамида ишлаш, ахборотни таҳлиллаш натижасида қандайдир муайян счимларни олиш ва уларни алоқа каналлари орқали узатишсиз тасаввур этиб бўлмайди. Компьютерга ҳам гажовуз объекти, ҳам гажовуз қилувчи инструмент сифатида қараш мумкин. Агар компьютер фақат гажовуз объекти бўлса, қонун бузилишини мавжуд ҳуқуқий меъёрлар орқали баҳолаш мумкин. Агар компьютер фақат инструмент бўлса «техник воситаларни қўллаш» аломати старли бўлади. Юқоридаги тушунчаларни бирлаштириш мумкин компьютер бир вақтнинг ўзида ҳам инструмент ҳам объект. Хусусан, бундай вазиятга машина ахборотининг ўғирланиши факти тааллуқли.

Агар ахборотнинг ўғирланиши моддий ва маънавий бойликларнинг йўқотилиши билан боғлиқ бўлса, бу факт жинойт сифатида баҳоланади. Шунингдек, агар ушбу факт билан миллий хавфсиз-

лик. муаллифлик манфаатлари боғлиқ бўлса, жиноий жавобгарлик Ўзбекистон Республикаси қонунларида бевосита кўзда тутилган.

Ҳар қандай давлатда ахборот хавфсизлигининг ҳуқуқий таъминоти халқаро ва миллий ҳуқуқий меъёрларни ўз ичига олади (3.1-расм).



3.1-расм. Ахборот хавфсизлигини таъминлашнинг ҳуқуқий меъёрлар.

Ҳуқуқий бошқариш предметлари қуйидагилар.

ахборот ҳимоясининг ҳуқуқий режими;

- ахборотлаштириш жараёнларида қонуний муносабат қатнашчиларининг ҳуқуқий мақоми;

субъектларнинг, уларнинг ахборот тузилмалари ва гизимлари ишлаши жараёнининг турли босқич ва сатҳларидан ҳуқуқий мақомини ҳисобга олган ҳолда, муносабатлари тартиби.

Ахборот хавфсизлиги бўйича қонунларни Ўзбекистон Республикаси бутун қонунлар тизимининг ажралмас қисми сифатида тасаввур қилиш мумкин, хусусан:

- таркибида ахборотлаштириш масалаларига доир меъёрлар бўлган конституция қонунлари:

– таркибида ахборотлаштириш масалаларига доир меъёрлар бўлган умумий асосий қонунлар (мулк, ер ости бойликлари, ер, фуқоролар ҳуқуқи, фуқаролик, солиқ ҳусусида);

– хўжалиқнинг алоҳида тузилмаларига, иктисодиётга, давлат органлари тизимига тегишли бошқариш ва уларнинг мақомини аниқлаш бўйича қонунлар. Бу қонунлар ахборот масалалари бўйича алоҳида меъёрларни ўз ичига олади;

– муносабатларнинг, хўжалиқ соҳаларининг, жараёнларнинг муайян муҳитига бутунлай тегишли махсус қонунлар. Буларга ахборотлаштириш бўйича қонунлар тааллуқли:

– ахборотлаштириш соҳасидаги қонун талабларининг бажарилишини регламентловчи меъёрий ҳужжатлар;

– қонунлар билан белгиланган ахборотлаштириш соҳасидаги меъёрий ҳужжатлар;

– таркибида ахборотлаштириш соҳасида қонун бузилишига жавобгарлик меъёрлари бўлган Ўзбекистон Республикасининг ҳуқуқни муҳофаза қилиш қонунлари.

Компьютер тармоқлари хавфсизлигини таъминловчи давлат ҳуқуқий механизмнинг ривожланмаган шароитида қорхонанинг давлат ва ходимлар жамоаси билан муносабатларни ҳуқуқий асосда ростловчи ҳужжатлари жиддий аҳамиятга эга бўлади. Бундай муҳим ҳужжатлар таркибига қуйидагиларни киритиш мумкин:

– қорхона (фирма, банк) устави;

– жамоа шартномаси;

– жамоа ходимлари билан тузилган, тижорат сири бўлган маълумотлар ҳимоясини таъминлаш бўйича талабларга эга меҳнат шартномалари;

– ишчи ва хизматчиларнинг ички меҳнат тартиб қоидалари;

– раҳбарлар, мутахассислар ва хизмат кўрсатувчи ходимларнинг мансаб билан боғланган мажбуриятлари.

3.2. Ахборот хавфсизлигининг ташкилий-маъмурий таъминоти

Ахборотни ишончли ҳимоя механизмини яратишда ташкилий тадбирлар муҳим рол ўйнайди, чунки конфиденциал ахборотлардан руҳсатсиз фойдаланиш асосан, техник жиҳатлар билан эмас, балки ҳимоянинг элементар қоидаларини эътиборга олмайдиган фойдаланувчилар ва ходимларнинг жиноятқорона ҳаракатлари, бепарволиги, совуққонлиги ва масъулиятсизлиги билан боғлиқ.

Ташкилий таъминот конфиденциал ахборотдан фойдаланишга имкон бермайдиган ёки жиддий қийинчилик туғдирувчи ижрочиларнинг ишлаб-чиқариш ва ўзаро муносабатларини меъёрий-хукукий асосида регламентлашдир.

Ташкилий тадбирларга қуйидагилар киради:

– хизматчи ва ишлаб чиқариш бино ва хоналарни лойихалашда, қуришда ва жиҳозлашда амалга ошириладиган тадбирлар. Бу тадбирларнинг асосий мақсади ҳудудга ва хоналарга яширинча кириш имконини йўқотиш; одамларнинг ва транспортнинг юриши назоратининг қулайлигини таъминлаш; фойдаланишнинг алоҳида тизимига эга бўлган ишлаб-чиқариш зоналарини яратиш ва ҳ.

– ходимларни танлашда амалга ошириладиган тадбирлар. Бу тадбирларга ходимлар билан танишиш, конфиденциал ахборот билан ишлаш қоидалари билан ишлашни ўргатиш, ахборот ҳимояси қондасини бузганлиги учун жавобгарлик даражаси ва ҳ. билан таништириш киради;

– ишончли пропуск режимини ва ташриф буюрувчиларнинг назоратини ташкил қилиш;

– хона ва ҳудудларни ишончли кўриклаш;

– ҳужжатлар ва конфиденциал ахборот элтувчиларини сақлаш ва ишлатиш, шу жумладан, қайд этиш, бериш, бажариш ва қайтариш тартибларига риоя қилиш;

– ахборот ҳимоясини ташкил этиш, яъни муайян ишлаб чиқариш жамоаларида ахборот хавфсизлигига жавобгар шахсни тайинлаш, конфиденциал ахборот билан ишловчи ходимлар ишини мунтазам текшириб туриш.

Бундай тадбирлар ҳар бир муайян ташкилот учун ўзига хос хусусиятга эга бўлади.

Ташкилий тадбирларнинг талайгина қисмини ходимлар билан ишлаш эгаллайди. Мулкчиликнинг турли шаклларига эга бўлган корхона ходимлари билан ишлашда ташкилий тадбирлар, умумий ҳолда қуйидагиларни ўз ичига олади:

– ишга қабул қилишда суҳбат. Суҳбат натижасида номзоднинг мос бўш жойга қабул қилиниши мақсадга мувофиқлиги аниқланади;

– муайян корхонада конфиденциал ахборот билан ишлаш қоидалари ва муолажалари билан танишиш; ишга қабул қилинувчи

корхона тижорат сирларини саклаши бўйича тилхат ва фирма сирларини ошкор қилмасликка ваъда беради:

– ходимларни конфиденциал ахборот билан ишлаш қоидалари ва муолажаларига ўқитиш. Ходимларни ўқитишда нафақат ишлаб-чиқариш кўникмаларига эга бўлиш ва уларни юқори даражада саклаш, балки уларни саноат (ишлаб чиқариш) махфийлиги ахборот хавфсизлиги, интеллектуал мулк ва тижорат сирлари химояси талабларини бажариш зарурлигига қатъий ишонч руҳида тарбиялаш кўзда тутилади. Мунтазам ўқитиш раҳбарият ва ходимларнинг қорхона тижорат манфаатларини химоя қилиш масалалари бўйича билимдонлик даражасини ошишига имкон яратади;

– ишдан бўшаётганлар билан суҳбат. Суҳбат давомида ишдан бўшаётган ходимнинг фирма сирларини фож килмасликка қатъий ваъда бериши лозимлиги таъкидланади ва бу ваъда, одатда, тилхат орқали расмийлаштиради.

Тадбирларнинг муҳим йўналишларидан бири иш юритиш ва ҳужжат юритиш тизимини пухта ташкил этиш ҳисобланади. Бу эса ўз навбатида иш юритиш тартибини, ҳужжатларни қайдлаш, ишлаш, саклаш, йўқотиш ва мавжудлигини ҳамда тўғри бажарилишини назорат қилишни таъминлайди. Тизимни амалга оширишда ҳужжатлар хавфсизлигига ва ахборот конфиденциаллигига алоҳида эътибор бериш лозим.

Ахборотни ҳужжатлаштириш қатъий белгиланган қоидалар ёрдамида амалга оширилади. Бу қоидаларнинг асосийлари ГОСТ 6.38-90 «Ташкилий-бошқарувчи ҳужжатлар тизими. Ҳужжатларни расмийлаштиришга талаблар», ГОСТ 6.10.4-84 «Унификацияланган ҳужжатлар тизими. Ҳисоблаш техника воситалари орқали яратилувчи машина элтувчиларидаги ва машинограммалардаги ҳужжатларга ҳуқуқий қуч бериш» қабилар баён этилган. Бу ГОСТларда ахборотга ҳужжат ҳуқуқини берувчи 31 та реквизитлар кўзда тутилган, аммо бу реквизитларнинг барчасининг ҳужжатда мавжудлиги шарт эмас. Асосий реквизит – матн. Шу сабабли, ҳар қандай раван баён этилган матн ҳужжат ҳисобланади ва унга ҳуқуқий қуч бериш учун сана ва имзо қабил муҳим реквизитларнинг мавжудлиги қифоя.

Автоматлаштирилган ахборот тизимларидан олинган ҳужжатлар учун алоҳида тартиб қўлланилади. Бунда, маълум ҳолларда, масофадан олинган ахборот электрон имзо билан тасдиқланади. Ахборотни химоялаш учун барча ташкилий тадбирларни таъмин-

ловчи махсус маъмурий хизматни яратиш талаб қилинади. Унинг штат тузилмаси, сони ва таркиби фирманинг реал эҳтиёжлари, ахборотининг конфиденциаллик даражаси ва хавфсизлигининг умумий ҳолати орқали аниқланади.

- Маъмурий тадбирларга қуйидагилар қиради:
 - операцион тизимнинг тўғри конфигурациясини мададлаш;
 - иш журналларининг назорати;
 - пароллар алмашишининг назорати;
 - химоя тизимида «рахна»ларни аниқлаш;
 - ахборотни химояловчи воситаларни тестлаш.
- Тармок операцион тизимининг тўғри конфигурациясини мададлаш масаласини, одатда, тизим маъмури ҳал этади. Маъмур операцион тизим (одамлар эмас) риюя қилиши лозим бўлган маълум коидаларни яратади. Тизимни маъмурлаш – конфигурация файлларини тўғри тузишдир. Бу файлларда (улар бир нечта бўлиши мумкин, масалан, тизимнинг ҳар бир қисмига биттадан файл) тизим ишлаши коидаларининг тавсифи бўлади.

Хавфсизлик маъмури компьютер тармоғи ҳолатини оператив тарзда (тармок компьютерлари химояланиши ҳолатини кузатиш орқали) ва оператив бўлмаган тарзда (ахборот химояси тизимидаги воқеаларни қайдловчи журналларни таҳлиллаш орқали) назоратлаш лозим. Ишчи станциялар сонининг ошиши ва турлитуман компонентлари бўлган дастурий воситаларнинг ишлатилиши ахборот химояси тизимидаги ходисаларни қайдлаш журналлар ҳажмини жиддий ошишига олиб келади. Журналлардаги маълумотлар ҳажми шунчалик ошиб кетиши мумкинки, маъмур улар таркибини жоиз вақт мобайнида таҳлиллай олмайди.

Тизим заифлигининг сабаби шундаки, биринчидан, фойдаланувчини аутентификациялаш тизими фойдаланувчи исмига ва унинг паролига (кўз тўридан фойдаланиш каби экзотик ҳоллар бундан мустасно), иккинчидан, фойдаланувчи тизимида тизимни маъмурлаш ҳукуки берилган супервизорнинг (supervisor) мавжудлигига асосланади. Супервизор паролини сақлаш режимининг бузилиши бутун тизимдан рухсатсиз фойдаланиш имконини яратади.

Ундан ташқари, бундай коидаларга асосланган тизим-статик, котиб қолган тизим. У фақат катъий маълум ҳужумларга қарши кўра олиши мумкин. Олдиндан кўзда тутилмаган қандайдир янги таҳдиднинг пайдо бўлишида тармок ҳужуми нафақат муваффақиятли, балки тизим учун кўринмайдиган бўлиши мумкин. Шу-

нинг учун, муассасада ишлатилувчи ахборотнинг қайсиси химояга мухтож эканлигини аниқ тасаввур қилиш муҳим ҳисобланади. Мавжуд ахборотни таҳлиллашдан бошлаш лозим. Бу муолажалар ахборот химоясини таъминлаш бўйича тадбирларни дифференциаллаш имконини беради ва натижада, сарф-харажатларнинг қисқаришига сабаб бўлади.

Ахборот химояси тизимини эксплуатация қилиш босқичида хавфсизлик маъмурининг фаолияти фойдаланувчилар ваколатларини ўз вақтида ўзгартиришдан ҳамда тармок компьютерларидаги химоя механизмларини созлашдан иборат бўлади. Фойдаланувчилар ваколатларини ва компьютер тармоқларида ахборотни химоялаш тизимини созлашни бошқариш муаммоси, масалан, тармокдан марказлаштирилган фойдаланиш тизимидан фойдаланиш асосида ҳал этилиши мумкин. Бундай тизимни амалга оширишда тармок асосий серверида ишловчи махсус фойдаланишни бошқарувчи сервердан фойдаланилади. Бу сервер марказий химоя маълумотлари базасини локал химоя маълумотлари базаси билан автоматик тарзда синхронлайди. Фойдаланишни бошқаришнинг бу тизимида фойдаланувчи ваколоти вақти-вақти билан ўзгартирилади ва марказий химоя маълумотлари базасига киритилади, уларнинг муайян компьютерларда ўзгариши навбатдаги синхронлаш сеансида вақтида амалга оширилади.

Ундан ташқари, фойдаланувчи паролини ишчи станцияларининг бирида ўзгартирса, унинг янги пароли марказий химоя маълумотлари базасида автоматик тарзда аксланади ҳамда бу фойдаланувчи ишлашига рухсат берилган ишчи станцияларга узатилади.

3.3. Ахборот хавфсизлиги бўйича стандартлар ва спецификациялар

Ахборот хавфсизлиги соҳасида мутахассислар ўз фаолиятларида мос стандартлар ва спецификацияларни четлаб ўтиша олмайдилар. Бунга сабаб, биринчидан стандартлар ва спецификациялар – аввало, ахборот хавфсизлигининг муолажавий ва дастурий-техник даражалари бўйича билимларини тўплаш шаклларидан бири. Уларда малакали мутахассислар томонидан ишлаб чиқилган, тасдиқланган юқори сифатли ечимлар ва методологиялар кайд этилган. Иккинчидан, стандартлар ва спецификациялар аппарат-

дастурий тизимлар ва уларнинг компонентларининг ўзаро кўшила олишлигини таъминловчи асосий восита ҳисобланади. (Internet-уюшмада бу восита ҳақиқатдан самарали ишламоқда).

Стандартлар ва спецификацияларнинг бир-биридан жиддий фаркланувчи иккита гуруҳини ажратиш мумкин:

- ахборот тизимларини ва хавфсизлик талаблари бўйича химоя воситаларини баҳолаш ва туркумлаш учун аталган баҳолаш стандартлари;

- химоя воситалари ва усулларини амалга ошириш ва улардан фойдаланишнинг турли жиҳатларини регламентловчи спецификациялар.

Бу гуруҳлар маълумки, ихтилофга бормайдилар, балки бир-бирини тўлдирадилар. Баҳолаш стандартлари ташкилий ва архитектуравий спецификациялар вазифасини ўтаган ҳолда ахборот тизимларининг ахборот хавфсизлиги нуқтаи назаридан муҳим бўлган тушунчалари ва жиҳатларини тавсифлайди. Спецификациялар эса архитектура белгилаган ахборот тизимини қандай куриш лозимлигини ва ташкилий талабларни қандай кондирилишини аниқлайди.

Халқаро эътирофни қозонган ва ахборот хавфсизлиги соҳасида кейинги ишланмаларда жуда кучли таъсир кўрсатган биринчи баҳолаш стандарти АҚШ мудофаа вазирлигининг «*Тўқ сарик китоб*» (мукованинг ранги бўйича) деб аталувчи «Ишончли компьютер тизимларини баҳолаш мезонлари» (Department of Defense Trusted Computer System Evaluation Criteria, TCSEC) стандарти бўлди. Муболағасиз тасдиқлаш мумкинки, «*Тўқ сарик китоб*»и ахборот хавфсизлигининг тушунчалар негизини ифодалайди. Ундаги тушунчаларнинг санаб ўтишнинг ўзи етарли: *хавфсиз ва ишончли тизимлар, хавфсизлик сиёсати, кафолатлик даражаси, ҳисоб-китоблиги, ишончли ҳисоблаш асоси, мурोजаатлар монитори, хавфсизликнинг ядроси ва периметри.*

«*Тўқ сарик китоб*»дан сўнг чиқарилган ҳужжатлардан бири «*Тўқ сарик китоб*»нинг тармоқ конфигурациялари учун *изоҳи*» (Trusted Network Interpretation) энг муҳим ҳужжат ҳисобланади. Бу ҳужжат икки қисмдан иборат. Биринчи қисм *изоҳ*нинг ўзига бағишланган бўлса, иккинчи қисмида ўзига хос ёки тармоқ конфигурациялари учун айниқса, муҳим бўлган *хавфсизлик сервислари* тавсифланади. Биринчи қисмга киритилган энг муҳим тушунчалардан бири – тармоқдаги ишончли ҳисоблаш асоси. Муҳим жиҳат–

тармок конфигурацияларининг динамиклиги. Ҳимоялаш механизмлари орасида *конфиденциалликлик ва яхлитликни таъминловчи криптография* ажратилган. Фойдаланувчанлик масалалари, уни таъминлашдаги архитектуравий принципларнинг шакллантирилиши ўз вақти учун тартибли ёндашиши бўлди.

Таксимланган ахборот тизимларини объектга мўлжалланган тарзда коммуникацияларни криптографик ҳимоялаш билан биргаликда декомпозициялашнинг назарий асосини – мурожаатлар мониторингини фрагментлашнинг корректлиги шартининг етарлилигини айтиб ўтиш лозим.

Баҳолаш стандартларидан яна бири «*Европа мамлакатларининг уйғунлаштирилган мезонлари*»да ахборот тизими ишлаши лозим бўлган шароитларга априор шартлар йўқ. Фараз қилинадики, аввал баҳолаш мақсади ифодаланади, сўнгра сертификациялаш органи бу мақсадга қанчалик тўлиқ эришилишини, яъни, муайян вазиятда хавфсизликнинг архитектураси ва амалга оширилиши механизмларининг қанчалик корректлигини ва самаралилигини аниқлайди. Баҳолаш мақсадини ифодалашни енгиллаштириш ниятида стандартда ҳукумат ва тижорат тизимларига хос функционалликнинг ўн тахминий синфлари тавсифланган.

Ушбу стандартда ахборот технологиялар тизимлари ва маҳсулотлари ўртасидаги фарқ таъкидланади, аммо талабларини унификациялаш ниятида ягона – *баҳолаш объекти* тушунчаси кiritилади. Стандартда хавфсизлик функциялари (сервислари) ва уларни амалга оширувчи механизмлар орасида фарқнинг кўрсатилиши ҳамда кафолатланишнинг икки жиҳати – хавфсизлик воситаларининг *самарадорлиги* ва *корректлигининг* ажратилиши муҳим ҳисобланади. Баҳолаш стандартлари гуруҳига ахборот хавфсизлигининг муайян, аммо муҳим ва мураккаб жиҳатини регламентловчи АҚШнинг «*Криптографик модуллар учун хавфсизлик талаблари*» Федерал стандарти ҳамда «*Ахборот технологиялар хавфсизлигини баҳоловчи мезонлар*» халқаро стандарти тааллуқли.

Техник спецификациялар орасида биринчи ўринга, сўзсиз, X800 «*Очик тизимлар ўзаро ҳаракати учун хавфсизлик архитектураси*» хужжатини кўйиш лозим. Бу хужжатда хавфсизликнинг энг муҳим тармок сервислари ажратилган: *аутентификация, фойдаланишни бошқариш*, маълумотларни конфиденциаллиги ва ёки яхлитлигини таъминлаш ҳамда қилинган ҳаракатдан *ташишнинг мумкин эмаслиги*. Сервисларни амалга ошириш учун хавфсизликнинг

қуйидаги тармок механизмлари ва уларнинг комбинациялари кўзда тутилган: *шифрлаш, электрон рақамли имзо, фойдаланишни бошқариш, маълумотлар яхлитлигининг назорати, аутентификация, трафикни тўлдириш, маршрутлашни бошқариш, нотаризация.* Хавфсизликнинг сервислари ва механизмлари амалга оширилувчи етти сатхли эталон моделининг сатхлари танланган. Нихоят, таксимланган конфигурациялар учун хавфсизлик воситаларининг маъмурлаш масалалари батафсил кўриб чиқилган.

Internet – уюшманинг RFC 1510 «Аутентификациянинг тармок сервери Kerberos (VS)» спецификацияси хусусий, аммо муҳим ва долзарб муаммога турли таксимланган муҳитда тармокка ягона кириш концепциясини мададлаган ҳолда аутентификациялашга тегишли.

Kerberos аутентификациялаш сервери ишончли учинчи гараф бўлиб, хизмат кўрсатилувчи субъектларнинг махфий калитларига эга ва уларга хақиқийликнинг жуфтлашиб текширишда ёрдам беради. Kerberosнинг миждоз компонентларининг аксарият замонавий операцион тизимларда мавжудлиги унинг калитлик муҳим эканлигидан далолат беради.

IPsec техник спецификацияси тармок сатҳида конфиденциаллик ва яхлитлик воситаларининг гўллик тўпламини тавсифлаган ҳолда, муболағасиз фундаментал аҳамиятга эга. IPsec асосида юкорирок сатҳ (таъбикий сатҳга кадар) протоколларини ҳимоялаш механизми ҳамда хавфсизликнинг тугалланган воситалари, хусусан виртуал хусусий тармоқлар қурилади. Албатта, IPsec криптографик механизмларига ва калит инфратузилмаларига таянади.

Транспорт сатҳи хавфсизлиги ва сигналлари (Transport Layer Security, TLS) ҳам шундай характерланади. TLS спецификацияси турли вазибаларни бажарувчи кўпгина дастурий маҳсулотларда ишлатилувчи оммавий Secure Socket Layer (SSL) протоколини ривожлантиради ва ойдинлаштиради.

Юқорида эслатиб ўтилган инфратузилма нуқтаи назаридан X.500 «*Директория хизмати: концепциялар, моделлар ва серверлар обзори*» (The Directory: Overview of concepts, models and services) ва X.509 «*Директория хизмати: сертификатлар, очик калитлар ва атрибутлар каркаслари*» (The Directory: Public-key and attribute certificate frameworks) тавсиялари жуда муҳим ҳисобланади. X.509 тавсияларида очик калитлар ва атрибутлар яъни очик калитлар инфратузилмаси ва имтиёзларни

бошқаришнинг базавий элементлари сертификатларининг формати тавсифланган.

Маълумки, ахборот хавфсизлигини таъминлаш комплекс муаммо бўлиб, конуний, маъмурий, муолажавий ва дастурий-техник сатхларда чораларни келишилган ҳолда кўришни талаб этади. Маъмурий сатхнинг базавий ҳужжати ташкилот *хавфсизлиги сиёсатини* ишлаб чиқишда ва амалга оширишда Internet – уюшманинг «Ташкилот ахборот хавфсизлиги бўйича қўлланма»си (Site Security Handbook) наъмунали кўмакчи вазифасини ўташи мумкин. Унда хавфсизлик сиёсати муолажаларини шакллантирилишининг амалий жиҳатлари ёритилади, маъмурий ва муолажавий сатхларнинг асосий тушунчалари изоҳланади, тавсия этувчи ҳаракатларнинг сабаблари кўрсатилган, хавф-хатарлар таҳлили, ахборот хавфсизлигининг бузилишига муносабат ва бузилиш бар-тараф этилганидан кейинги ҳаракат мавзуларига тўхтаб ўтилган.

«Ахборот химояси бузилишига қандай муносабат билдириш лозим» (Expectations for Computer Security Incident Response) тавсиясида юқорида келтирилган масалалардан ташқари фойдали ахборот ресурсларига ҳаволаларни ҳамда муолажавий даражадаги амалий маслаҳатларни топиш мумкин.

Корпоратив ахборот тизимини ривожлантиришда ва қайта тузишда «*Internet-хизмат билан таъминловчини қандай танлаш лозим*» (Site Security Handbook Addendum for ISPs) тавсияси сўзсиз фойдалидир. Биринчи галда унинг қоидаларига ташкилий ва архитектуравий химоялашни шакллантириш жараёнида риоя қилиш лозим.

Британия стандарти BS 7799 «Ахборот хавфсизлигини бошқариш. Амалий қоидалар» (Code of practice for information security management) ахборот хавфсизлигига жавобгар ташкилот раҳбарлари учун фойдали ҳисобланади. Бу стандарт жиддий ўзгартиришсиз ISO/IEC 17799 халқаро стандартга кўчирилган.

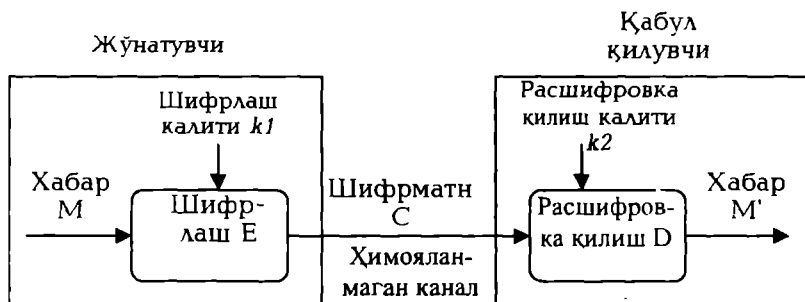
Бу борада мустақил диёримиз Ўзбекистон Республикасида аҳамиятга молик бўлган улкан ишлар олиб борилмоқда. Бунга мисол тариқасида Ўзбекистон алоқа ва ахборотлаштириш агентлигининг илмий-техник ва маркетинг тадқиқотлари маркази томонидан ишлаб чиқилган O‘z DSt 1092:2005 «Ахборот технологияси. Маълумотларни криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари», O‘z DSt 1105:2006 «Ахборот технологияси. Маълумотларни криптографик муҳофа-

заси. Маълумотларни шифрлаш алгоритми», O‘z DSt 1106:2006 «Ахборот технологияси. Маълумотларни криптографик муҳофазази. Хешлаш функцияси» ва O‘z DSt 1108:2006 «Ахборот технологияси. Очик тизимлар ўзаро боғлиқлиги. Электрон рақамли имзо очик калити сертификати ва атрибут сертификатининг тузилмаси» стандартларини ва RH 45-187:2006 «Хавфсизлик талаблари» бошқарув ҳужжатини кўрсатиб ўтиш мумкин. Ушбу марказ томонидан ишлаб чиқилган стандартлар №05-11 12.04.2006 йилда ўзбекистон стандартлаштириш, метрология ва сертификациялаш агентлиги томонидан тасдиқланган.

Бундан ташқари, юртимизда ахборот хавфсизлиги соҳасида фаолият юритаётган ўзбекистон алоқа ва ахборотлаштириш агентлиги қошидаги «UZINFOCOM», «UZ-CERT» ва бошқа ташкилотларни айтиб ўтиш лозим.

4.1. Криптографиянинг асосий қондалари ва таърифлари

Ахборотнинг химоялашнинг аксарият механизмлари асосини шифрлаш ташкил этади. Ахборотни шифрлаш деганда очик ахборотни (дастлабки матни) шифрланган ахборотга ўзгартириш (шифрлаш) ва аксинча (расшифровка қилиш) жараёни тушунилади. Шифрлаш криптолизимининг умумлаштирилган схемаси 4.1-расмда келтирилган.



4.1-расм. Шифрлаш криптолизимининг умумлаштирилган схемаси.

Узатиловчи ахборот матни M криптографик ўзгартириш E_{k1} ёрдамида шифрланади, натижада, шифрматн C олинади:

$$C = E_{k1}(M)$$

бу ерда, $k1$ – шифрлаш калити деб аталувчи E функциянинг параметри.

Шифрлаш калити ёрдамида шифрлаш натижаларини ўзгартириш мумкин. Шифрлаш калити муайян фойдаланувчига ёки фойдаланувчилар гуруҳига тегишли ва улар учун ягона бўлиши

мумкин. Муайян калит ёрдамида шифрланган ахборот фақат ушбу калит эгаси (ёки эгалари) томонидан расшифровка қилиниши мумкин.

Ахборотни тескари ўзгартириш қуйидаги кўринишга эга:

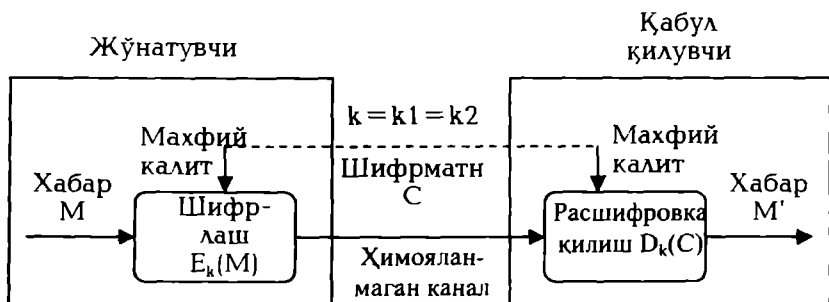
$$M' = D_{k_2}(C)$$

D функцияси E функцияга нисбатан тескари функция бўлиб, шифр матни расшифровка қилади. Бу функция ҳам k_2 калит кўринишидаги кўшимча параметрга эга. k_1 ва k_2 калитлар бир маъноли мосликка эга бўлишлари шарт. Бу ҳолда расшифровка қилинган M' ахборот M га эквивалент бўлади. k_2 калити ишончли бўлмаса D функция ёрдамида $M' = M$ дастлабки матни олиб бўлмайди.

Криптотизимларнинг иккита синфи фаркланади:

- симметрик криптотизим (бир калитли);
- асимметрик криптотизим (иккита калитли).

Шифрлашнинг симметрик криптотизимида шифрлаш ва расшифровка қилиш учун битта калитнинг ўзи ишлатилади. Демак, шифрлаш калитидан фойдаланиш ҳуқуқига эга бўлган ҳар қандай одам ахборотни расшифровка қилиши мумкин. Шу сабабли, симметрик криптотизимлар махфий калитли криптотизимлар деб юритилади. Яъни шифрлаш калитидан фақат ахборот аталган одамгина фойдалана олиши мумкин. Шифрлашнинг симметрик криптотизими схемаси 4.2-расмда келтирилган.



4.2-расм. Симметрик шифрлаш криптотизимнинг схемаси.

Электрон ҳужжатларни узатишнинг конфиденциаллигини симметрик криптоанизим ёрдамида таъминлаш масаласи шифрлаш калити конфиденциаллигини таъминлашга келтирилади. Одатда, шифрлаш калити маълумотлар файли ва массивидан иборат бўлади ва шахсий калит элтувчисида масалан, дискетда ёки смарт-картада сақланади. Шахсий калит элтувчиси эгасидан бошқа одамларнинг фойдаланишига қарши чоралар кўрилиши шарт.

Симметрик шифрлаш ахборотни «ўзи учун», масалан, эгаси йўклигида ундан руҳсатсиз фойдаланишни олдини олиш мақсадида, шифрлашда жуда қулай ҳисобланади. Бу танланган файлларни архивли шифрлаш ва бутун бир мантикий ёки физик дискларни шаффоф (автоматик) шифрлаш бўлиши мумкин.

Симметрик шифрлашнинг ноқулайлиги - ахборот алмашинуви бошланмасдан олдин барча манзилатлар билан махфий калитлар билан айирбошлаш заруриятидир. Симметрик криптоанизимда махфий калитни алоканинг умумфойдаланувчи каналлари орқали узатиш мумкин эмас. Махфий калит жўнатувчига ва қабул қилувчига калитлар тарқатилувчи химояланган каналлар орқали узатилиши керак.

Симметрик шифрлаш алгоритмининг маълумотларни абонентли шифрлашда, яъни шифрланган ахборотни абонентга, масалан, Internet орқали, узатишда амалга оширилган вариантлари мавжуд. Бундай криптографик тармокнинг барча абонентлари учун битта калитнинг ишлатилиши хавфсизлик нуқтаи назаридан ноқонозир. Ҳақиқатан, калит обрўсизлантирилганда (йўқотилганида, ўғирлатилганда) барча абонентларнинг ҳужжат алмашиши хавф остида қолади. Бу ҳолда калитларнинг матрицаси (4.3-расм) ишлатилиши мумкин.

	1	2	3	...	n	
1	k_{11}	k_{12}	k_{13}		k_{1n}	1-абонент учун калитлар тўплами
2	k_{21}	k_{22}	k_{23}	...	k_{2n}	2-абонент учун калитлар тўплами
3	k_{31}	k_{32}	k_{33}		k_{3n}	3-абонент учун калитлар тўплами

n	k_{n1}	k_{n2}	k_{n3}	...	k_{nn}	n-абонент учун калитлар тўплами

4.3-расм. Калитлар матрицаси.

Калитлар матрицаси абонентларнинг жуфт-жуфт боғланишли жадвалидан иборат. Жадвалнинг ҳар бир элементи i ва j абонентларни боғлашга мўлжалланган ва ундан факат ушбу абонентлар фойдалана оладилар. Мас ҳолда, калитлар матрицаси элементлари учун қуйидаги тенглик ўринли.

$$K_{ij} = K_{ji}.$$

Матрицанинг ҳар бир i - катори муайян i абонентнинг қолган $N-1$ абонентлар билан боғланишини таъминловчи калитлар тўпамидан иборат. Калитлар тўплами (тармок тўпламлари) криптографик тармокнинг барча абонентлари ўртасида тақсимланади. Тақсимлаш алоканинг ҳимояланган каналлари орқали ёки қўлдан-қўлга тарзда амалга оширилади.

Асимметрик криптотизимларда ахборотни шифрлашда ва расшифровка қилишда турли калитлардан фойдаланилади:

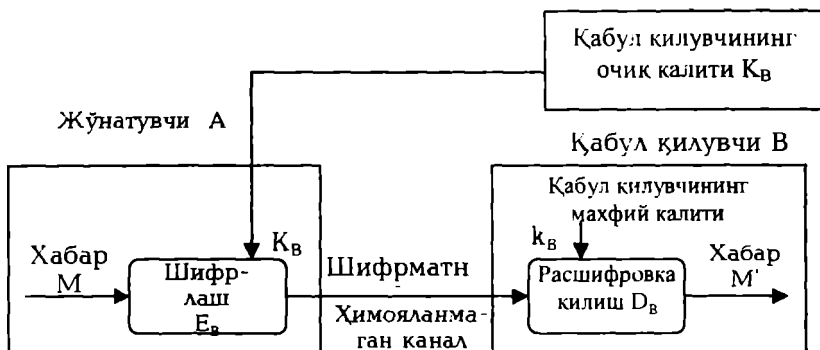
- *очик калит* K ахборотни шифрлашда ишлатилади, махфий калит k дан ҳисоблаб чиқарилади;

- *махфий калит* k , унинг жуфти бўлган очик калит ёрдамида шифрланган ахборотни расшифровка қилишда ишлатилади.

Махфий ва очик калитлар жуфт-жуфт генерацияланади. Махфий калит эгасида қолиши ва уни руҳсатсиз фойдаланишдан ишончли ҳимоялаш зарур (симметрик алгоритмдаги шифрлаш калитига ўхшаб). Очик калитнинг нусхалари махфий калит эгаси ах-

борот алмашинадиган криптографик тармоқ абонентларининг хар бирида бўлиши шарт.

Асимметрик шифрлашнинг умумлаштирилган схемаси 4.4-расмда келтирилган.



4.4-расм. Асимметрик шифрлашнинг умумлаштирилган схемаси.

Асимметрик криптоотизимда шифрланган ахборотни узатиш куйидагича амалга оширилади:

1. Тайёргарлик боскичи:

абонент B жуфт калитни генерациялайди: махфий калит k_B ва очик калит K_B ;

– очик калит K_B абонент A га ва қолган абонентларга жўна-тилади.

2. A ва B абонентлар ўртасида ахборот алмашиш:

– абонент A абонент B нинг очик калити K_B ёрдамида ахборотни шифрлайди ва шифрматнни абонент B га жўнатади;

– абонент B ўзининг махфий калити k_B ёрдамида ахборотни расшифровка қилади. Ҳеч ким (шу жумладан, абонент A ҳам) ушбу ахборотни расшифровка қилаолмайди, чунки абонент B нинг махфий калити унда йўқ.

Асимметрик криптоотизимда ахборотни химоялаш ахборот қабул қилувчи калити k_B нинг махфийлигига асосланган.

Асимметрик криптоотизимларнинг асосий хусусиятлари куйидагилар:

1. Очик калитни ва шифр матнни химояланган канал орқали жўнатиш мумкин, яъни нияти бузук одамга улар маълум бўлиши мумкин.

2. Шифрлаш $E_B: M \rightarrow C$ ва расшифровка қилиш $D_B: C \rightarrow M$ алгоритмлари очик.

4.2. Симметрик шифрлаш тизими

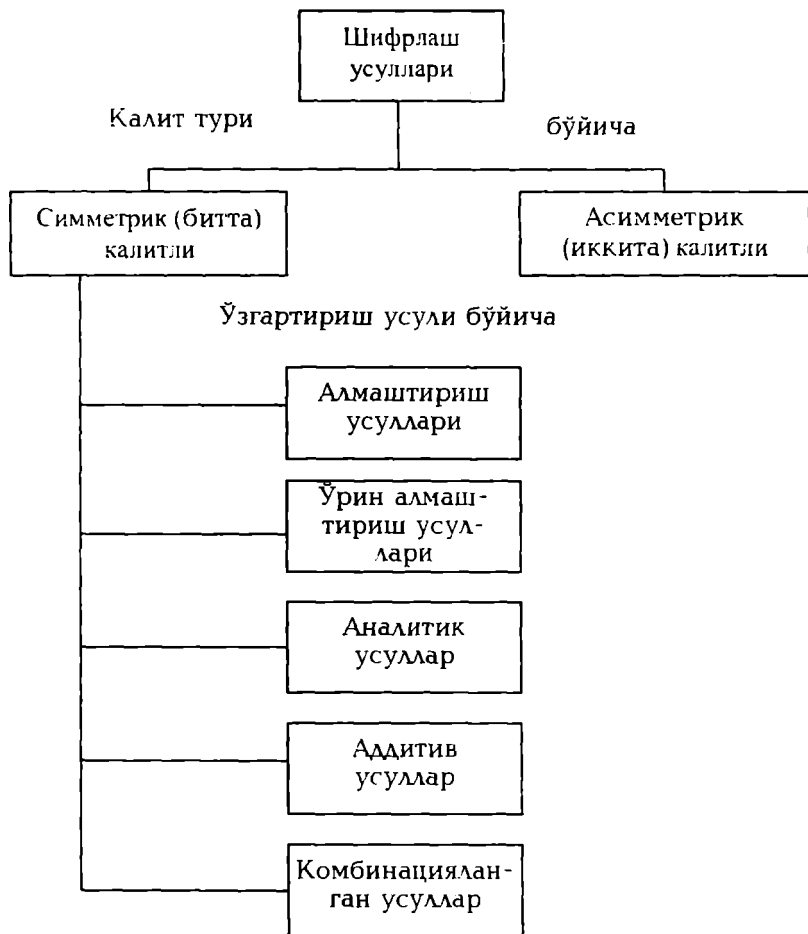
Шифрлаш усуллари турли аломатлари бўйича туркумланиши мумкин. Туркумланиш вариантларидан бири 4.5-расмда келтирилган.

Алмаштириш усуллари. Алмаштириш (подстановка) усуллари моҳияти бир алфавитда ёзилган ахборот символларини бошқа алфавит символлари билан маълум койда бўйича алмаштиришдан иборатдир. Энг содда усул сифатида *тўғридан тўғри алмаштиришни* кўрсатиш мумкин. Дастлабки ахборот ёзилувчи A_0 алфавитнинг s_{0i} символларига шифрловчи A_1 алфавитнинг s_{1i} символлари мос қуйилади. Оддий ҳолда иккала алфавит ҳам бир хил символлар тўпламига эга бўлиши мумкин.

Иккала алфавитдаги символлар ўртасидаги мослик маълум алгоритм бўйича K символлар узунлигига эга бўлган дастлабки матн T_0 символларининг рақамли эквивалентларини ўзгартириш орқали амалга оширилади.

Моноалфавитли алмаштириш алгоритми қуйидаги қадамлар кетма-кетлиги кўринишда ифодаланиши мумкин

1-қадам. $[1xR]$ ўлчамли дастлабки A_0 алфавитдаги ҳар бир символ $s_0 \in T(i=\overline{1, K})$ ни A_0 алфавитдаги s_{0i} символ тартиб рақамига мос келувчи $h_{0i}(s_{0i})$ сонга алмаштириш йўли билан рақамлар кетма-кетлиги L_{0h} ни шакллантириш.



4.5-расм. Шифрлаш усуллариининг туркумланиши.

2-қадам. L_{0i} кетма-кетлигининг ҳар бир сонини $h_{1i}=(k_1 \times h_{0i}(s_{0i}) + k_2) \pmod{R}$ формула орқали ҳисобланувчи L_{1i} кетма-кетликнинг мос сони h_{1i} га алмаштириш йўли билан L_{1i} сон кетма-кетлигини шакллантириш, бу ерда, k_1 -ўнлик коэффицент; k_2 -силжитиш коэффицент-и. Танланган k_1 , k_2 коэффицентлар h_{0i} , h_{1i} сонларнинг бир маъноли мослигини таъминлаши лозим, $h_{1i} \neq 0$ олинганида эса $h_{1i} = R$ алмашинуви бажарилиши керак.

3-кадам. L_{ih} кетма-кетликнинг ҳар бир сони $h_{ij}(s_{ij})$ ни $[1 \times R]$ ўлчамли шифрлаш алфавитнинг мос $s_{ij} \in T_j (i=1, K)$ симболи билан алмаштириш йўли билан T_j шифрматнни ҳосил қилиш.

4-кадам. Олинган шифрматн ўзгармас b узунликдаги блоklarга ажратилади. Агар охириги блок тўлиқ бўлмаса блок орқасига махсус символ-тўлдирувчилар жойлаштирилади (масалан, *).

$T_0 = \langle \text{ХИМОЯ ХИЗМАТИ} \rangle$

$A_0 = \langle \text{АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒХ} \rangle$

$A_1 = \langle \text{ОРЁБЯТЭ-ЖМЧХАВДЙФҚКСЕЗПИЦГҲЛЫШБУЮ} \rangle$

$\text{КҒН} \rangle$

$R=36; k_1=3; k_2=15; b=4$

Алгоритмнинг кадамба-кадам бажарилиши куйидаги натижаларни олинишига олиб келади.

1-кадам. $L_{oh} = \langle 35, 10, 14, 16, 31, 36, 23, 10, 9, 14, 1, 20, 10 \rangle$

2-кадам. $L_{ih} = \langle 12, 9, 21, 17, 36, 14, 12, 9, 6, 21, 18, 3, 9 \rangle$

3-кадам. $T_j = \langle \text{ХЖЕФНВХЖТЕКЁЖ} \rangle$

4-кадам. $T_j = \langle \text{ХЖЕФ НВХЖ ТЕКЁ Ж***} \rangle$

Расшифровка қилишда блоklar бирлаштирилиб K символли шифрматн T_j ҳосил қилинади. Расшифровка қилиш учун куйидаги бутун сонли тенгламани ечиш лозим:

$$k_1 h_{0i} + k_2 = nR + h_{1i}$$

k_1, k_2, h_{1i} ва R бутун сонлар маълум бўлганда h_{0i} катталиги n ни саралаш орқали ҳисобланади. Бу муолажани шифрматннинг барча символларига татбиқ қилиш унинг расшифровка қилинишига олиб келади.

Алмаштириш усулининг камчилиги сифатида дастлабки ва берилган матнлар статистик характеристикаларининг бир хиллигидир. Дастлабки матн қайси тилда ёзилганлигини билган криптоаналитик ушлаб қолинган ахборотларни статистик ишлаб, иккала алфавитдаги символлар ўртасидаги мувофиқликни аниқлаши мумкин.

Полиалфавитли алмаштириш усуллари айтарлича юкори криптобардошликка эга. Бу усуллар дастлабки матн символларини алмаштириш учун бир неча алфавитдан фойдаланишга асосланган. Расман полиалфавитли алмаштиришни куйидагича тасаввур этиш мумкин. N -алфавитли алмаштиришда дастлабки A_0 алфавитдаги s_{0i} симболи A_1 алфавитдаги s_{1i} симболи билан алмаштирилади ва ҳ. ш. s_{0i} ни s_{1i} символ билан алмаштирилганидан сўнг $S_{0i \times 1}$ символнинг ўрнини A_1 алфавитдаги $S_{1i \times 1}$ символ олади ва ҳ.

Полиалфавитли алмаштириш алгоритмлари ичида **Вижинер жадвали (матрицаси)** T_n ни ишлагувчи алгоритм энг кенг таркалган. Вижинер жадвали $[R \times R]$ ўлчамли квадрат матрицадан иборат бўлиб, (R -ишлатилаётган алфавитдаги символлар сони) биринчи каторида символлар алфавит тартибида жойлаштирилади. Иккинчи катордан бошлаб символлар чапга битта ўринга силжитилган ҳолда ёзилади. Сиқиб чиқарилган символлар ўнг тарафдаги бўшаган ўринни гўлдиради (циклик силжитиш). Агар ўзбек алфавити ишлатилса, Вижинер матрицаси $[36 \times 36]$ ўлчамга эга бўлади (4.6-расм).

АБВГД.....ЎҚГХ
БВГДЕ.....ҚҒХА
ВГДЕЖ.....ҒХАБ
АБВГ.....ЯЎҚҒХ

4.6-расм. Вижинер матрицаси.

Шифрлаш такрорланмайдиған M символдан иборат калит ёрдамида амалга оширилади. Вижинернинг тўлик матрицасидан $[(M+1), R]$ ўлчамли шифрлаш матрицаси T_{III} ажратилади. Бу матрица биринчи катордан ва биринчи элементлари калит символларига мос келувчи каторлардан иборат бўлади.

Агар калит сифатида <ҒЎЗА> сўзи танланган бўлса, шифрлаш матрицаси бешта катордан иборат бўлади (4.7-расм).

T_{III}	АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒХ_
	ҒХ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚ
	ЎҚҒХ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯ
	ЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒХ_АБВДЕЁЖ
	АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒХ_

4.7-расм. «Ғўза» калити учун шифрлаш матрицаси.

Вижинер жадвали ёрдамида шифрлаш алгоритми куйидаги кадамлар кетма-кетлигидан иборат.

1-кадам. Узунлиги M символли калит K ни танлаш.

2-кадам. Танланган калит K учун $[(M+1), R]$ ўлчамли шифрлаш матрицаси $T_{III} = (b_{ij})$ ни куриш.

3- қадам. Дастлабки матннинг ҳар бир симболи s_{or} тагига калит симболи k_m жойлаштирилади. Калит кераклича такрорланади.

4-қадам. Дастлабки матн символлари шифрлаш матрицаси T_m дан қуйидаги қоида бўйича танланган символлар билан кетма-кет алмаштирилади.

1) K калитнинг алмаштирилувчи s_{or} символга мос k_m симболи аниқланади;

2) шифрлаш матрицаси T_m даги $k_m = b_{ij}$ шарт бажарилувчи i қатор топилади.

3) $s_{or} = b_{ij}$ шарт бажарилувчи j устун аниқланади.

4) s_{or} симболи b_{ij} симболи билан алмаштирилади.

5-қадам. Шифрланган кетма-кетлик маълум узунликдаги (масалан 4 символли) блоklarга ажратилади. Охириги блокнинг бўш жойлари махсус символ-гўлдирувчилар билан гўлдирилади.

Расшифровка қилиш қуйидаги кетма-кетликда амалга оширилади.

1-қадам. Шифрлаш алгоритмининг 3-қадамидагидек шифр-матн тагига калит символлари кетма-кетлиги ёзилади.

2-қадам. Шифрматндан s_{ir} символлари ва мос калит символлари k_m кетма-кет танланади. T_m матрицада $k_m = b_{ij}$ шартни қаноатлантирувчи i қатор аниқланади. i -қаторда $b_{ij} = s_{ir}$ элемент аниқланади. Расшифровка қилинган матнда r - ўрнига b_{ij} симболи жойлаштирилади.

3-қадам. Расшифровка қилинган матн ажратилмасдан ёзилади. Хизмагчи символлар олиб ташланади.

Мисол. $K = \langle \text{ҒЎЗА} \rangle$ калити ёрдамида $T = \langle \text{ПАХТА ҒАРАМИ} \rangle$ дастлабки матнни шифрлаш ва расшифровка қилиш талаб этилсин. Шифрлаш ва расшифровка қилиш механизми 4.8-расмда келтирилган.

Полиалфавитли алмаштириш усулларининг криптобардошлиги оддий алмаштириш усулларига қараганда айтарлича юқори. Чунки уларда дастлабки кетма-кетликнинг бир хил символлари турли символлар билан алмаштирилиши мумкин. Аммо шифрнинг статистик усулларига бардошлилиги калит узунлигига боғлиқ.

Дастлабки матн ПАХТА ҒАРАМИ

Калит ҒЎЗА ҒЎЗА ҒЎЗА

Алмаштирилган

сўнги матн МЎЮТГ ЯЕАНЎУИ

Шифрматн	МЎЮТ ҒЯЕАНЎУИ
Калит	ҒЎЗА ҒЎЗА ҒЎЗА
Расшифровка	
килингн матн	ПАХТ А ҒА РАМИ
Дастлабки матн	ПАХТА ҒАРАМИ

4.8-расм. Вижинер матрицаси ёрдамида шифрлаш мисоли.

Ўрин алмаштириш усуллари. Ўрин алмаштириш усулларига биноан дастлабки матн белгиланган узунликдаги блокларга ажратилиб ҳар бир блок ичидаги символлар ўрни маълум алгоритм бўйича алмаштирилади.

Энг осон ўрин алмаштиришга мисол тарикасида дастлабки ахборот блокни матрицага катор бўйича ёзишни, ўқишни эса устун бўйича амалга оширишни кўрсатиш мумкин. Матрица каторларини тўлдириш ва шифрланган ахборотни устун бўйича ўқиш кетма-кетлиги калит ёрдамида берилиши мумкин. Усулнинг криптобардошлиги блок узунлигига (матрица улчамига) боғлиқ. Масалан, узунлиги 64 символга тенг бўлган блок (матрица ўлчами 8x8) учун калитнинг $1,6 \cdot 10^9$ комбинацияси бўлиши мумкин. Узунлиги 256 сим-волга тенг бўлган блок (матрица ўлчами 16x16) калитнинг мумкин бўлган комбинацияси $1,4 \cdot 10^{26}$ га етиши мумкин. Бу ҳолда калитни саралаш масаласи замонавий ЭХМлар учун ҳам мураккаб ҳисобланади.

Гамильтон маршрутларига асосланган усулда ҳам ўрин алмаштиришлардан фойдаланилади. Ушбу усул куйидаги кадамларни бажариш орқали амалга оширилади.

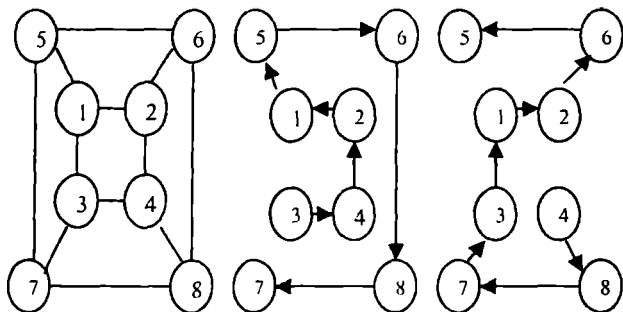
1-кадам. Дастлабки ахборот блокларга ажратилади. Агар шифрланувчи ахборот узунлиги блок узунлигига каррали бўлмаса, охириги блокдаги бўш ўринларга махсус хизматчи символлар-тўлдирувчилар жойлаштирилади (масалан, *).

2-кадам. Блок символлари ёрдамида жадвал тўлдирилади ва бу жадвалда символнинг тартиб рақами учун маълум жой ажратилади (4.9-расм).

3-кадам. Жадвалдаги символларни ўқиш маршрутларнинг бири бўйича амалга оширилади. Маршрутлар сонининг ошиши шифр криптобардошлигини оширади. Маршрутлар кетма-кет танланади ёки уларнинг навбатланиши калит ёрдамида берилади.

4-қадам. Символларнинг шифрланган кетма-кетлиги белги-ланган L узунликдаги блокларга ажратилади. L катталиқ 1-қадамда дастлабки ахборот бўлинадиган блоклар узунлигидан фарқлиниши мумкин.

Расшифровка қилиш тесқари тартибда амалга оширилади. Қалитга мос ҳолда маршрут танланади ва бу маршрутга биноан жадвал тўлдирилади.



4.9-расм. 8-элементли жадвал ва Гамильтон маршрутлари вариантлари.

Жадвалдан символлар элемент рақамлари келиши тартибда ўқилади.

Мисол. Дастлабки матн T_0 «ЎРИН АЛМАШТИРИШ УСУЛИ»ни шифрлаш талаб этилсин. Қалит ва шифрланган блоклар узунлиги мос ҳолда куйидагиларга тенг: $K=\langle 2,1,1 \rangle$, $L=4$. Шифрлаш учун 4.9-расмда келтирилган жадвал ва иккита маршрутдан фойдаланилади. Берилган шартлар учун матрицалари тўлдирилган маршрутлар 4.10-расмда келтирилган кўринишга эга.

1-қадам. Дастлабки матн учта блокка ажратилади. $B1=\langle \text{ЎРИН_АЛМ} \rangle$, $B2=\langle \text{АШТИРИШ-} \rangle$, $B3=\langle \text{УСУЛИ**} \rangle$;

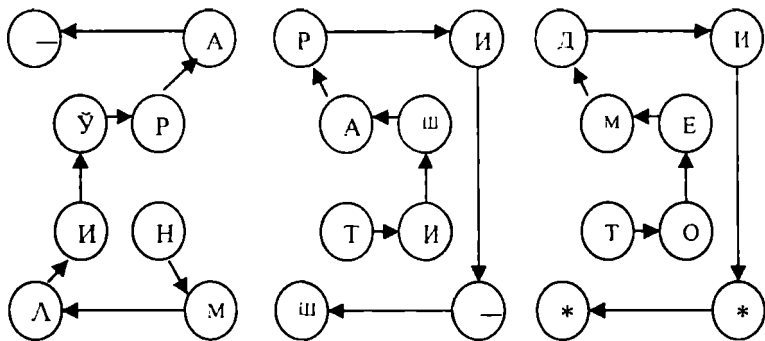
2-қадам. 2,1,1 маршрутгли учта матрица тўлдирилади;

3-қадам. Маршрутларга биноан символларни жой-жойига қўйиш орқали шифрматнни ҳосил қилиш.

$T_1=\langle \text{НМЛИЎРА_ТИШАРИ_ШТОЕМДИ**} \rangle$

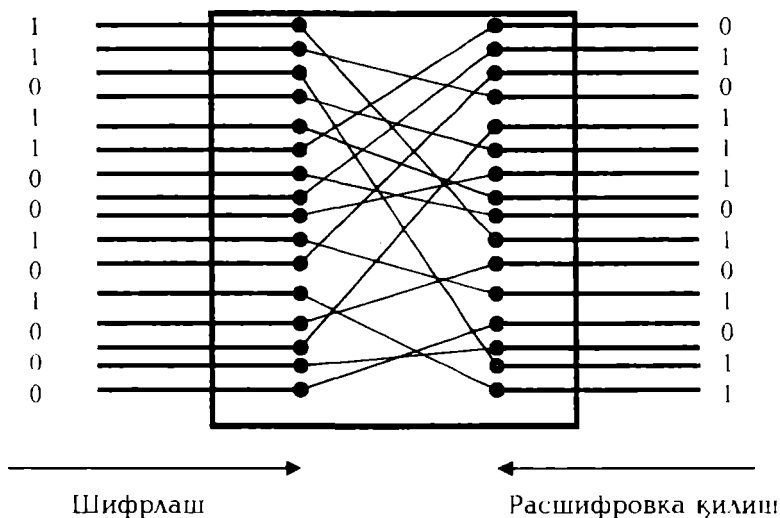
4-қадам. Шифрматнни блокларга ажратиш.

$T_1=\langle \text{НМЛИ ЎРА_ТИША_РИ_Ш_ТОЕМ_ДИ**} \rangle$



4.10-расм. Гамильтон маршрути ёрдамида шифрлаш мисоли.

Амалиётда ўрин алмаштириш усулини амалга оширувчи махсус аппарат воситалар кагта ахамиятга эга (4.11-расм).



4.11-расм. Ўрин алмаштириш схемаси.

Дастлабки ахборот блокларининг параллел иккили коди (масалан, икки байт) схемага берилди. Ички коммутация ҳисобига схемада битларнинг блоклардаги ўринлари алмаштирилади. Расшифровка

килиш учун эса схеманинг кириш ва чиқиш йўллари ўзаро алмаштирилади.

Ўрин алмаштириш усулларининг амалга оширилиши содда бўлсада, улар иккита жиддий камчиликларга эга. Биринчидан, бу усулларни статистик ишлаш орқали фош қилиш мумкин. Иккинчидан, агар дастлабки матн узунлиги K символлардан ташкил топган блокларга ажратилса, шифрни фош этиш учун шифрлаш тизимига биттасидан бошқа барча символлари бир хил бўлган тест ахборотининг $K-1$ блокини юбориш кифоя.

Шифрлашнинг аналитик усуллари. Матрица алгебрасига асосланган шифрлаш усуллари энг кўп тарқалган. Дастлабки ахборотнинг $B_k = \|b_j\|$ вектор кўринишида берилган k - блокини шифрлаш $A = \|a_{ij}\|$ матрица калитни B_k векторга кўпайтириш орқали амалга оширилади. Натижада, $C_k = \|c_i\|$ вектор кўринишидаги шифрматн блоки ҳосил қилинади. Бу векторнинг элементлари $c_i = \sum_j a_{ij} b_j$ ифодаси орқали аниқланади.

Ахборотни расшифровка қилиш C_k векторларини A матрицага тескари бўлган A^{-1} матрицага кетма-кет кўпайтириш орқали аниқланади.

Мисол. $T_0 = \langle \text{АЙЛАНА} \rangle$ сўзини матрица-калит

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$$

ёрдамида шифрлаш ва расшифровка қилиш талаб этилсин.

Дастлабки сўзни шифрлаш учун куйидаги кадамларни бажариш лозим.

1-кадам. Дастлабки сўзнинг алфавитдаги харфлар тартиб рақами кетма-кетлигига мос сон эквивалентини аниқлаш.

$$T_1 = \langle 1, 10, 12, 1, 14, 1 \rangle$$

2-кадам. A матрицани $B_1 = \{1, 10, 12\}$ ва $B_2 = \{1, 14, 1\}$ векторларга кўпайтириш.

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 10 \\ 12 \end{vmatrix} = \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix}$$

$$C_2 = \left| \begin{array}{ccc|c} 1 & 4 & 8 & 1 \\ 3 & 7 & 2 & 14 \\ 6 & 9 & 5 & 1 \end{array} \right| = \left| \begin{array}{c} 65 \\ 103 \\ 137 \end{array} \right|$$

3-қадам. Шифрланган сўзни кетма-кет сонлар кўринишида ёзиш.

$$T_1 = \langle 137, 97, 156, 65, 103, 137 \rangle$$

Шифрланган сўзни расшифровка қилиш қуйидагича амалга оширилади:

1-қадам. A матрицанинг аниқловчиси ҳисобланади:

$$|A| = -115.$$

2-қадам. Ҳар бир элементи A матрицадаги a_{ij} элементнинг алгебраик тўлдирувчиси бўлган бириктирилган матрица A^* аниқланади.

$$A^* = \left| \begin{array}{ccc} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{array} \right|$$

3-қадам. Транспонирланган матрица A^T аниқланади.

$$A^T = \left| \begin{array}{ccc} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{array} \right|$$

4-қадам. Қуйидаги формула бўйича тесқари матрица A^{-1} ҳисобланади:

$$A^{-1} = \frac{A^T}{|A|}$$

Ҳисоблаш натижасида қуйидагини оламиз.

$$A^{-1} = \left| \begin{array}{ccc} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{array} \right|$$

5-қадам. B_1 ва B_2 векторлар аниқланади:

$$B_1 = A^{-1}C_1; \quad B_2 = A^{-1}C_2.$$

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix} = \begin{vmatrix} 1 \\ 10 \\ 12 \end{vmatrix}$$

$$B_2 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 65 \\ 103 \\ 137 \end{vmatrix} = \begin{vmatrix} 1 \\ 14 \\ 1 \end{vmatrix}$$

6-қадам. Расшифровка килинган сўзнинг сон эквиваленти $T_3 = \langle 1, 10, 12, 1, 14, 1 \rangle$ символлар билан алмаштирилади. Натижада, дастлабки сўз $T_0 = \langle \text{АЙЛАНА} \rangle$ ҳосил бўлади.

Шифрлашнинг аддитив усуллари. Шифрлашнинг *аддитив усуллари*га биноан дастлабки ахборот символларига мос келувчи рақам кодларини кетма-кетлиги *гамма* деб аталувчи қандайдир символлар кетма-кетлигига мос келувчи кодлар кетма-кетлиги билан кетма-кет жамланади. Шу сабабли, шифрлашнинг аддитив усуллари *гаммалаш* деб ҳам аталади.

Ушбу усуллар учун қалит сифатида гамма ишлатилади. Аддитив усулнинг криптобардошлиги қалит узунлигига ва унинг статис-тик характеристикаларининг текислигига боғлиқ. Агар қалит шифрланувчи символлар кетма-кетлигидан қисқа бўлса, шифрматн криптоаналитик томонидан статистик усуллар ёрдамида расшифровка қилиниши мумкин. Қалит ва дастлабки ахборот узунликлари қанчалик фаркланса, шифр-матнга муваффақиятли ҳужум эҳтимоллиги шунчалик ортади. Агар қалит узунлиги шифрланувчи ахборот узунлигидан катта бўлган тасодифий сонларнинг даврий бўлмаган кетма-кетлигидан иборат бўлса, қалитни билмасдан туриб шифрматнни расшифровка қилиш амалий жиҳатдан мумкин эмас. Алмаштириш усулларидагидек гаммалашда қалит сифатида рақамларнинг такрорланмайдиган кетма-кетлиги ишлатилиши мумкин.

Амалиётда асосини псевдотасодифий сонлар генераторлари (датчиклари) ташкил этган аддитив усуллар энг кўп тарқалган ва самарали ҳисобланади. Генератор псевдотасодифий сонларнинг

чексиз кетма-кетлигини шакллантиришда нисбатан киска узунликдаи дастлабки ахборотдан фойдаланади.

Псевдотасодифий сонлар кетма-кетлигини шакллантиришда конгруэнт генераторлардан ҳам фойдаланилади. Бу синф генераторлари сонларнинг шундай псевдотасодифий кетма-кетликларини шакллантирадики, улар учун генераторларнинг даврийлиги ва чиқиш йўли кетма-кетликларининг тасодифийлиги каби асосий характеристикаларини катъий математик тарзда ифодалаш мумкин.

Конгруэнт генераторлар ичида ўзининг соддалиги ва самаралилиги билан чизикли генератор ажралиб тўради. Бу генератор куйидаги муносабат бўйича сонларнинг псевдотасодифий кетма-кетликларини шакллантиради:

$$T(i+1) = (a \cdot T(i) + c) \bmod m ;$$

бу ерда, a ва c - ўзгармаслар, $T(0)$ -туғдирувчи (сабаб бўлувчи) сон сифатида танланган дастлабки катталиқ.

Бундай дагчикнинг такрорланиш даври a ва c катталикларига боғлиқ. m киймаги одатда 2^s га тенг қилиб олинади. бу ерда, s -ЭХМдаги сўзнинг битлардаги узунлиги. Шакллантирувчи сон кетма-кетликларининг такрорланиш даври c -ток сон ва $a \pmod{4} = 1$ бўлгандагина максималъ бўлади. Бундай генераторларни аппарат ёки программ воситалари орқали осонгина яратиш мумкин.

Шифрлашнинг комбинацияланган усуллари. Қудратли компьютерлар, гармок технологиялари ва нейронли ҳисоблашларнинг пайдо бўлиши ҳозиргача умуман фош қилинмайди деб ҳисобланган криптографик тизимларни обрўсизлантирилишига сабаб бўлди. Бу эса ўз навбатида юқори бардошликка эга криптографик тизимларни яратиш устида ишлашни такозо этди. Бундай криптографик тизимларни яратиш усулларида бири шифрлаш усуллари комбинациялашдир. Куйида энг кам вақт сарфида криптобардошликни жиддий ошишини таъминловчи шифрлашнинг комбинацияланган усули устида сўз боради. Шифрлашнинг ушбу комбинацияланган усулига биноан маълумотларни шифрлаш икки босқичда амалга оширилади. Биринчи босқичда маълумотлар стандарт усул (масалан, DES усул) ёрдамида шифрланса, иккинчи босқичда шифрланган маълумотлар махсус усул бўйича қайта шифрланади. Махсус усул сифатида маълумотлар векторини элементлари нолдан фаркли бўлган сон матричасига кўпайтиришдан фойдаланиш мумкин.

Гаммалашни қўллашда агар шифр гаммаси сифатда ракамларнинг такрорланмайдиган кетма-кетлиги ишлатилса шифрланган матнни фoш қилиш жуда қийин. Одатда, шифр гаммаси ҳар бир шифрланувчи сўз учун тасодифий ўзгариши лозим. Агар шифр гаммаси шифрланган сўз узунлигидан катта бўлса ва дастлабки матннинг ҳеч қандай қисми маълум бўлмаса, шифрни факат тўғридан-тўғри саралаш орқали фoш этиш мумкин. Бунда криптобардошлик қалит ўлчами орқали аниқланади. Шифрлашнинг бу усулидан кўпинча химоя тизимининг дастурий амалга оширилишида фойдаланилади ва шифрлашнинг бу усулига асосланган тизимларда бир секундда маълумотларнинг бир неча юз байтини шифрлаш имконияти мавжуд. Расшифровка қилиш жараёни-қалит маълум бўлганида шифр гаммасини қайта генерациялаш ва уни шифрланган маълумотларга сингдиришдан иборат.

Шифрланган маълумотлар векторини матрицага кўпайтиришни қўллашда шифрланган матн бир байт узунликдаги f_i векторларга ажратилади ва ҳар бир вектор квадрат матрица $\|M_{ij}\|$ га кўпайтирилади ва шифрланган векторлар шакллантирилади:

$$f_i^* = f_i \cdot \|M_{ij}\|$$

Бу усулнинг асосий афзаллиги сифатида унинг маълумотлар ишланишининг турли жабҳаларидаги мосланувчанлигини кўрсатиш мумкин. Ҳар бир вектор алоҳида шифрланганлиги сабабли маълумотлар блоқини ўзатиш ва дастурланган маълумотлардан ихтиёрий фойдаланиш имконияти туғилади. Ушбу усулни аппарат ёки дастурий усулда амалга ошириш мумкин.

Расшифровка қилиш жараёнида шифрланган f^* векторларни тескари матрица $\|M_{ij}^{-1}\|$ га кўпайтирилади.

$$f_i = f_i^* \cdot \|M_{ij}^{-1}\|$$

Комбинацияланган усулларнинг юқори самарадорлигига унинг иккала босқичини аппарат усулда амалга ошириш орқали эришиш мумкин. Аммо бу ускуна харажатларининг жиддий ошишига олиб келади. Дастурий усулда амалга оширилишида эса маълумотларни шифрлаш ва расшифровка қилиш вақти ошиб кетади. Шу сабабли комбинацияланган усулларни аппарат-дастурий усулда, яъни усулнинг бир босқичи аппарат усулда, иккинчи босқичи дастурий усулда амалга оширилиши мақсадга мувофиқ ҳисобланади.

4.3. Асимметрик шифрлаш тизимлари

Асимметрик шифрлаш тизимларида иккита калит ишлатилади. Ахборот очик калит ёрдамида шифрланса, махфий калит ёрдамида расшифровка қилинади. Асимметрик шифрлаш тизимларини очик калитли шифрлаш тизимлар деб ҳам юритилади.

Очик калитли тизимларини қўллаш асосида қайтарилмас ёки бир томонли функциялардан фойдаланиш ётади. Бундай функциялар қуйидаги хусусиятларга эга. Маълумки X маълум бўлса $y=f(x)$ функцияни аниқлаш осон. Аммо унинг маълум қиймати бўйича x ни аниқлаш амалий жиҳатдан мумкин эмас. Криптографияда яширин деб аталувчи йўлга эга бўлган бир томонли функциялар ишлатилади. Z параметрли бундай функциялар қуйидаги хусусиятларга эга. Маълум Z учун E_z ва D_z алгоритмларини аниқлаш мумкин. E_z алгоритми ёрдамида аниқлик соҳасидаги барча x учун $f_z(x)$ функцияни осонгина олиш мумкин. Худди шу тарика D_z алгоритми ёрдамида жоиз қиймаглар соҳасидаги барча y учун тескари функция $x=f^{-1}(y)$ ҳам осонгина аниқланади. Айни вақтда жоиз қийматлар соҳасидаги барча Z ва деярли барча, y учун ҳатто E_z маълум бўлганида ҳам $f^{-1}(y)$ ни ҳисоблашлар ёрдамида топиб бўлмайди. Очик калит сифатида y ишлатилса, махфий калит сифатида x ишлатилади.

Очик калитни ишлатиб шифрлаш амалга оширилганда ўзаро мулоқотда бўлган субъектлар ўртасида махфий калитни алмашиш зарурияти йўқолади. Бу эса ўз навбатида узатилувчи ахборотнинг криптохимоясини соддалаштиради.

Очик калитли криптогизимларни бир томонли функциялар кўриниши бўйича фарқлаш мумкин. Буларнинг ичида RSA, Эль-Гамал ва Мак-Элис тизимларини алоҳида тилга олиш ўринли. Ҳозирда энг самарали ва кенг тарқалган очик калитли шифрлаш алгоритми сифатида RSA алгоритмини кўрсатиш мумкин. RSA номи алгоритмни яратувчилари фамилияларининг биринчи харфидан олинган (Rivest, Shamir ва Adleman).

Алгоритм модуль арифметикасининг даражага кўтариш амалидан фойдаланишга асосланган. Алгоритмни қуйидаги кадамлар кетма-кетлиги кўринишида ифодалаш мумкин.

1-кадам. Иккита 200дан катта бўлган туб сон p ва q танланади.

2-кадам. Калитнинг очик ташкил қуввчиси n ҳосил қилинади

$$n=p*q.$$

3-кадам. Куйидаги формула бўйича Эйлер функцияси ҳисобланади:

$$f(p,q)=(p-1)(q-1).$$

Эйлер функцияси p билан ўзаро туб, 1 дан p гача бўлган бутун мусбат сонлар сонини кўрсатади. Ўзаро туб сонлар деганда 1 дан бошқа бирорта умумий бўлувчисига эга бўлмаган сонлар тушунилади.

4-кадам. $f(p,q)$ киймати билан ўзаро туб бўлган катта туб сон d танлаб олинади.

5-кадам. Куйидаги шартни қаноатлантирувчи e сони аниқланади:

$$e \cdot d = 1 \pmod{f(p,q)}.$$

Бу шартга биноан $e \cdot d$ кўпайтманинг $f(p,q)$ функцияга бўлишдан қолган қолдиқ 1 га тенг. e сони очик қалитнинг иккинчи ташкил этувчиси сифатида қабул қилинади. Махфий қалит сифатида d ва n сонлари ишлатилади.

6-кадам. Дастлабки ахборот унинг физик табиатидан қатъий назар рақамли иккили кўринишда ифодаланади. Битлар кетма-кетлиги L бит узунликдаги блоklarга ажратилади, бу ерда, $L - L \geq \log_2(n+1)$ шартини қаноатлантирувчи энг кичик бутун сон. Ҳар бир блок $[0, n-1]$ ораликка тааллуқли бутун мусбат сон қаби кўрилади. Шундай қилиб, дастлабки ахборот $X(i)$, $i=1, I$ сонларнинг кетма-кетлиги орқали ифодаланади. i нинг киймати шифрланувчи кетма-кетликнинг узунлиги орқали аниқланади.

7-кадам. Шифрланган ахборот куйидаги формула бўйича аниқланувчи $Y(i)$ сонларнинг кетма-кетлиги кўринишида олинади:

$$Y(i) = (X(i))^e \pmod{n}.$$

Ахборотни расшифровка қилишда куйидаги муносабатдан фойдаланилади:

$$X(i) = (Y(i))^d \pmod{n}.$$

Мисол. <ГАЗ> сўзини шифрлаш ва расшифровка қилиш талаб этилсин. Дастлабки сўзни шифрлаш учун куйидаги қадамларни бажариш лозим.

1-кадам. $p=3$ ва $q=11$ танлаб олинади.

2-кадам. $n = 3 \cdot 11 = 33$ ҳисобланади.

3-кадам. Эйлер функцияси аниқланади.

$$f(p, q) = (3-1) \cdot (11-1) = 20$$

4-қадам. Ўзаро туб сон сифатида $d=3$ сони танлаб олинади.

5-қадам. $(e \cdot 3) \pmod{20} = 1$ шаргини каноатлантирувчи сони танланади. Айтайлик, $e=7$.

6-қадам. Дастлабки сўзнинг алфавитдаги ҳарфлар гариб рақами кетма-кетлигига мос сон эквиваленти аниқланади. А ҳарфига -1, Г ҳарфига-4, З ҳарфига -9. Ўзбек алфавитида 36 та ҳарф ишлагилиши сабабли иккили кодда ифодалаш учун 6 та иккили хона керак бўлади. Дастлабки ахборот иккили кодда куйидаги кўринишга эга бўлади:

000100 000001 001001.

Блок узунлиги L бутун сонлар ичидан $L \geq \log_2(33+1)$ шартини каноатлантирувчи минимал сон сифатида аниқланади. $n=33$ бўлганлиги сабабли $L=6$.

Демак, дастлабки матн $X(i) \leq \langle 4, 1, 9 \rangle$ кетма-кетлик кўринишида ифодаланади.

7-қадам. $X(i)$ кетма-кетлиги очик калит $\{7, 33\}$ ёрдамида шифрланади:

$$Y(1) = (4^7) \pmod{33} = 16384 \pmod{33} = 16$$

$$Y(2) = (1^7) \pmod{33} = 1 \pmod{33} = 1$$

$$Y(3) = (9^7) \pmod{33} = 4782969 \pmod{33} = 15$$

Шифрланган сўз $Y(i) = \langle 16, 1, 15 \rangle$

Шифрланган сўзни расшифровка қилиш махфий калит $\{3, 33\}$ ёрдамида бажарилади:

$$Y(1) = (16^3) \pmod{33} = 4096 \pmod{33} = 4$$

$$Y(2) = (1^3) \pmod{33} = 1 \pmod{33} = 1$$

$$Y(3) = (15^3) \pmod{33} = 3375 \pmod{33} = 9$$

Дастлабки сон кетма-кетлиги расшифровка қилинган $X(i) = \langle 4, 1, 9 \rangle$ кўринишида дастлабки матн $\langle \text{ГАЗ} \rangle$ билан алмаш-гирилади.

Келтирилган мисолда ҳисоблашларнинг соддалигини таъминлаш мақсадида мумкин бўлган кичик сонлардан фойдаланилди.

Эль-Гамал тизими чекли майдонларда дискрет логарифмларнинг ҳисобланиш мураккаблигига асосланган. RSA ва Эль-Гамал тизимларининг асосий камчилиги сифатида модуль арифметикасидаги мураккаб амалларнинг бажарилиши заруриятини кўрсатиш

мумкин. Бу ўз навбатида айтарлича ҳисоблаш ресурсларини талаб қилади.

Мак-Элис криптолизмида хатоликларни тузатувчи кодлар ишлатилади. Бу тизим RSA тизимига нисбатан тезроқ амалга оширилсада, жиддий камчиликка эга. Мак-Элис криптолизмида катта узунликдаги калит ишлатилади ва олинган шифрматн узунлиги дастлабки матн узунлигидан икки марта катта бўлади.

Барча очик калитли шифрлаш усуллари учун *NP-тўлик* масалани (тўлик саралаш масаласи) ечишга асосланган криптотахлил усулидан бошқа усулларининг йўқлиги катъий исботланмаган. Агар бундай масалаларни ечувчи самарали усуллар пайдо бўлса, бундай ҳилдаги криптолизим обрўсизлантирилади.

Юқорида кўрилган шифрлаш усулларининг криптобардошлиги калит узунлигига боғлиқ бўлиб, бу узунлик замонавий тизимлар учун, лоақал, 90 битдан катта бўлиши шарт.

Айрим муҳим кўлланишларда нафақат калит, балки шифрлаш алгоритми ҳам махфий бўлади. Шифрларнинг криптобардошлигини ошириш учун бир неча калит (одатда, учта) ишлатилиши мумкин. Биринчи калит ёрдамида шифрланган ахборот иккинчи калит ёрдамида шифрланади ва х.

4.4. Шифрлаш стандартлари

Россиянинг ахборотни шифрлаш стандарти. Россия Федерациясида ҳисоблаш машиналари, комплекслари ва гармоқларида ахборотни криптографик ўзгартириш алгоритмларига давлат стандарти (ГОСТ 2814-89) жорий этилган. Бу алгоритмлар махфийлик даражаси ихтиёрий бўлган ахборотни ҳеч қандай чекловсиз шифрлаш имконини беради. Алгоритмлар аппарат ва дастурий усулларда амалга оширилиши мумкин.

Стандартда ахборотни криптографик ўзгартиришнинг қуйидаги алгоритмлари мавжуд:

- оддий алмашгириш;
- гаммалаш;
- тескари боғланишли гаммалаш;
- имитовставка.

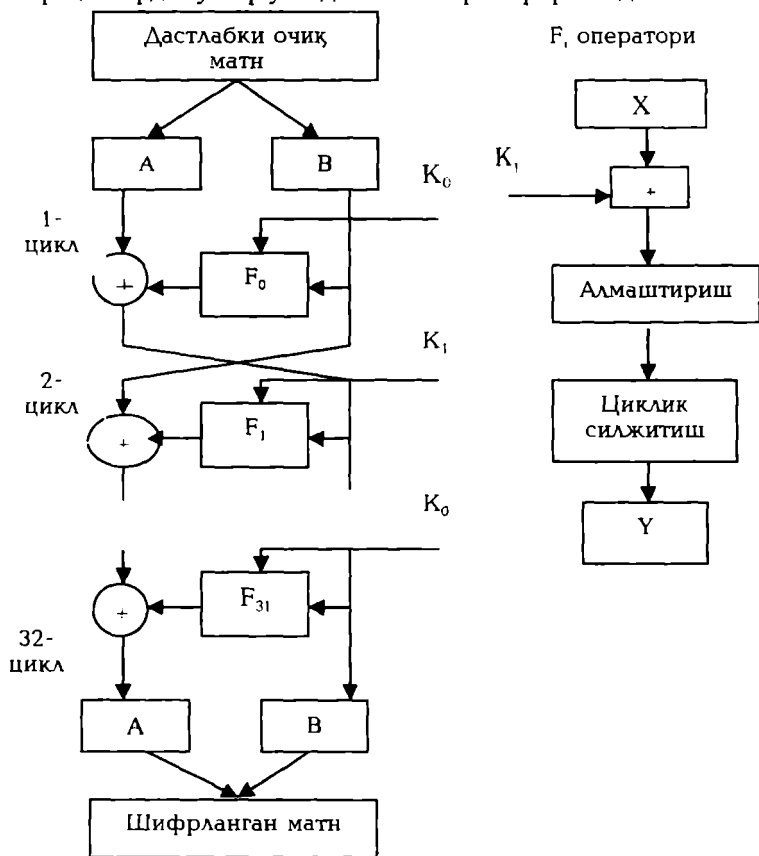
Бу алгоритмлар учун 8 га 32 хонали иккили сўзларга ажратилган 256 бит ўлчамли калитнинг ишлатилиши ҳамда дастлабки шифрланувчи иккили кетма-кетликнинг 64 битли блоklarга ажратилиши умумий ҳисобланади.

Оддий аламштириш алгоритмининг моҳияти қуйидагича (4.12-расм).

Дастлабки кетма-кетликнинг 64 битли блоқи иккига 32 хонали А ва В иккили сўзларга ажратилади. А сўзлар блокнинг кичик хо-

наларини B сўзлар эса катта хоналарини ташкил этади. Бу сўзларга сони $i=32$ бўлган циклик итерация оператори F_i қўлланилади. Блокнинг кичик битларидаги сўз (биринчи итерациядаги A сўзи) калитнинг 32 хонали сўзи билан $\text{mod} 2^{32}$ бўйича жамланади; ҳар бири 4 битдан иборат қисмларга (4 хонали кириш йўли векторлари) ажратилади; махсус алмаштириш узеллари ёрдамида ҳар бир вектор бошқаси билан алмаштирилади; олинган векторлар 32 хонали сўзга бирлаштирилиб, чап тарафга циклик равишда силжитилади ва 64 хонали блокдаги бошқа 32 хонали сўз (биринчи итерациядаги B сўзи) билан $\text{mod} 2$ бўйича жамланади.

Биринчи итерация тугаганидан сўнг кичик битлар ўрнида B сўз жойланади, чап тарафда эса A сўз жойланади. Кейинги итерацияларда сўзлар устидаги амаллар такрорланади.



4.12-расм. Оддий алмаштириш алгоритмида шифрлаш жараёнинини блок-схемаси.

Ҳар бир i -итерацияда K_i калитнинг (калитлар 8 та) 32 хонали сўзи куйидаги коидага биноан танланади:

$$K_i = \begin{cases} (i-1) \bmod 8, & 1 \leq i \leq 24 \quad \text{бўлганда,} \\ 32 - i, & i \geq 25 \quad \text{бўлганда,} \\ 0, & i = 32 \quad \text{бўлганда,} \end{cases}$$

Демак, шифрлашда калитнинг танланиш тартиби куйидаги кўринишда бўлади:

$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7,$

$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0.$

Расшифровка қилишда калитлар тесқари тартибда ишлатилади.

Алмаштириш блоки кетма-кет танланувчи 8 та алмаштириш узелларидан иборат. Алмаштириш узели ҳар бирида алмаштириш вектори (4 бит) жойлашган 16 қаторли жадвалдан иборат. Кириш йўли вектори жадвалдаги қатор манзилини аниқласа, қатордаги сон алмаштиришнинг чиқиш йўли вектори ҳисобланади. Алмаштириш жадвалига ахборот олдиндан ёзилади ва камдан-кам ўзгартирилади.

Гаммалаш алгоритмида дастлабки битларнинг кетма-кетлиги гамманинг битлари кетма-кетлиги билан $\bmod 2$ бўйича жамланади. Гамма оддий алмаштириш алгоритмига биноан ҳосил қилинади. Гаммани шакллантиришда иккита махсус доимийлардан ҳамда 64-хонали иккили кетма-кетлик синхросилкадан фойдаланилади. Ахборотни фақат синхросилка борлигида расшифровка қилиш мумкин.

Синхросилка махфий бўлмайди ва очик ҳолда ҳисоблаш машинаси хотирасида сақланиши ёки алоқа канали орқали узатилиши мумкин.

Тесқари боғланишли гаммалаш алгоритми гаммалаш алгоритмидан фақат шифрлаш жараёнининг биринчи қадамидаги ҳаракатлар билан фарқланади.

Имитовставка нотўғри ахборотни зўрлаб киритилишидан химоялашда ишлатилади. Имитовставка дастлабки ахборот ва махфий калитни ўзгартириш функцияси ҳисобланади. У k бит узунликдаги иккили кетма-кетликдан иборат бўлиб, k нинг қиймати нотўғри ахборотнинг зўрлаб киритилиши эҳтимоллиги P_{jk} билан куйидаги муносабат билан боғланган.

$$P_{jk} = \frac{1}{2^k}$$

Имитовставка шаклантириш алгоритми куйидаги харакатлар кетма-кетлигидан иборат. Очик ахборот 64 битли $T(i)$ ($i=1,2,3,\dots,m$) блокларга ажратилади, бу ерда m -шифрланувчи ахборот хажми орқали аникланади. Биринчи блок $T(1)$ оддий алмаштириш алгоритмининг биринчи 16 итерацияларига биноан ўзгартирилади. Калит сифатида дастлабки ахборот шифрланишда ишлатиладиган калит олинади. Олинган 64 битли иккили сўз иккинчи блок $T(2)$ билан mod2 бўйича жамланади. $T(1)$ блок усгида қандай итерация ўзгартиришлари бажарилган бўлса жамлаш натижаси устида ҳам шундай ўзгартиришлар амалга оширилади ва охирида $T(3)$ блок билан mod2 бўйича жамланади. Бундай харакатлар дастлабки ахборотнинг $m-1$ блоки бўйича такрорланади. Агар охириги $T(m)$ блок тўлик бўлмаса, у 64 хонагача ноллар билан тўлдиради. Бу блок $T(m-1)$ блок ишланиш натижаси билан mod2 бўйича жамланади ва оддий алмаштириш алгоритмининг биринчи 16 итерациялари бўйича ўзгартирилади. Ҳосил бўлган 64 хонали блокдан k бит узунликдаги сўз ажратиб олинади ва бу сўз имитовставка ҳисобланади.

Имитовставка шифрланган ахборотнинг охирига жойлаштирилади. Бу ахборот олингандан сўнг, у расшифровка қилинади. Расшифровка қилинган ахборот бўйича имитовставка аникланади ва олингани билан солиштирилади. Агар имитовставкалар мос келмаса, расшифровка қилинган ахборот нотўғри деб ҳисобланади.

АҚШнинг ахборотни шифрлаш стандарти. АҚШда давлат стандарти сифатида DES(Data Encryption Standart) стандарти ишлатилган. Бу стандарт асосини ташкил этувчи шифрлаш алгоритми IBM фирмаси томонидан ишлаб чиқилган бўлиб, АҚШ Миллий Хавфсизлик Агентлигининг мутахассислари томонидан текширилгандан сўнг давлат стандарти макomini олган. DES стандартидан нафақат федерал департаментлар, балки нодавлат ташкилотлар, нафақат АҚШда, балки бутун дунёда фойдаланиб келинган.

DES стандартида дастлабки ахборот 64 битли блокларга ажратилади ва 56 ёки 64 битли калит ёрдамида криптографик ўзгартирилади.

Дастлабки ахборот блоклари ўрин алмаштириш ва шифрлаш функциялари ёрдамида итерацион ишланади. Шифрлаш функциясини ҳисоблаш учун 64 битли калитдан 48 битлигини олиш, 32-битли кодни 48 битли кодга кенгайтириш, 6-битли кодни 4-битли

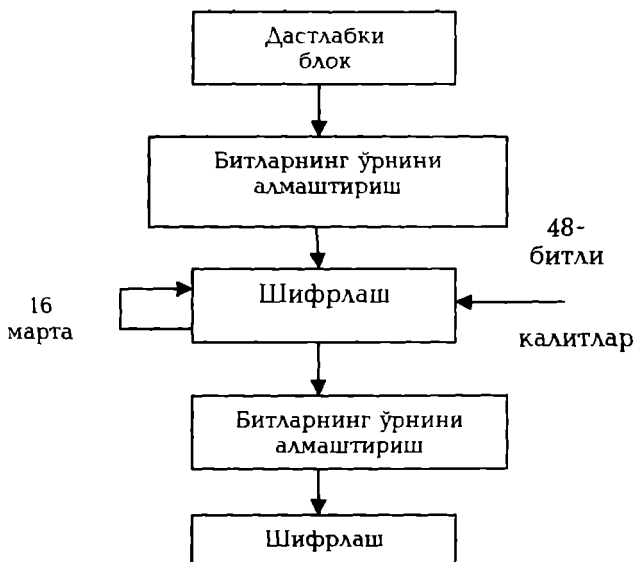
кодга ўзгартириш ва 32-битли кетма-кетликнинг ўрнини алмаштириш кўзда тутилган.

DES алгоритмидаги шифрлаш жараёнининг блок-схемаси 4.13-расмда келтирилган.

Расшифровка жараёни шифрлаш жараёнига инверс бўлиб, шифрлашда ишлатиладиган калит ёрдамида амалга оширилади.

Ҳозирда бу стандарт қуйидаги иккита сабабга кўра фойдаланишга бутунлай яроксиз ҳисобланади:

- калитнинг узунлиги 56 битни ташкил этади, бу ЭХМларнинг замонавий ривожини учун жуда кам;
- алгоритм яратилаётганида унинг аппарат усулда амалга оширилиши кўзда тутилган эди, яъни алгоритмда микропроцессорларда бажарилишида кўп вақт талаб қилувчи амаллар бор эди (масалан, машина сўзида маълум схема бўйича битларнинг ўрнини алмаштириш каби).



4.13-расм. DES алгоритмида шифрлаш жараёнининг блок-схемаси.

Бу сабаблар АКШ стандартлаш институтининг 1997 йилда симметрик алгоритмнинг янги стандартига танлов эълон қилишига олиб келди. Танлов шартларига биноан алгоритмга қуйидаги талаблар қўйилган эди:

- алгоритм симметрик бўлиши керак;
- алгоритм блокчи шифр бўлиши керак;
- блок узунлиги 128 бит бўлиб, 128, 192, ва 256 битли калит узунликларини таъминлаши лозим.

Ундан ташқари танловда иштирок этувчилар учун қуйидаги тавсиялар берилган эди:

- ҳам аппарат усулда ҳам программ усулда осонгина амалга оширилувчи амаллардан фойдаланиш;

- 32 хонали процессорлардан фойдаланиш;
- иложи борича шифр тузилмасини мураккаблаштирмаслик. Бу ўз навбатида барча кизиқувчиларнинг алгоритмни мустақил тарзда криптоtahlil қилиб, унда қандайдир ҳужжатсиз имкониятлар йўқлигига ишонч ҳосил қилишлари учун зарур ҳисобланади.

2000 йил 2 октябрда танлов натижаси эълон қилинди. Танлов ғолиби деб Бельгия алгоритми RIJNDAEL топилди ва шу ондан бошлаб алгоритм-ғолибдан барча патент чегараланишлари олиб ташланди.

Ҳозирда AES (Advanced Encryption Standard) деб аталувчи ушбу алгоритм Дж. Деймен (J. Daemen) ва В. Райджмен (V. Rijmen) томонидан яратилган. Бу алгоритм ноанъанавий блокчи шифр бўлиб, кодланувчи маълумотларнинг ҳар бир блоқи қабул қилинган блок узунлигига қараб 4x4, 4x6 ёки 4x8 ўлчамдаги байтларнинг икки ўлчамли массивлари кўринишига эга.

Шифрдаги барча ўзгартиришлар қатъий математик асосга эга. Амалларнинг тузилмаси ва кетма-кетлиги алгоритмнинг ҳам 8-битли, ҳам 32-битли микропроцессорларда самарали бажарилишига имкон беради. Алгоритм тузилмасида баъзи амалларнинг параллел ишланиши ишчи станцияларида шифрлаш тезлигининг 4 марта ошишига олиб келади.

Ўзбекистоннинг ахборотни шифрлаш стандарти. Ушбу «Маълумотларни шифрлаш алгоритми» стандарти Ўзбекистон алоқа ва ахборотлаштириш агентлигининг илмий-техник ва маркетинг тадқиқотлари маркази томонидан ишлаб чиқилган ва унда Ўзбекистон Республикасининг «Электрон рақамли имзо хусуси-

да»ги ва «Электрон хужжат алмашинуви хусусида»ги қонунларининг меъёрлари амалга оширилган.

Ушбу стандарт – криптографик алгоритм, электрон маълумотларни химоялашга мўлжалланган. Маълумотларни шифрлаш алгоритми симметрик блокли шифр бўлиб, ахборотни шифрлаш ва расшифровка қилиш учун ишлатилади. Алгоритм 128 ёки 256 бит узунлигидаги маълумотларни шифрлашда ва расшифровка қилишда 128, 256, 512 битли калитлардан фойдаланиши мумкин.

Стандарт ЭХМ тармоқларида, телекоммуникацияда, алоҳида ҳисоблаш комплекслари ва ЭХМда ахборотни ишлаш тизимлари учун ахборотни шифрлашнинг умумий алгоритмини ва маълумотларни шифрлаш қондасини белгилайди.

Шифрлаш алгоритми дастурий ва аппарат усулларда амалга оширилиши мумкин.

Симметрик шифрлашнинг барча тизимлари қуйидаги камчиликларга эга:

- ахборот алмашувчи иккала субъект учун махфий калитни узатиш каналининг ишончлилиги ва хавфсизлигига қўйиладиган талабларнинг қатъийлиги;

- калитларни яратиш ва тақсимлаш хизматида қўйиладиган талабларнинг юқорилиги. Сабаби, ўзаро алоқанинг «хар ким – хар ким билан» схемасида « n » та абонент учун $n(n-1)/2$ та калит талаб этилади, яъни калитлар сонининг абонентлар сонига боғлиқлиги квадратли. Масалан, $n=1000$ абонент учун талаб қилинадиган калитлар сони $n(n-1)/2=499500$. Шу сабабли, фойдаланувчилари юз миллиондан ошиб кетган «Internet» тармоғида симметрик шифрлаш тизимини қўшимча усул ва воситаларсиз қўллашнинг иложи йўқ.

Асимметрик шифрлашнинг биринчи ва кенг тарқалган криптоалгоритми RSA (4.3 га қаралсин) 1993 йилда стандарт сифатида қабул қилинди. Ушбу криптоалгоритм хар гарафлама тасдиқланган ва калитнинг етарли узунлигида бардошлиги эътироф этилган. Ҳозирда 512 битли калит бардошлиқни таъминлашда етарли ҳисобланмайди ва 1024 битли калитдан фойдаланилади. Баъзи муаллифларнинг фикрича процессор қувватининг ошиши RSA криптоалгоритмининг тўлиқ саралаш ҳужумларга бардошлигининг йўқолишига олиб келади. Аммо, процессор қувватининг ошиши янада узун калитлардан фойдаланишга, ва демак, RSA бардошлигини ошишига имкон яратади.

Асимметрик криптоалгоритмларда симметрик криптоалгоритмлардаги камчиликлар бартарф этилган:

- калитларни махфий тарзда отказиш зарурияти йўқ; асимметрик шифрлаш очик калитларни динамик тарзда етказишга имкон беради, симметрик шифрлашда эса химояланган алока сеанси бошланишидан аввал махфий калитлар алмашилиши зарур эди;
- калитлар сонининг фойдаланувчилар сонига квадратли боғланишлиги йўқолади: RSA асимметрик криптотизимда калитлар сонининг фойдаланувчилар сонига боғликлиги чизикли кўринишга эга (N фойдаланувчиси бўлган тизимда $2N$ калит ишлатилади).

Аммо асимметрик криптотизимлар, хусусан, RSA криптотизими, камчиликлардан холи эмас:

- hozirgacha асимметрик алгоритмларда ишлатилувчи функцияларнинг қайтарилмаслигининг математик исботи йўқ;

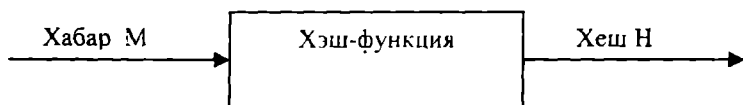
- асимметрик шифрлаш симметрик шифрлашга нисбаган секин амалга оширилади, чунки шифрлашда ва расшифровка қилишда катта ресурс талаб этиладиган амаллар ишлатилади (хусусан, RSAда катта сонни катта сонли даражага ошириш талаб этилади). Шу сабабли асимметрик алгоритмларни аппарат амалга оширилиши, симметрик алгоритмлардагига нисбатан анчагина мураккаб;

- очик калитларни алмаштириб қўйилишидан химоялаш зарур. Фараз қилайлик « A » абонентнинг компьютерида « B » абонентнинг очик калити « K_B » сақланади. « m » нияти бузук одам « A » абонентда сақланаётган очик калитлардан фойдалана олади. У ўзининг жуфт (очик ва махфий) « K_n » ва « k_n » калитларини яратади ва « A » абонентда сақланаётган « B » абонентнинг « K_B » калитини ўзининг очик « K_n » калити билан алмаштиради. « A » абонент қандайдир ахборотни « B » абонентга жўнатиш учун уни « K_n » калитда (бу « K_B » калит деб ўйлаган ҳолда) шифрлайди. Нагижала, бу хабарни « B » абонент ўқий олмайди, « m » абонент осонгина расшифровка қилади ва ўқийди. Очик калитларни алмаштиришни олдини олишда калитларни сертификациялашдан фойдаланилади.

4.5. Хэшлаш функцияси

Хэшлаш функцияси (хэш-функцияси) шундай ўзгартиришки, кириш йўлига узунлиги ўзгарувчан хабар M берилганида чиқиш йўлида белгиланган узунликдаги катор $h(M)$ ҳосил бўлади. Бошқача айтганда, хеш-функция $h(\cdot)$ аргумент сифатида узунлиги

ихтиёрий хабар (хужжат) M ни қабул қилади ва белгиланган узунликдаги хеш-қиймат (хеш) $H=h(M)$ ни қайтаради (4.14-расм).



4.14-расм. Хэшни шакллантириш схемаси.

Хэш-қиймат $h(M)$ – хабар M нинг *дайджести*, яъни ихтиёрий узунликдаги асосий хабар M нинг хичлантирилган иккилик ифодаси. Хэшлаш функцияси ўлчами мегабайт ва ундан катта бўлган имзо чекилувчи хужжат M ни 128 ва ундан катта битга (хусусан, 128 ёки 256 бит) зичлаштиришга имкон беради. Таъкидлаш лозимки, хеш-функция $h(M)$ қийматининг хужжат M га боғлиқлиги мураккаб ва хужжат M нинг ўзини тиклашга имкон бермайди.

Хэшлаш функцияси қуйидаги хусусиятларга эга бўлиши лозим:

1. Хэш-функция ихтиёрий ўлчамли аргументга қўлланиши мумкин.

2. Хэш-функция чиқиш йўлининг қиймати белгиланган ўлчамга эга.

3. Хэш-функция $h(x)$ ни ихтиёрий x' учун етарлича осон ҳисобланади. Хэш-функцияни ҳисоблаш тезлиги шундай бўлиши керакки, хэш-функция ишлатилганида электрон рақамли имзони тузиш ва текшириш тезлиги хабарнинг ўзидан фойдаланилганига қараганда анчагина катта бўлсин.

4. Хэш-функция матн M даги орасига қўйишлар (вставка), чиқариб ташлашлар (выбросы), жойини ўзгартиришлар ва x каби ўзгаришларга сезгир бўлиши лозим.

5. Хэш-функция қайтарилмаслик хусусиятига эга бўлиши лозим.

6. Иккита турли хужжатлар (уларнинг узунлигига боғлиқ бўлмаган ҳолда) хэш-функциялари қийматларининг мос келиши эҳтимоллиги жуда кичкина бўлиши шарт, яъни ҳисоблаш нуктаи назаридан $h(x')=h(x)$ бўладиган $x' \neq x$ ни топиш мумкин эмас.

Иккита турли хабарни битга тугунчага (свертка) зичлаштириш назарий жихатдан мумкин. Бу коллизия ёки тўқнашиш деб аталади. Шунинг учун хэшлаш функциясининг бардошлигини таъминлаш максимида тўқнашишларга йўл қўймасликни кўзда тутиш лозим. Тўқнашишларга бутунлай йўл қўймаслик мумкин эмас, чунки умумий ҳолда мумкин бўлган хабарлар сони хэшлаш функциялари чиқиш йўллари кийматларининг мумкин бўлган сонидан ортик. Аммо, тўқнашишлар эҳтимоллиги паст бўлиши лозим.

5-хусусият $h(.)$ бир томонлама эканлигини билдирса, 6 хусусият бир бир хил тугунчани берувчи иккита ахборотни топиш мумкин эмаслигини кафолатлайди. Бу сохталаштиришни олдини олади.

Шундай қилиб, хэшлаш функциясидан хабар ўзгаришини пайкашда фойдаланиш мумкин, яъни у *криптографик назорат йигиндисини* (ўзгаришларни пайкаш коди ёки хабарни аутентификациялаш коди деб ҳам юритилади) шакллантиришга хизмат қилиши мумкин. Бу сифатда хэш-функция хабарнинг яхлитлигини назоратлашда, электрон рақамли имзони шакллантиришда ва текширишда ишлатилади.

Хэш-функция фойдаланувчини аутентификациялашда ҳам кенг қўлланилади. Ахборот хавфсизлигининг қатор технологияларида шифрлашнинг ўзига хос усули *бир томонлама хэш-функция ёрдамида шифрлаш* ишлагилади. Бу шифрлашнинг ўзига хослиги шундан иборатки, у моҳияти бўйича, бир томонламадир, яъни тескари муолажа – қабул қилувчи томонда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) хэш-функция асосидаги бир томонлама шифрлаш муолажасидан фойдаланади.

Энг оммабоп хэш-функциялар – MD2, MD4, MD5 ва SHA.

MD2, MD4 ва MD5 – P.Райвест томонидан ишлаб чиқилган ахборот дайджестини ҳисобловчи алгоритмлар. Уларнинг ҳар бири 128 битли хэш-кодни тузади. MD2 алгоритми энг секин ишласа, MD4 алгоритми тез ишлайди. MD5 алгоритми MD4 алгоритмининг модификацияси бўлиб, Натижада, хавфсизликнинг оширилиши эвазига тезликдан ютказилган. SHA(Secure Hash Algorithm) 160 битли хэш-кодни тузувчи ахборот дайджестини ҳисобловчи алгоритм. Бу алгоритм MD4 ва MD5 алгоритмларига нисбаган ишончлироқ.

4.6. Электрон рақамли имзо

Электрон ҳужжатларни тармок орқали алмашишда уларни ишлаш ва саклаш харажатлари камаяди, кидириш тезлашади. Аммо, электрон ҳужжат муаллифини ва ҳужжатнинг ўзини аутентификациялаш, яъни муаллифнинг ҳақиқийлигини ва олинган электрон ҳужжатда ўзгаришларнинг йўқлигини аниқлаш муаммоси пайдо бўлади.

Электрон ҳужжатларни аутентификациялашдан мақсад уларни мумкин бўлган жинояткорона ҳаракатлардан химоялашдир. Бундай ҳаракатларга қуйидагилар киради:

– *фаол ушлаб қолиш* – тармокқа уланган бузғунчи ҳужжатларни (файлларни) ушлаб қолади ва ўзгартиради.

– *маскарад* – абонент *C* ҳужжатларни абонент *B* га абонент *A* номидан юборади;

– *рenegатлик* – абонент *A* абонент *B* га хабар юборган бўлсада, юбормаганман дейди;

– *алмаштириш* – абонент *B* ҳужжатни ўзгартиради, ёки янгисини шакллантиради ва уни абонент *A* дан олганман дейди;

– *такрорлаш* – абонент *A* абонент *B* га юборган ҳужжатни абонент *C* такрорлайди.

Жинояткорона ҳаракатларнинг бу турлари ўз фаолиятида компьютер ахборот технологияларидан фойдаланувчи банк ва тижорат тузилмаларига, давлат корхона ва ташкилотларига хусусий шахсларга анча-мунча зарар етказиши мумкин.

Электрон рақамли имзо методологияси хабар яхлитлигини ва хабар муаллифининг ҳақиқийлигини текшириш муаммосини самарали ҳал этишга имкон беради.

Электрон рақамли имзо телекоммуникация каналлари орқали узатишувчи матнларни аутентификациялаш учун ишлатилади. Рақамли имзо ишлаши бўйича оддий қўлёзма имзога ўхшаш бўлиб, қуйидаги афзалликларга эга:

– имзо чекилган матн имзо қўйган шахсга тегишли эканлигини тасдиқлайди;

– бу шахсга имзо чекилган матнга боғлиқ мажбуриятларидан тониш имкониятини бермайди;

– имзо чекилган матн яхлитлигини кафолатлайди.

Электрон рақамли имзо-имзо чекилувчи матн билан бирга узатилувчи қўшимча рақамли хабарнинг нисбатан катта бўлмаган сонидир.

Электрон рақамли имзо асимметрик шифрларнинг қайтарувчанлигига ҳамда хабар таркиби, имзонинг ўзи ва калитлар жуфтнинг ўзаро боғлиқлигига асосланади. Бу элементларнинг ҳатто бирининг ўзгариши рақамли имзонинг ҳақиқийлигини тасдиқлашга имкон бермайди. Электрон рақамли имзо шифрлашнинг асимметрик алгоритмлари ва хеш-функциялари ёрдамида амалга оширилади.

Электрон рақамли имзо тизимининг қўлланишида бир-бирига имзо чекилган электрон ҳужжатларни жўнатувчи абонент тармоғининг мавжудлиги фараз қилинади. Ҳар бир абонент учун жуфт - махфий ва очик калит генерацияланади. Махфий калит абонентда сир сақланади ва ундан абонент электрон рақамли имзони шакллантиришда фойдаланади.

Очик калит бошқа барча фойдаланувчиларга маълум бўлиб, ундан имзо чекилган электрон ҳужжатни қабул қилувчи электрон рақамли имзони текширишда фойдаланади.

Электрон рақамли имзо тизими иккита асосий муолажани амалга оширади:

- рақамли имзони шакллантириш муолажаси;
- рақамли имзони текшириш муолажаси.

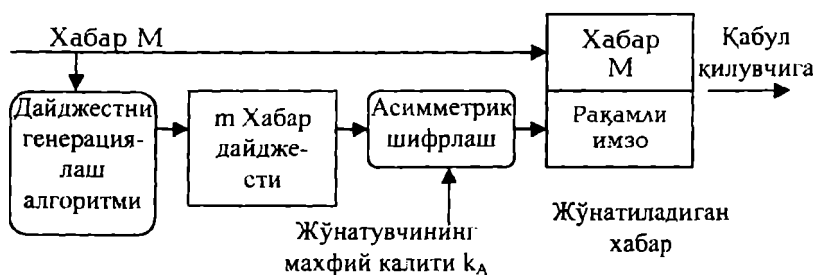
Имзони шакллантириш муолажасида хабар жўнатувчисининг махфий калити ишлатилса, имзони текшириш муолажасида жўнатувчининг очик калитидан фойдаланилади.

Рақамли имзони шакллантириш муолажаси.

Ушбу муолажани гайёрлаш босқичида хабар жўнатувчи абонент A иккита калитни генерациялайди: махфий калит k_A ва очик калит K_A . Очик калит K_A унинг жуфти бўлган махфий калит k_A дан ҳисоблаш орқали олинади. Очик калит K_A тармокнинг бошқа абонентларига имзони текширишда фойдаланиш учун тарқатилади.

Рақамли имзони шакллантириш учун жўнатувчи A аввал имзо чекилувчи матн M нинг хэш функцияси $L(M)$ кийматини ҳисоблайди (4.15-расм).

Хэш-функция имзо чекилувчи дастлабки матн M ни дайджест m га зичлаштиришга хизмат қилади. Дайджест M -бутун матн M ни характерловчи битларнинг белгиланган катта бўлмаган сонидан иборат нисбатан қиска сондир. Сўнгра жўнатувчи A ўзининг махфий калити k_A билан дайджест m ни шифрлайди. Натижада, олинган сонлар жуфти берилган M матн учун рақамли имзо ҳисобланади. Хабар M рақамли имзо билан биргаликда қабул қилувчининг манзилига юборилади.

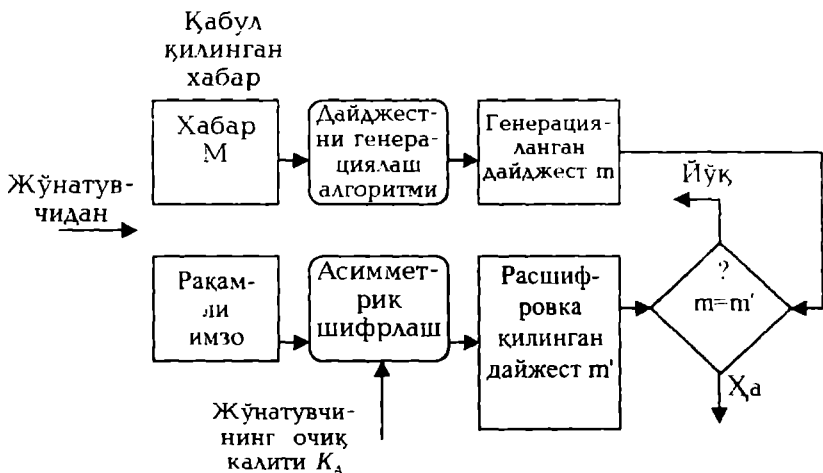


4.15-расм. Электрон рақамли имзони шакллантириш схемаси.

Рақамли имзони текшириш муолажаси.

Тармоқ абонентлари олинган хабар M нинг рақамли имзосини ушбу хабарни жўнатувчининг очик калити K_A ёрдамида текширишлари мумкин (4.16-расм).

Электрон рақамли имзони текширишда хабар M ни қабул қилувчи B қабул қилинган дайджестни жўнатувчининг очик калити K_A ёрдамида расшифровка қилади. Ундан ташқари, қабул қилувчини ўзи хэш-функция $h(M)$ ёрдамида қабул қилинган хабар M нинг дайджести m ни ҳисоблайди ва уни расшифровка қилингани билан таққослайди. Агар иккала дайджест m ва m мос келса рақамли имзо ҳақиқий ҳисобланади. Акс ҳолда имзо қалбақлаштирилган ёки ахборот мазмуни ўзгартирилган бўлади.



4.16-расм. Электрон рақамли имзони текшириш схемаси.

Электрон рақамли имзо тизимининг принципиал жиҳати-фойдаланувчининг электрон рақамли имзосини унинг имзо чекишдаги махфий калитини билмасдан қалбакилаштиришнинг мумкин эмаслигидир. Шунинг учун имзо чекишдаги махфий калитни руҳсатсиз фойдаланишдан ҳимоялаш зарур. Электрон рақамли имзонинг махфий калитини, симметрик шифрлаш калитига ўхшаб, шахсий калит элитувчисида, ҳимояланган ҳолда сақлаш тавфсия этилади.

Электрон рақамли имзо-имзо чекилувчи ҳужжат ва махфий калит орқали аниқланувчи ноёб сондир. Имзо чекилувчи ҳужжат сифатида ҳар қандай файл ишлатилиши мумкин. Имзо чекилган файл имзо чекилмаганига бир ёки бир нечта электрон имзо кўшилиши орқали яратилади.

Имзо чекилувчи файлга жойлаштирилувчи электрон рақамли имзо имзо чекилган ҳужжат муаллифини идентификацияловчи қўшимча ахборотга эга. Бу ахборот ҳужжатга электрон рақамли имзо ҳисобланмасидан олдин кўшилади. Ҳар бир имзо қуйидаги ахборотни ўз ичига олади:

- имзо чекилган сана;
- ушбу имзо калити таъсирининг тугаши муддати;

- файлга имзо чекувчи шахс хусусидаги ахборот (Ф.И.Ш., мансаби, иш жойи);
- имзо чекувчининг индентификатори (очик калит номи);
- ракамли имзонинг ўзи.

Асимметрик шифрлашга ўхшаш, электрон ракамли имзони текшириш учун ишлатиладиган очик калитнинг алмаштирилишига йўл қўймаслик лозим. Фараз қилайлик, нияти бузук одам «*n*» абонент «*B*» компьютерида сакланаётган очик калитлардан, хусусан, абонент *A* нинг очик калити K_A дан фойдалана олади. Унда у қуйидаги ҳаракатларини амалга ошириши мумкин:

- очик калит K_A сакланаётган файлдан абонент *A* хусусидаги индентификация ахборотини ўқиши;
- ичига абонент *A* хусусидаги индентификация ахборотини ёзган ҳолда шахсий жуфт калитлари k_n ва K_n ни генерациялаши;
- абонент *B*да сакланаётган очик калит K_A ни ўзининг очик калити K_n билан алмаштириши.

Сўнгра нияти бузук одам *n* абонент *B* га ҳужжатларни ўзининг махфий калити k_n ёрдамида имзо чекиб жўнагиши мумкин. Бу ҳужжатлар имзосини текширишда абонент *B* абонент *A* имзо чеккан ҳужжатларни ва уларнинг электрон ракамли имзоларини тўғри ва ҳеч ким томонидан модификацияланмаган деб ҳисоблайди. Абонент *A* билан муносабатларини бевосита ойдинлаштирилишигача *B* абонентда олинган ҳужжатларнинг ҳақиқийлигига шубҳа туғилмайди.

Электрон ракамли имзонинг қатор алгоритмлари ишлаб чиқилган. 1977 йилда АҚШ да яратилган RSA тизими биринчи ва дунёда машҳур электрон ракамли имзо тизими ҳисобланади ва юкорида келтирилган принципларни амалга оширади. Аммо ракамли имзо алгоритми RSA жиддий камчиликка эга. У нияти бузук одамга махфий калитни билмасдан, хэшлаш натижасини имзо чекиб бўлинган ҳужжатларнинг хэшлаш натижаларини кўпайтириш орқали ҳисоблаш мумкин бўлган ҳужжатлар имзосини шакллантиришга имкон беради.

Ишончлилигининг юкорилиги ва шахсий компьютерларда амалга оширилишининг қулайлиги билан ажралиб турувчи ракамли имзо алгоритми 1984 йилда Эль Гамал томонидан ишлаб чиқилди. Эль Гамалнинг ракамли имзо алгоритми (EGSA) RSA ракамли имзо алгоритмидаги камчиликлардан холи бўлиб, АҚШ нинг стандарт-

лар ва технологияларнинг Миллий университети томонидан рақамли имзонинг миллий стандартига асос қоби қабул қилинди.

4.7. Криптографик қалитларни бошқариш

Ҳар қандай криптографик тизим криптографик қалитлардан фойдаланишга асосланган. Қалит ахбороти деганда ахборот тармоқлари ва тизимларида ишлатилувчи барча қалитлар мажмуи тушунилади. Агар қалит ахборотларининг старлича ишончли бошқарилиши таъминланмаса, нияти бузук одам унга эга бўлиб олиб тармоқ ва тизимдаги барча ахборотдан хоҳлаганича фойдаланиши мумкин. Қалитларни бошқариш қалитларни генерациялаш, сақлаш ва тақсимлаш қоби вазифаларни бажаради. Қалитларни тақсимлаш қалитларни бошқариш жараёнидаги энг масъулиятли жараён ҳисобланади.

Симметрик криптогафизимдан фойдаланилганда ахборот алмашинувида иштирок этувчи иккала томон аввал махфий сессия қалити, яъни алмашинув жараёнида узатиладиган барча хабарларни шифрлаш қалити бўйича қелишишлари лозим. Бу қалитни бошқа барча билмаслиги ва уни вақти-вақти билан жўнатувчи ва қабул қилувчида бир вақтда алмаштириб туриш лозим. Сессия қалити бўйича қелишиш жараёни қалитларни алмаштириш ёки тақсимлаш деб ҳам юритилади.

Асимметрик криптогафизимда иккита қалит-очик ва ёпик (махфий) қалит ишлатилади. Очик қалитни ошкор этиш мумкин, ёпик қалитни яшириш лозим. Хабар алмашинувида фақат очик қалитни унинг ҳақиқийлигини таъминлаган ҳолда жўнатиш лозим.

Қалитларни тақсимлашга қуйидаги талаблар қўйилади:

- тақсимлашнинг оперативлиги ва аниқлиги;
- тақсимланувчи қалитларнинг конфиденциаллиги ва яхлитлиги.

Компьютер тармоқларидан фойдаланувчилар ўртасида қалитларни тақсимлашнинг қуйидаги асосий усулларидан фойдаланилади.

1. Калитларни тақсимловчи битга ёки бир нечта маркалардан фойдаланиш.

2. Тармоқ фойдаланувчилари ўртасида калитларни тўғридан-тўғри алмашиш.

Биринчи усулнинг муаммоси шундаки, калитларни тақсимлаш марказига кимга, қайси калитлар тақсимланганлиги маълум. Бу эса тармоқ бўйича узатилаётган барча хабарларни ўқишга имкон беради. Бўлиши мумкин бўлган суиистеъмоллар тармоқ хавфсизлигининг жиддий бузилишига олиб келиши мумкин.

Иккинчи усулдаги муаммо – тармоқ субъектларининг ҳақиқий эканлигига ишонч ҳосил қилишдир.

Калитларни тақсимлаш масаласи қуйидагиларни таъминловчи калитларни тақсимлаш протоколини қуришга келтирилади:

- сеанс қатнашчиларининг ҳақиқийлигига иккала томоннинг тасдиғи;

- сеанс ҳақиқийлигининг тасдиғи;

- калитлар алмашинувида хабарларнинг минимал сонидан фойдаланиш.

Биринчи усулга мисол тариқасида Kerberos деб аталувчи калитларни аутентификациялаш ва тақсимлаш тизимини кўрсатиш мумкин.

Иккинчи усулга-тармоқ фойдаланувчилари ўртасида калитларни тўғридан-тўғри алмашишга батафсил тўхталамиз.

Симметрик калитли криптогизимдан фойдаланилганда криптографик химояланган ахборот алмашинувини истаган иккала фойдаланувчи умумий махфий калитга эга бўлишлари лозим. Бу фойдаланувчилар умумий калитни алоқа канали бўйича хавфсиз алмашишлари лозим. Агар фойдаланувчилар калитни тез-тез ўзгартириб турсалар калитни етказиш жиддий муаммога айланади.

Бу муаммони ечиш учун қуйидаги иккита асосий усул қўлланилади:

1. Симметрик криптогизимнинг махфий калитини химоялаш учун очик калитли асимметрик криптогизимдан фойдаланиш

2. Диффи-Хеллманнинг калитларни очик тақсимлаш гизимидан фойдаланиш.

Биринчи усул симметрик ва асимметрик калитли комбинацияланган криптоанизим доирасида амалга оширилади. Бундай ёндашишда симметрик криптоанизим дастлабки очик матнни шифрлаш ва узатишда ишлатилса, очик калитли асимметрик криптоанизим фақат симметрик криптоанизимнинг махфий калитини шифрлаш, узатиш ва кейинги расшифровка килишда ишлатилади. Шифрлашнинг бундай комбинацияланган (гибрид) усули очик калитли асимметрик криптоанизимнинг юкори махфийлиги билан махфий калитли симметрик криптоанизимнинг юкори тезкорлигининг уйғун-лашишга олиб келади. Бундай ёндашиш баъзида *электрон рақамли конверт* схемаси деб юритилади.

Фараз килайлик, фойдаланувчи A хабар M ни фойдаланувчи B га химояланган узатиш учун шифрлашнинг комбинацияланган усулидан фойдаланмоқчи. Унда фойдаланувчиларнинг ҳаракатлари куйидагича бўлади.

Фойдаланувчи A нинг ҳаракатлари:

1. Симметрик сеанс махфий калит K_S ни ярагади (масалан, тасодифий тарзда генерациялайди).

2. Хабар M ни симметрик сеанс махфий калит K_S да шифрлайди.

3. Махфий сеанс калит K_S ни фойдаланувчи (хабар қабул килувчи) B нинг очик калити K_B да шифрлайди.

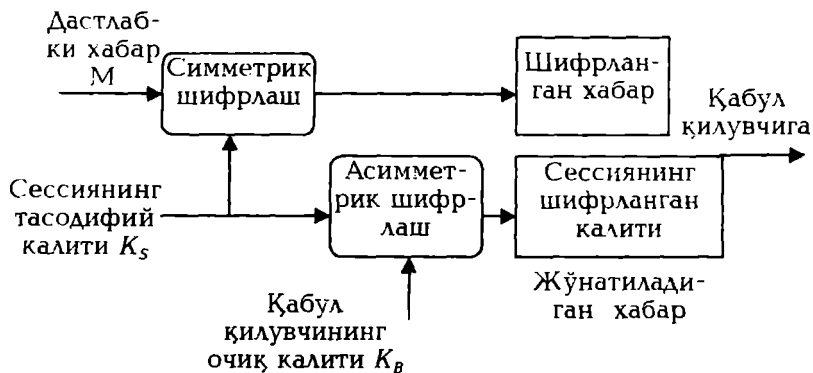
4. Фойдаланувчи B манзилига алоканинг очик канали бўйича шифрланган хабар M ни шифрланган сеанс калити K_S билан биргаликда узатади.

Фойдаланувчи A нинг ҳаракатларини 4.17-расмда келтирилган хабарларни комбинацияланган усул бўйича шифрлаш схемаси орқали тушуниш мумкин.

Фойдаланувчи B нинг ҳаракатлари (электрон рақамли конвертни-шифрланган хабар M ни ва шифрланган сеанс калити K_S ни олганидан сўнгги) куйидагича:

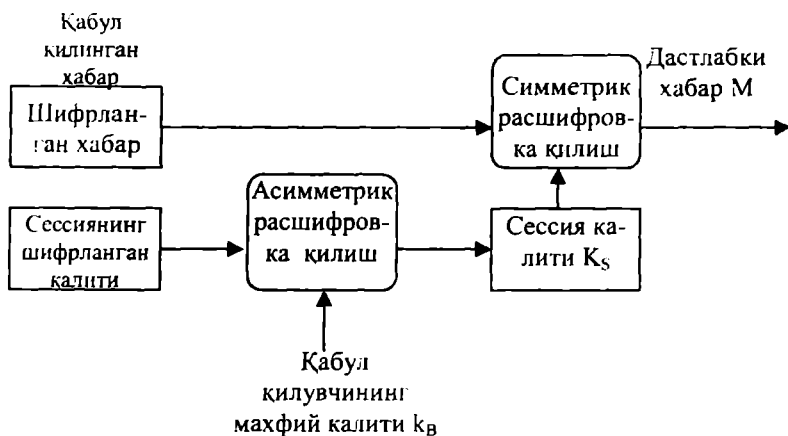
1. Ўзининг махфий калити k_B бўйича сеанс калити K_S ни расшифровка килади.

2. Олинган сеанс калити K_S бўйича олинган хабар M ни



4.17-расм. Комбинацияланган усул бўйича хабарни шифрлаш схемаси.

Фойдланувчи B нинг ҳаракатларини 4.18-расмда келтирилган хабарларни комбинацияланган усул бўйича расшифровка қилиш схемаси орқали тушуниш мумкин.



4.18-расм. Комбинацияланган усул бўйича хабарни расшифровка қилиш схемаси.

Олинган электрон ракамли конвертни фақат қонуний қабул қилувчи-фойдаланувчи B очиши мумкин. Фақат шахсий махфий калит k_B эгаси бўлган фойдаланувчи B махфий сеанс калити K_S ни

тўғри расшифровка қилиш ва сўнгра бу калит ёрдамида олинган хабар M ни расшифровка қилиши ва ўқиши мумкин.

Рақамли конверт усулида симметрик ва асимметрик криптоалгоритмларнинг камчиликлари қуйидагича компенсацияланади:

- симметрик криптоалгоритм калитларини гарқатиш муаммоси баргараф қилинади, чунки хабарни шифрловчи сеанс калити K_2 очик канал бўйича шифрланган кўринишда узагилади, калит K_2 ни расшифровка қилиш учун асимметрик криптоалгоритмдан фойдаланилади;

- бу ҳолда асимметрик шифрлаш тезкорлигининг секинлиги муаммоси пайдо бўлмайди, чунки асимметрик алгоритм бўйича фақат қисқа калит K_2 шифрланади, барча маълумотлар эса тезкор симметрик криптоалгоритм бўйича шифрланади.

Натижада тезкор шифрлаш билан биргаликда калитларнинг қулай тақсимланиши амалга оширилади.

Шифрлашнинг комбинацияланган усулида симметрик ҳам асимметрик криптоалгоритмларнинг криптографик калитларидан фойдаланилади. Равшанки, криптоалгоритмнинг ҳар бир тури учун калитлар узунлигини шундай танлаш лозимки, нияти бузук одамга комбинацияланган криптоалгоритм химоясининг ҳар қандай механизмига ҳужум қилиш бир хил қийинчилик туғдирсин.

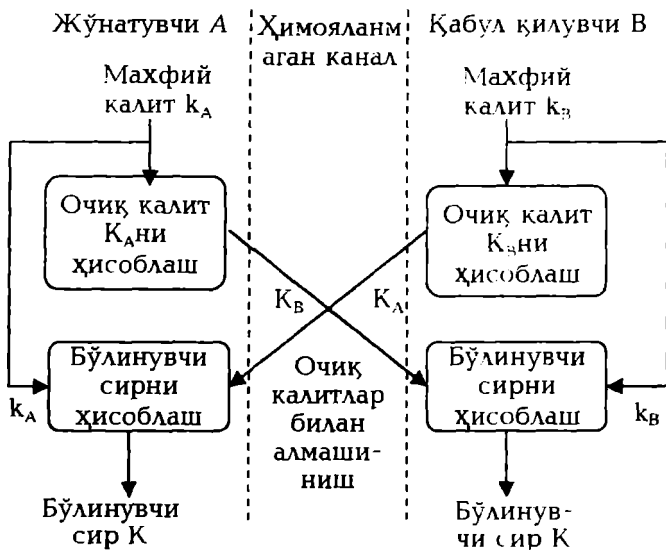
4.1-жадвалда кўп учрайдиган симметрик ва асимметрик криптоалгоритмлар калитларининг узунлиги келтирилган.

4.1-жадвал

Симметрик криптоалгоритм калитлари узунлиги, битлар	Асимметрик криптоалгоритм калитлари узунлиги, битлар
56	384
64	512
80	768
112	1792
128	2304

У. Диффи ва М.Хеллман томонидан кашф этилган калитларни очик тақсимлаш усули фойдаланувчиларга калитларни химояланмаган алоқа каналлари орқали алмашишга имкон беради. Унинг ҳавфсизлиги чегараланган соҳада дискрет логарифмларни ҳисоблашнинг мушкуллигига асосланади.

Диффи-Хеллман усулининг моҳияти қуйидагича (4.19-расм).



4.19-расм. Диффи-Хеллманнинг калитларни очик таксимлаш схемаси.

Ахборот алмашинувида иштирок этувчи фойдаланувчилар А ва В мустақил равишда ўзларининг махфий калитларини k_A ва k_B ни генерациялайдилар (k_A ва k_B калитлар-фойдаланувчилар А ва В лар сир сакловчи тасодикий катга бутун сонлар).

Сўнгра фойдаланувчи А ўзининг махфий калити k_A асосида очик калитни ҳисоблайди:

$$K_A = g^{k_A} \pmod{N}.$$

Бир вақтнинг ўзида фойдаланувчи В ўзининг махфий калити k_B асосида очик калитни ҳисоблайди:

$$K_B = g^{k_B} \pmod{N}.$$

Бу ерда, N ва g – катга бутун оддий сонлар. Арифметик амаллар M нинг модулига келгириш оркали бажарилади. N ва g сонларни сир саклаш шарт эмас. чунки одатда, бу кийматлар тармок ва тизимдан фойдаланувчиларнинг барчаси учун умумий ҳисобланади.

Сўнгра фойдаланувчилар А ва В ўзларининг очик калитларини химояланмаган канал оркали алмашадилар ва умумий сессия махфий калити $K_{ни}$ (бўлинувчи сирни) ҳисоблашда ишлатадилар:

фойдаланувчи А: $K = (K_B)^{k_A} \pmod N = (g^{k_B})^{k_A} \pmod N$,

фойдаланувчи В: $K' = (K_A)^{k_B} \pmod N = (g^{k_A})^{k_B} \pmod N$,

бунда $K = K'$, чунки $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} \pmod N$.

Шундай қилиб, ушбу амаллар натижасида иккала махфий калит k_A ва k_B ларнинг функцияси бўлган умумий сессия махфий калити ҳосил қилинади.

Очик калитлар K_A ва K_B қиймагларини ушлаб қолган нияти бузук одам сессия махфий калити K ни ҳисоблай олмайди, чунки у махфий калитлар k_A ва k_B қийматларини билмайди. Бир томонлама функциянинг ишлатилиши сабабли очик калитни ҳисоблаш амали қайтарилмайдиган амал, яъни абонентнинг очик калити қиймати бўйича унинг махфий калитини ҳисоблаш мумкин эмас.

Диффи-Хеллман усулининг ноёблиги шундан иборатки, абонентлар жуфти тармоқ орқали очик калитларни узатганларида фақат ўзларига маълум махфий сонни олиш имкониятига эга. Сўнгра абонентлар узатилаётган ахборотни маълум текширилган усулни – олинган умумий сессия махфий калитидан фойдаланган ҳолда симметрик шифрлашни ишлатиб химоялашга киришишлари мумкин.

Диффи-Хеллман схемаси маълумотларни ҳар бир сеансда янги калитларда шифрлаш имконини беради. Бу сирларни дискетларда ёки бошқа элтувчиларда сақламасликка имкон беради, чунки бундай сақлаш уларни рақиблар ёки нияти бузук одамлар кўлига тушиб қолиш эҳтимоллигини оширади.

Диффи-Хеллман схемаси *узатилаётган маълумотларнинг конфиденциаллигини ва аутентлигини (аслига тўғрилигини) комплекс химоялаш* усулини ҳам амалга ошириш имконини беради. Алгоритм фойдаланувчига рақамли имзони ва симметрик шифрлашни бажаришда бир хил калитларни шакллантириш ва ишлатиш имконини беради.

Маълумотлар яхлитлигини ва конфиденциаллигини бир вақтда химоялаш учун шифрлаш ва электрон рақамли имзодан комплекс фойдаланиш максадга мувофиқ ҳисобланади. Диффи-Хеллман схемаси ишлашининг оралик натижаларидан узатилаётган маълумотларнинг яхлитлигини ва конфиденциаллигини комплекс химоялаш усулини амалга оширишда фойдаланиш мумкин. Ҳақиқатан, ушбу алгоритмга биноан фойдаланувчилар A ва B аввал ўзларининг махфий калитлари k_A ва k_B ни генерациялайдилар ва очик калитлари K_A

ва K_B ни ҳисоблайдилар. Сўнгра абонентлар A ва B бу оралик на-тижалардан маълумотларни симметрик шифрлашда фойдаланили-ши мумкин бўлган умумий бўлинувчи махфий калити K ни бир вақтда ҳисоблаш учун ишлатади.

Узатилаётган маълумотларнинг конфиденциаллигини ва аутентилигини комплекс химоялаш усули куйидаги схема бўйича ишлайди:

– абонент A рақамли имзонинг стандарт алгоритмидан фойдаланиб, ўзининг махфий калити k_A ёрдамида хабар M га имзо чекади; абонент A ўзининг махфий калити k_A ва абонент B нинг очик калити K_B дан Диффи-Хеллман алгоритми бўйича умумий бўлинувчи махфий калити K ни ҳисоблайди;

– абонент A олинган ўзаро бўлинувчи махфий калитда алмашинув бўйича шериги билан келишилган симметрик шифрлаш алгоритмидан фойдаланган ҳолда хабар M ни шифрлайди;

– абонент B шифрланган хабар M ни олиши билан ўзининг махфий калити k_B ва абонент A нинг очик калити K_A дан Диффи-Хеллман алгоритми бўйича ўзаро бўлинувчи махфий калит K ни ҳисоблайди;

– абонент B олинган хабар M ни калити K да расшифровка қилади;

– абонент B абонент A нинг очик калит K_A ёрдамида расшифровка қилинган хабар M имзосини текширади.

Диффи-Хеллман схемаси асосида тармоқ сатҳида химояланган виртуал тармоқлар VPN курилишида қўлланилувчи криптокалитларни бошқариш протоколлари SKIP (Simple Key Management for Internet Protocols) ва IKE (Internet Key Exchange) ишлайди.

5.1. Асосий тушунчалар ва туркумланиши

Компьютер тизимида рўйхатга олинган ҳар бир субъект (фойдаланувчи ёки фойдаланувчи номидан ҳаракатланувчи жараён) билан уни бир маънода индентификацияловчи ахборот боғлиқ.

Бу ушбу субъектга ном берувчи сон ёки символлар сатри бўлиши мумкин. Бу ахборот субъект *идентификатори* деб юритилади. Агар фойдаланувчи тармоқда рўйхатга олинган идентификаторга эга бўлса у легал (қонуний), акс холда легал бўлмаган (ноқонуний) фойдаланувчи ҳисобланади. Компьютер ресурсларидан фойдаланишдан аввал фойдаланувчи компьютер тизимининг идентификация ва аутентификация жараёнидан ўтиши лозим.

Идентификация (Identification) – фойдаланувчини унинг идентификатори (номи) бўйича аниқлаш жараёни. Бу фойдаланувчи тармоқдан фойдаланишга уринганида биринчи галда бажариладиган функциядир. Фойдаланувчи тизимга унинг сўрови бўйича ўзининг идентификаторини билдиради, тизим эса ўзининг маълумотлар базасида унинг борлигини текширади.

Аутентификация (Authentication) -- маълум килинган фойдаланувчи, жараён ёки курилманинг ҳақиқий эканлигини текшириш муолажаси. Бу текшириш фойдаланувчи (жараён ёки курилма) ҳақиқатан айнан ўзи эканлигига ишонч ҳосил қилишга имкон беради. Аутентификация ўтказишда текширувчи тараф текширилувчи тарафнинг ҳақиқий эканлигига ишонч ҳосил қилиши билан бир қаторда текширилувчи тараф ҳам ахборот алмашинув жараёнида фаол катнашади. Одатда, фойдаланувчи тизимга ўзи хусусидаги ноёб, бошқаларга маълум бўлмаган ахборотни (масалан, парол ёки сертификат) киритиши орқали идентификацияни тасдиқлайди.

Идентификация ва аутентификация субъектларнинг (фойдаланувчиларнинг) ҳақиқий эканлигини аниқлаш ва текширишининг ўзаро боғланган жараёнидир. Муайян фойдаланувчи ёки жараёнинг тизим ресурсларидан фойдаланишига тизимнинг рухсати

айнан шуларга боғлиқ. Субъектни идентификациялаш ва аутентификациялашдан сўнг уни авторизациялаш бошланади.

Авторизация (Authorization) – субъектга тизимда маълум ваколат ва ресурсларни бериш муолажаси, яъни авторизация субъект харакати доирасини ва у фойдаланадиган ресурсларни белгилайди. Агар тизим авторизацияланган шахсни авторизацияланмаган шахсдан ишончли ажрата олмаса бу тизимда ахборотнинг конфиденциаллиги ва яхлитлиги бузилиши мумкин. Аутентификация ва авторизация муолажалари билан фойдаланувчи харакатини маъмурлаш муолажаси узвий боғланган.

Маъмурлаш (Accounting) – фойдаланувчининг тармоқдаги харакатини, шу жумладан, унинг ресурслардан фойдаланишга уринишини кайд этиш. Ушбу ҳисобот ахбороти хавфсизлик нуктаи назаридан тармоқдаги хавфсизлик ходисаларини ошкор қилиш, таҳлиллаш ва уларга мос реакция кўрсатиш учун жуда муҳимдир.

Маълумотларни узатиш каналларини химоялашда *субъектларнинг ўзаро аутентификацияси*, яъни алоқа каналлари орқали боғланадиган субъектлар хақиқийлигининг ўзаро тасдиғи бажарилиши шарт. Хақиқийликнинг тасдиғи одатда, сеанс бошида, абонентларнинг бир-бирига уланиш жараёнида амалга оширилади. «Улаш» атамаси орқали тармоқнинг иккита субъекти ўртасида мантикий боғланиш тушунилади. Ушбу муолажанинг максади – ўлаш қонуний субъект билан амалга оширилганлигига ва барча ахборот мўлжалланган манзилга боришлигига ишончни таъминлашдир.

Ўзининг хақиқийлигининг тасдиқлаш учун субъект тизимга турли асосларни кўрсатиши мумкин. Субъект кўрсатадиган асосларга боғлиқ ҳолда аутентификация жараёнлари қуйидаги категорияларга бўлиниши мумкин:

– *бирор нарсага билмиш асосида*. Мисол сифатида парол, шахсий идентификация коди PIN (Personal Identification Number) ҳамда «сўров жавоб» хилидаги протоколларда намоёнлиги этилувчи махфий ва очик қалитларни кўрсатиш мумкин;

бирор нарсага эғалиги асосида. Одатда, булар магнит карталар, смарт-карталар, сертификатлар ва touch memory қурилмалари;

– *қандайдир дахлсиз характеристикалар асосида*. Ушбу категория ўз таркибига фойдаланувчининг биометрик характеристикаларига (овозлар, кўзининг рангдор пардаси ва тўр

пардаси, бармоқ излари, кафт геометрияси ва х.) асосланган усулларни олади. Бу категорияда криптографик усуллар ва воситалар ишлатилмайди. Бесометрик характеристикалар бинодан ёки қандайдир техникадан фойдаланишни назоратлашда ишлатилади.

Парол – фойдаланувчи ҳамда унинг ахборот алмашинувидаги шериги биладиган нарса. Ўзаро аутентификация учун фойдаланувчи ва унинг шериги ўртасида парол алмашилиши мумкин. Пластик карта ва смарт-карта эгасини аутентификациясида шахсий идентификация номери PIN синалган усул ҳисобланади. PIN – коднинг махфий киймати фақат карта эгасига маълум бўлиши шарт.

Динамик – (бир марталик) парол – бир марта ишлатилганидан сўнг бошқа умуман ишлатилмайдиган парол. Амалда одатда доимий паролга ёки таянч иборога асосланувчи мунтазам ўзгариб турадиган киймат ишлатилади.

«Сўров-жавоб» тизими – тарафларнинг бири ноёб ва оқидиндан билиб бўлмайдиган «сўров» кийматини иккинчи тарафга жўнатиш орқали аутентификацияни бошлаб беради, иккинчи тараф эса сўров ва сир ёрдамида ҳисобланган жавобни жўнатади. Иккала тарафга битта сир маълум бўлгани сабабли, биринчи тараф иккинчи тараф жавобини тўғрилигини текшириши мумкин.

Сертификатлар ва рақамли имзолар – агар аутентификация учун сертификатлар ишлатилса, бу сертификатларда рақамли имзонинг ишлатилиши талаб этилади. Сертификатлар фойдаланувчи ташкилотининг масъул шахси, сертификатлар сервери ёки ташки ишончли ташкилот томонидан берилади. Internet доирасида очик қалит сертификатларини тарқатиш учун очик қалитларни бошқарувчи қатор тижорат инфратузилмалари PKI (Public Key Infrastructure) пайдо бўлди. Фойдаланувчилар турли даража сертификатларини олишлари мумкин.

Аутентификация жарёнларини таъминланувчи хавфсизлик даражаси бўйича ҳам туркумлаш мумкин. Ушбу ёндашишга биноан аутентификация жараёнлари қуйидаги турларга бўлинади:

пароллар ва рақамли сертификатлардан фойдаланувчи аутентификация;

криптографик усуллар ва воситалар асосидаги қатъий аутентификация;

– ноллик билим билан исботлаш хусусиятига эга бўлган аутентификация жараёнлари (протоколлари);

– фойдаланувчиларни биометрик аутентификацияси.

Хавфсизлик нуктан назаридан юкорида келтирилганларнинг хар бири ўзига хос масалаларни ечишга имкон беради. Шу сабабли аутентификация жараёнлари ва протоколлари амалда фаол ишлатилади. Шу билан бир каторда таъкидлаш лозимки, ноллик билим билан исботлаш хусусиятига эга бўлган аутентификацияга кизиқиш амалий характерга нисбатан кўпрок назарий характерга эга. Балким, якин келажакда улардан ахборот алмашинувини химоялашда фаол фойдаланишлари мумкин.

Аутентификация протоколларига бўладиган асосий хужумлар куйидагилар:

– *маскарад* (impersonation). Фойдаланувчи ўзини бошка шахс деб кўрсатишга уриниб, у шахс тарафидан харакатларнинг имкониятларига ва имтиёзларига эга бўлишни мўлжаллайди;

– аутентификация алмашинуви *тарофини алмаштириб қўйиш* (interleaving attack). Нияти бузук одам ушбу хужум мобайнида икки тараф орасидаги аутентификацион алмашинуви жараёнида трафикни модификациялаш ниятида қатнашади. Алмаштириб қўйишнинг куйидаги хили мавжуд: иккита фойдаланувчи ўртасидаги аутенти-фикация муваффақиятли ўтиб, уланиш ўрнатилганидан сўнг бузғунчи фойдаланувчилардан бирини чиқариб ташлаб, унинг номидан ишни давом эттиради;

– *такрорий узатиш* (replay attack). Фойдаланувчиларнинг бири гомонидан аутентификация маълумотлари такроран узатилади;

– *узатишни қайтариш* (reflection attack). Олдинги хужум вариантларидан бири бўлиб, хужум мобайнида нияти бузук одам протоколнинг ушбу сессия доирасида ушлаб қолинган ахборотни оркага қайтаради;

– *мажбурий кечикиш* (forced delay). Нияти бузук одам қандайдир маълумотни ушлаб қолиб, бирор вақтдан сўнг узатади;

– *матн танлаш* (chosen text attack). Нияти бузук одам аутентификация графигини ушлаб қолиб, узок муддатли криптографик калитлар хусусидаги ахборотни олишга уринади.

Юкорида келтирилган ҳужумларни бартараф қилиш учун аутентификация протоколларини куришда қуйидаги усуллардан фойдаланилади:

– «сўров-жавоб», вақт белгилари, тасодифий сонлар, индентификаторлар, рақамли имзолар каби механизмлардан фойдаланиш;

– аутентификация натижасини фойдаланувчиларнинг тизим доирасидаги кейинги ҳаракатларига боғлаш. Бундай ёндашишга мисол тариқасида аутентификация жараёнида фойдаланувчиларнинг кейинги ўзаро алоқаларида ишлатилувчи махфий ссанс калитларини алмашишни кўрсатиш мумкин;

– алоканинг ўрнатилган сеанси доирасида аутентификация муолажасини вақти-вақти билан бажариб туриш ва х.

«Сўров-жавоб» механизми қуйидагича. Агар фойдаланувчи A фойдаланувчи B дан оладиган хабари ёлғон эмаслигига ишонч ҳосил қилишни истаса, у фойдаланувчи B учун юборадиган хабарга олдиндан билиб бўлмайдиган элемент – X сўровини (масалан, қандайдир тасодифий сонни) қўшади. Фойдаланувчи B жавоб беришда бу амал устида маълум амални (масалан, қандайдир $f(X)$ функцияни ҳисоблаш) бажариши лозим. Буни олдиндан бажариб бўлмайди, чунки сўровда қандай тасодифий сон X келиши фойдаланувчи B га маълум эмас. Фойдаланувчи B ҳаракати натижасини олган фойдаланувчи A фойдаланувчи B нинг хақиқий эканлигига ишонч ҳосил қилиши мумкин. Ушбу усулнинг камчилиги – сўров ва жавоб ўртасидаги қонуниятни аниқлаш мумкинлиги.

Вақтни белгилаш механизми ҳар бир хабар учун вақтни қайдлашни кўзда тутати. Бунда тармоқнинг ҳар бир фойдаланувчиси келган хабарнинг қанчалик эскирганини аниқлаши ва уни қабул қилмаслик қарорига келиши мумкин, чунки у ёлғон бўлиши мумкин. Вақтни белгилашдан фойдаланишда сеанснинг хақиқий эканлигини тасдиқлаш учун *кечкикишнинг жоиз вақт оралиғи* муаммоси пайдо бўлади. Чунки, «вақт тамғаси»ли хабар, умуман, бир лаҳзада узатилиши мумкин эмас. Ундан ташқари, қабул қилувчи ва жўнатувчининг соатлари мутлақо синхронланган бўлиши мумкин эмас.

Аутификация протоколларини таккослашда ва танлашда куйидаги характеристикаларни ҳисобга олиш зарур:

– *ўзаро аутентификациянинг мавжудлиги*. Ушбу хусусият аутентификацион алмашув тарафлари ўртасида иккиёклама аутентификациянинг зарурлигини акс эттиради;

– *ҳисоблаш самардорлиги*. Протоколни бажаришда зарур бўлган амаллар сони;

– *коммуникацион самардорлик*. Ушбу хусусият аутентификацияни бажариш учун зарур бўлган хабар сони ва узунлигини акс эттиради;

– *учинчи тарафнинг мавжудлиги*. Учинчи тарафга мисол тариқасида симметрик калитларни тақсимловчи ишончли серверни ёки очик калитларни тақсимлаш учун сертификатлар дарахтини амалга оширувчи серверни кўрсатиш мумкин;

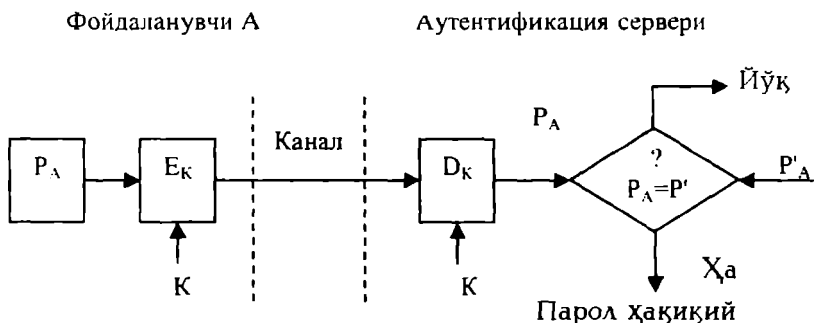
– *хавфсизлик кафолати асоси*. Мисол сифатида ноллик билим билан исботлаш хусусиятига эга бўлган протоколларни кўрсатиш мумкин;

– *сириш сақлаш*. Жиддий калитли ахборотни сақлаш усули кўзда тутилади.

5.2. Пароллар асосида аутентификациялаш

Аутентификациянинг кенг тарқалган схемаларидан бири *оддий аутентификациялаш* бўлиб, у анъанавий кўп мартали паролларни ишлатишига асосланган. Тармоқдаги фойдаланувчини оддий аутентификациялаш муолажасини куйидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган фойдаланувчи компьютер клавиатурасида ўзининг идентификатори ва паролни тиради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аутентификация серверида сақланаётган фойдаланувчи идентификатори бўйича маълумотлар базасидан мос ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан такқосланади. Агар улар мос келса, аутентификация муваффақиятли ўтган ҳисобланади ва фойдаланувчи тегад (конуний) мақомини ва авторизация гизими орқали унинг мақоми учун аниқланган ҳуқуқларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади.

Паролдан фойдаланган холда оддий аутентификациялаш схемаси 5.1-расмда келтирилган.



5.1-расм. Паролдан фойдаланган холда оддий аутентификациялаш.

Равшанки, фойдаланувчининг паролни шифрлашдан узатиш орқали аутентификациялаш варианты хавфсизликнинг ҳатто минимал даражасини кафолатламайди. Паролни химоялаш учун уни химояланмаган канал орқали узатишдан олдин шифрлаш зарур. Бунинг учун схемага шифрлаш E_K ва расшифровка қилиш D_K воситалари киритилган. Бу воситалар бўлинувчи махфий калит K орқали бошқарилади. Фойдаланувчининг ҳақиқийлигини текшириш фойдаланувчи юборган парол P_A билан аутентификация серверида сақланувчи дастлабки қиймат P'_A ни таққослашга асосланган. Агар P_A ва P'_A қийматлар мос келса, парол P_A ҳақиқий, фойдаланувчи A эса қонуний ҳисобланади.

Оддий аутентификацияни ташкил этиш схемалари нафақат паролларни узатиш, балки уларни сақлаш ва текшириш гуруҳлари билан ажралиб туради. Энг кенг тарқалган усул – фойдаланувчилар паролни гизимли файлларда, очик холда сақлаш усулидир. Бунда файлларга ўқиш ва ёзишдан химоялаш атрибутлари ўрнатилади (масалан, операцион тизимдан фойдаланишни назоратлаш рўйхатидаги мос имтиёزلарни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида сақланаётган ёзув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функ-

циялар каби криптографик механизмлар ишлатилмайди. Ушбу усулнинг камчилиги – нияти бузук одамнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан, парол файлларидан фойдаланиш имкониятидир.

Хавфсизлик нуқтаи назаридан паролларни бир томонлама функциялардан фойдаланиб узатиш ва саклаш қулай ҳисобланади. Бу ҳолда фойдаланувчи паролнинг очик шакли урнига унинг бир томонлама функция $h(.)$ дан фойдаланиб олинган тасвирини юбориши шарт. Бу ўзгартириш ғаним томонидан паролни унинг тасвири орқали ошқор қила олмаганлигини кафолатлайди, чунки ғаним ечилмайдиган сонли масалага дуч келади.

Кўп мартали паролларга асосланган оддий аутентификациялаш тизимининг бардошлиги паст, чунки уларда аутентификацияловчи ахборот маъноли сўзларнинг нисбатан катта бўлмаган тўпламидан жамланади. Кўп мартали паролларнинг таъсир муддати ташкилотнинг хавфсизлиги сиёсатида белгиланиши ва бундай паролларни мунгазам равишда алмаштириб туриш лозим. Паролларни шундай танлаш лозимки, улар луғатда бўлмасин ва уларни топиш кийин бўлсин.

Бир мартали паролларга асосланган аутентификациялашда фойдаланишга ҳар бир сўров учун турли пароллар ишлатилади. Бир мартали динамик парол фақат тизимдан бир марта фойдаланишга ярокли. Агар, ҳатто кимдир уни ушлаб қолса ҳам парол фойда бермайди. Одатда, бир мартали паролларга асосланган аутентификациялаш тизими масофадаги фойдаланувчиларни текширишда қўлланилади.

Бир мартали паролларни генерациялаш аппарат ёки дастурий усул оқали амалга оширилиши мумкин. Бир мартали пароллар асосидаги фойдаланишнинг аппарат воситалари ташқаридан тўлов пластик карточкаларига ўхшаш микропроцессор ўрнатилган миниатюр қуриямалар кўринишда амалга оширади. Одатда, калитлар дсб аталувчи бундай карталар клавиатурага ва катта бўлмаган дисплей дарчасига эга.

Фойдаланувчиларни аутентификациялаш учун бир мартали паролларни қўллашнинг қуйидаги усуллари маълум:

1. Ягона вақт тизимига асосланган вақт белгилари механизmidан фойдаланиш.

2. Легал фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар рўйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланиш.

3. Фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланиш.

Биринчи усулни амалга ошириш мисоли сифатида SecurID аутентикациялаш технологиясини кўрсатиш мумкин. Бу технология Security Dynamics компанияси томонидан ишлаб чиқилган бўлиб, қатор компанияларнинг, хусусан Cisco Systems компаниясининг серверларида амалга оширилган.

Вакт синхронизациясидан фойдаланиб аутентификациялаш схемаси тасодифий сонларни вақтнинг маълум оралиғидан сўнг генерациялаш алгоритмига асосланган. Аутентификация схемаси қуйидаги иккита параметрдан фойдаланади:

- ҳар бир фойдаланувчига аталган ва аутентификация серверида ҳамда фойдаланувчининг аппарат қалитида сақланувчи ноёб 64-битли сондан иборат махфий қалит;
- жорий вақт қиймати.

Масофадаги фойдаланувчи тармоқдан фойдаланишга уринганида ундан шахсий идентификация рақами PINни киритиш таклиф этилади. PIN тўртта ўнли рақамдан ва аппарат қалити дисплейида аксланувчи тасодифий соннинг олти рақамидан иборат. Сервер фойдаланувчи томонидан киритилган PIN-коддан фойдаланиб маълумотлар базасидаги фойдаланувчининг махфий қалити ва жорий вақт қиймати асосида тасодифий сонни генерациялаш алгоритмини бажаради. Сўнгра сервер генерацияланган сон билан фойдаланувчи киритган сонни таққослайди. Агар бу сонлар мос келса, сервер фойдаланувчига тизимдан фойдаланишга рухсат беради.

Аутентификациянинг бу схемасидан фойдаланишда аппарат қалит ва сервернинг қатъий вақтий синхронланиши талаб этилади. Чунки аппарат қалит бир неча йил ишлаши ва демак сервер ички соати билан аппарат қалитининг мувофиқлиги аста-секин бузилиши мумкин.

Ушбу муаммони ҳал этишда Security Dynamics компанияси қуйидаги икки усулдан фойдаланади:

- аппарат калити ишлаб чиқиладиганида унинг таймер частотасининг меъеридан четлашиши аниқ ўлчанади. Четлашишнинг бу киймати сервер алгоритми параметри сифатида ҳисобга олинади;

- сервер муайян аппарат калит генерациялаган кодларни кузатади ва зарурият туғилганида ушбу калитга мослашади.

Аутентификациянинг бу схемаси билан яна бир муаммо боғлиқ. Аппарат калит генерациялаган тасодифий сон катта бўлмаган вақт оралиғи мобайнида ҳақиқий парол ҳисобланади. Шу сабабли, умуман, қисқа муддатли вазият содир бўлиши мумкинки, хакер PIN-кодни ушлаб қолиши ва уни тармоқдан фойдаланишга ишлатиши мумкин. Бу вақт синхронизациясига асосланган аутентификация схемасининг энг заиф жойи ҳисобланади.

Бир мартали паролдан фойдаланувчи аутентификациялашни амалга оширувчи яна бир вариант – «сўров-жавоб» схемаси бўйича аутентификациялаш. Фойдаланувчи тармоқдан фойдаланишга уринганида сервер унга тасодифий сон кўринишидаги сўровни узади. Фойдаланувчининг аппарат калити бу тасодифий сонни, масалан, DES алгоритми ва фойдаланувчининг аппарат калити хотирасида ва сервернинг маълумотлар базасида сақланувчи махфий калити ёрдамида расшифровка қилади. Тасодифий сон – сўров шифрланган кўринишда серверга қайтарилади. Сервер ҳам ўз навбатида ўша DES алгоритми ва сервернинг маълумотлар базасидан олинган фойдаланувчининг махфий калити ёрдамида ўзи генерациялаган тасодифий сонни шифрлайди. Сўнгра сервер шифрлаш натижасини аппарат калитидан келган сон билан таққослайди. Бу сонлар мос келганида фойдаланувчи тармоқдан фойдаланишга рухсат олади. Таъкидлаш лозимки, «сўров-жавоб» аутентификациялаш схемаси ишлатишда вақт синхронизациясидан фойдаланувчи аутентификация схемасига караганда мураккаброк.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг иккинчи усули фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар рўйхатидан ва уларнинг ишончли синхронлаш механизmidан фойдаланишга асосланган. Бир мартали паролларнинг бўлинувчи рўйхати махфий пароллар кетма-кетлиги ёки тўплами бўлиб, ҳар бир парол фақат бир марта ишлатилади. Ушбу рўйхат аутентификацион алмашинув тарафлар ўртасида олдиндан тақсимланиши шарт. Ушбу усулнинг бир вариантыга биноан сўров-жавоб жадвали ишлатилади. Бу жадвалда ау-

тентификацилаш учун тарафлар томонидан ишлатилувчи сўровлар ва жавоблар мавжуд бўлиб, ҳар бир жуфт факат бир марта ишлатилиши шарт.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг учинчи усули фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки кийматли псевдотасодифий сонлар генераторидан фойдаланишга асосланган. Бу усулни амалга оширишнинг куйидаги вариантлари мавжуд:

- *ўзгартирилувчи бир мартали пароллар кетма-кетлиги.* Навбатдаги аутентификациялаш сессиясида фойдаланувчи айнан шу сессия учун олдинги сессия паролдан олинган махфий калитда шифрланган паролни яратади ва узатади;

- *бир томонлама функцияга асосланган пароллар кетма-кетлиги.* Ушбу усулнинг моҳиятини бир томонлама функциянинг кетма-кет ишлатилиши (Лампартнинг машҳур схемаси) ташкил этади. Хавфсизлик нуқтаи назаридан бу усул кетма-кет ўзгартирилувчи пароллар усулига нисбатан афзал ҳисобланади.

Кенг тарқалган бир мартали паролдан фойдаланишга асосланган аутентификациялаш протоколларидан бири Internet да стандартлаштирилган S/Key (RFC1760) протоколдир. Ушбу протокол масофадаги фойдаланувчиларнинг ҳақиқийлигини текширишни талаб этувчи кўпгина тизимларда, хусусан, Cisco компаниясининг TACACS+ тизимида амалга оширилган.

5.3. Сертификатлар асосида аутентификациялаш

Тармоқдан фойдаланувчилар сони миллионлаб ўлчанганида фойдаланувчилар паролларининг гайинланиши ва сақланиши билан боғлиқ фойдаланувчиларни дастлабки рўйхатга олиш муолажаси жуда катта ва амалга оширилиши кийин бўлади. Бундай шароитда рақамли сертификатлар асосидаги аутентификациялаш пароллар қўлланишига рационал альтернатива ҳисобланади.

Рақамли сертификатлар ишлатилганида компьютер тармоғи фойдаланувчилар хусусидаги ҳеч қандай ахборотни сақламайди. Бундай ахборотни фойдаланувчиларнинг ўзи сўров-сертификатларида тақдим этадилар. Бунда махфий ахборотни, хусусан махфий калитларни сақлаш вазифаси фойдаланувчиларнинг ўзига юкланади.

Фойдаланувчи шахсини тасдиқловчи рақамли сертификатлар фойдаланувчилар сўрови бўйича махсус ваколатли ташкилот-сертификация маркази СА (Certificate Authority) томонидан, маълум шартлар бажарилганида берилади. Таъкидлаш лозимки, сертификат олиш муолажасининг ўзи ҳам фойдаланувчининг хақиқийлигини текшириш (яъни, аутентификациялаш) босқичини ўз ичига олади. Бунда текширувчи тараф сертификацияловчи ташкилот (сертификация маркази СА) бўлади.

Сертификат олиш учун мижоз сертификация марказига шахсини тасдиқловчи маълумотни ва очик калитини тақдим этиши лозим. Зарурий маълумотлар рўйхати олинадиган сертификат турига боғлиқ. Сертификацияловчи ташкилот фойдаланувчининг хақиқий-лиги тасдиғини текширганидан сўнг ўзининг рақамли имзосини очик калит ва фойдаланувчи хусусидаги маълумот бўлган файлга жойлаштиради ҳамда ушбу очик калитнинг муайян шахсга тегишли эканлигини тасдиқлаган ҳолда фойдаланувчига сертификат беради.

Сертификат электрон шакл бўлиб, таркибида кўйидаги ахборот бўлади:

- ушбу сертификат эгасининг очик калити;
- сертификат эгаси хусусидаги маълумот, масалан, исми, электрон почта манзили, ишлайдиган ташкилот номи ва ҳ.;
- ушбу сертификатни берган ташкилот номи;
- сертификацияловчи ташкилотнинг электрон имзоси – ушбу ташкилотнинг махфий калити ёрдамида шифрланган сертификациядаги маълумотлар.

Сертификат фойдаланувчини тармок ресурсларига мурожаат этганида аутентификацияловчи восита ҳисобланади. Бунда текширувчи тараф вазифасини корпоратив тармокнинг аутентификация сервери бажаради. Сертификатлар нафақат аутентификациялашда, балки фойдаланишнинг маълум ҳуқуқларини тақдим этишда ишлатилиши мумкин. Бунинг учун сертификатга кўшимча хошиялар киритилиб уларда сертификация эгасининг фойдаланувчиларнинг у ёки бу категориясига мансублиги кўрсатилади.

Очик калитларнинг сертификатлар билан узвий боғлиқлигини алоҳида таъкидлаш лозим. Сертификат нафақат шахсни, балки очик калит мансублигини тасдиқловчи ҳужжатдир. Рақамли сертификат очик калит ва унинг эгаси ўртасидаги мосликни ўрнатади ва

кафолатлайди. Бу очик калитни алмаштириш хавфини бартараф этади.

Агар абонент ахборот алмашинуви бўйича шеригидан сертификат таркибидаги очик калитни олса, у бу сертификатдаги сертификация марказининг рақамли имзосини ушбу сертификация марказининг очик калити ёрдамида текшириши ва очик калит манзили ва бошқа маълумотлари сертификатда кўрсатилган фойдаланувчига тегишли эканлигига ишонч ҳосил қилиши мумкин. Сертификатлардан фойдаланилганда фойдаланувчилар рўйхатини уларнинг пароллари билан корпорация серверларида сақлаш зарурияти йўқолади. Серверда сертификацияловчи ташкилотларнинг номлари ва очик калитларининг бўлиши етарли.

Сертификатларнинг ишлатилиши сертификацияловчи ташкилотларнинг нисбатан камлигига ва уларнинг очик калитларидан кизикқан барча шахслар ва ташкилотлар фойдалана олиши (масалан, журналлардаги нашрлар ёрдамида) тахминига асосланган.

Сертификатлар асосида аутентификациялаш жараёнини амалга оширишда сертификацияловчи ташкилот вазифасини қим бажариши хусусидаги масалани счиш муҳим ҳисобланади. Ходимларни сертификат билан таъминлаш масаласини корхонанинг ўзи ечиши жуда табиий ҳисобланади. Корхона ўзининг ходимларини яхши билади ва улар шахсини тасдиқлаш вазифасини ўзига олиши мумкин. Бу сертификат берилишидаги дастлабки аутентификациялаш муолажасини осонлаштиради. Корхоналар сертификатларни генерациялаш, бериш ва уларга хизмат кўрсатиш жараёнларини автоматлаштиришни таъминловчи мавжуд дастурий маҳсулотлардан фойдаланишлари мумкин. Масалан, Netscape Communications компанияси серверларини корхоналарга шахсий сертификатларини чиқариш учун таклиф этади.

Сертификацияловчи ташкилот вазифасини бажаришда тижорат асосида сертификат бериш бўйича мустақил марказлар ҳам жалб этилиши мумкин. Бундай хизматларни, хусусан, Verisign компаниясининг сертификацияловчи маркази таклиф этади. Бу компаниянинг сертификатлари халқаро стандарт X.509 талабларига жавоб беради. Бу сертификатлар маълумотлар химоясининг қатор маҳсулотларида, жумладан, химояланган канал SSL протоколида ишлатилади.

5.4. Қатъий аутентификациялаш

Криптографик протоколларида амалга оширилувчи қатъий аутентификациялаш ғояси куйидагича. Текширилувчи (исботловчи) тараф қандайдир сирни билишини намойиш этган ҳолда текширувчига ўзининг ҳақиқий эканлигини исботлайди. Масалан, бу сир аутентификацион алмашиш тарафлари ўртасида олдиндан хавфсиз усул билан тақсимланган бўлиши мумкин. Сирни билишлик исботи криптографик усул ва воситалардан фойдаланилган ҳолда сўров ва жавоб кетма-кетлиги ёрдамида амалга оширилади.

Энг муҳими, исботловчи тараф фақат сирни билишлигини намойиш этади, сирни ўзи эса аутентификацион алмашиш мобайнида очилмайди. Бу текширувчи тарафнинг турли сўровларига исботловчи тарафнинг жавоблари ёрдами билан таъминланади. Бунда яқуний сўров фақат фойдаланувчи сирга ва протокол бошланишида ихтиёрий танланган катта сондан иборат бошланғич сўровга боғлиқ бўлади.

Аксарият ҳолларда қатъий аутентификациялашга биноан ҳар бир фойдаланувчи ўзининг махфий калитига эгаллиги аломати бўйича аутентификацияланади. Бошқача айтганда фойдаланувчи алоқа бўйича шеригининг тегишли махфий калитга эгаллигини ва у бу калитни ахборот алмашинуви бўйича ҳақиқий шерик эканлигини исботлашга ишлата олиши мумкинлигини аниқлаш имкониятига эга.

Х.509 стандарти тавсияларига биноан қатъий аутентификациялашнинг куйидаги муолажалари фаркланади:

- бир томонлама аутентификация;
- икки томонлама аутентификация;
- уч томонлама аутентификация.

Бир томонлама аутентификациялаш бир томонга йўналтирилган ахборот алмашинувини кўзда тутади. Аутентификациянинг бу тури куйидагиларга имкон яратади:

ахборот алмашинувчининг фақат бир тарафини ҳақиқийлигини тасдиқлаш;

узатилаётган ахборот яхлитлигининг бузилишини аниқлаш;

- «узатишнинг тақрори» гишидаги хужумни аниқлаш;

– узатилаётган аутентификацион маълумотлардан фақат текширувчи тараф фойдаланишини кафолатлаш.

Икки томонлама аутентификациялашда бир томонлиликка нисбатан исботловчи тарафга текширувчи тарафнинг қўшимча жавоби бўлади. Бу жавоб текширувчи томонни алоқанинг айнан аутентификация маълумотлари мўлжалланган тараф билан ўрнатилаётганига ишонтириши лозим.

Уч томонлама аутентификациялаш таркибида исботловчи тарафдан текширувчи тарафга қўшимча маълумотлар узатиш мавжуд. Бундай ёндашиш аутентификация ўтказишда вақт белгиларидан фойдаланишдан воз кечишга имкон беради.

Таъкидлаш лозимки, ушбу туркумлаш шартлидир. Амалда ишлатилувчи усул ва воситалар тўплами аутентификация жараёнини амалга оширишдаги муайян шарт-шароитларга боғлиқ. Қатъий аутентификациянинг ўтказилиши ишлатиладиган криптографик алгоритмлар ва қатор қўшимча параметрларни тарафлар томонидан сўзсиз мувофиқлаштиришни талаб этади.

Қатъий аутентификациялашнинг муайян вариантларини кўришдан олдин бир мартали параметрларнинг вазифалари ва имкониятларига тўхташ лозим. Бир мартали параметрлар баъзида «onces» – бир мақсадга бир мартадан ортиқ ишлатилмайдиган катталиқ деб аталади.

Ҳозирда ишлатиладиган бир мартали параметрлардан тасодикий сонлар, вақт белгилари ва кетма-кетликларнинг рақамларини кўрсатиш мумкин.

Бир мартали параметрлар узатишнинг такрорланишини, аутентификацион алмашинув тарафларини алмаштириб қўйишни ва очик матни танлаш билан ҳужум қилишни олдини олишга имкон беради. Бир мартали параметрлар ёрдамида узатиладиган хабарларнинг ноёблигини, бир маънолилигини ва вақтий кафолатларини таъминлаш мумкин. Бир мартали параметрларнинг турли хиллари алоҳида ишлатилиши, ёки бир-бирини тўлдириши мумкин.

Бир мартали параметрларнинг қуйидаги ишлатилиш мисолларини кўрсатиш мумкин:

– «сўров-жавоб» принципида қурилган протоколларда ўз вақтидалигини текшириш. Бундай текширишда тасодикий сонлар, соатларни синхронлаш билан вақт белгилари ёки муайян жуфт

(текширувчи, исботловчи) учун кетма-кетликларнинг рақамларидан фойдаланиш мумкин;

– ўз вақтидалигини ёки ноёблик кафолатини таъминлаш. Протоколнинг бир мартали параметрларини бевосита (тасодифий сонни танлаш йўли билан) ёки билвосита (бўлинувчи сирдаги ахборотни таҳлиллаш ёрдамида) назоратлаш орқали амалга оширилади;

– хабарни ёки хабарлар кетма-кетлигини бир маъноли идентификациялаш. Бир оҳангда ўсувчи кетма-кетликнинг бир мартали кийматини (масалан, серия номерлари ёки вақт белгилари кетма-кетлиги) ёки мос узунликдаги тасодифий сонларни тузиш орқали амалга оширилади.

Таъкидлаш лозимки, бир мартали параметрлар криптографик протоколларнинг бошқа вариантларида ҳам (масалан, калит ахборотини тақсимлаш протоколларида) кенг қўлланилади.

Қатъий аутентификациялаш протоколларини қўлланиладиган криптографик алгоритмларига боғлиқ ҳолда қуйидаги гуруҳларга ажратиш мумкин:

– шифрлашнинг симметрик алгоритмлари асосидаги қатъий аутентификациялаш протоколлари;

– бир томонлама калитли хэш-функциялар асосидаги қатъий аутентификациялаш протоколлари;

– шифрлашнинг асимметрик алгоритмлари асосидаги қатъий аутентификациялаш протоколлари;

– электрон рақамли имзо алгоритмлари асосидаги қатъий аутентификациялаш протоколлари.

Симметрик алгоритмларга асосланган қатъий аутентификациялаш. Kerberos протоколи

Симметрик алгоритмлар асосида қурилган аутентификациялашнинг ишлаши учун текширувчи ва исботловчи айни бошидан битта махфий калитга эга бўлишлари зарур. Фойдаланувчилари кўп бўлмаган ёпик тизимлар учун фойдаланувчиларнинг ҳар бир жуфти махфий калитни ўзаро бўлиб олишлари мумкин. Симметрик шифрлаш технологиясини қўлловчи катта тақсимланган тизимларда ишончли сервер катнашувидаги аутентификациялаш протоколларидан фойдаланилади. Бу сервер билан ҳар бир гараф калитни билишнинг иштирокида иштирокида.

Ушбу ёндашиш содда бўлиб туюлсада, аслида бундай аутентификациялаш протоколини ишлаб чиқиш мураккаб ва хавфсизлик нуктаи назаридан шубҳасиз эмас.

Куйида шифрлашнинг симметрик алгоритмларига асосланган. ISO/IEC 9798-2да спецификацияланган аутентификациялаш протоколларининг учта мисоли келтирилган. Бу протоколлар бўлинувчи махфий калитларни олдиндан тақсимланишини кўзда гутади. Аутентификациялашнинг куйидаги вариантларини кўриб чиқамиз.

– вақт белгиларидан фойдаланувчи бир томонлама аутентификациялаш;

– тасодифий сонлардан фойдаланувчи бир томонлама аутентификациялаш;

– икки томонлама аутентификациялаш.

Бу вариантларнинг ҳар бирида фойдаланувчи махфий калитни билишини намоиш қилган ҳолда, ўзининг хақиқийлигини исботлайди, чунки ушбу махфий калит ёрдамида сўровларни расшифровка қилади. Аутентификациялаш жараёнида симметрик шифрлашни қўллашда узатиладиган маълумотларнинг яхлитлигини таъминлаш механизмини расм бўлиб қолган усуллар асосида амалга ошириш ҳам зарур.

Куйидаги белгилашларни киритамиз:

t_A – катнашувчи А генерациялаган тасодифий сон;

t_B – катнашувчи В генерациялаган тасодифий сон;

t_A – катнашувчи А генерациялаган вақт белгиси;

E_K – калит Кда симметрик шифрлаш (калит К олдиндан А ва В ўртасида тақсимланиши шарт).

Вақт белгиларига асосланган бир томонлама аутентификациялаш:

$$A \rightarrow B: E_K(t_A, B) \quad (1)$$

Ушбу хабарни олиб расшифровка қилганидан сўнг катнашувчи В вақт меткаси t_A хақиқий эканлигига ва хабарда кўрсатилган идентификатор ўзиники билан мос келишига ишонч ҳосил қилади. Ушбу хабарни қайгадан узатишни олдини олиш калитни билмасдан туриб вақт меткаси t_A ни ва идентификатор B ни ўзгартириш мумкин эмаслигига асосланади.

Тасодифий сонлардан фойдаланишга асосланган бир томонлама аутентификациялаш:

$$A \leftarrow B: r_n \quad (1)$$

$$A \rightarrow B : E_K(r_B, B) \quad (2)$$

Қатнашувчи B қатнашувчи A га тасодиғий сон r_B ни жўнатади.

Қатнашувчи A олинган сон r_B ва идентификатор B дан иборат хабарни шифрлайди ва шифрланган хабарни қатнашувчи B га жўнатади. Қатнашувчи B олинган хабарни расшифровка қилади ва хабардаги тасодиғий сонни қатнашувчи A га юборгани билан таққослайди. Қўшимча у хабардаги исмни текширади.

Тасодиғий қийматлардан фойдаланувчи икки томонлама аутентификациялаш:

$$A \leftarrow B : r_B \quad (1)$$

$$A \rightarrow B : E_K(r_A, r_B, B) \quad (2)$$

$$A \leftarrow B : E_K(r_A, r_B) \quad (3)$$

Иккинчи ахборотни олиши билан қатнашувчи B олдинги протоколдаги текширишни амалга оширади ва қатнашувчи A га аталган учинчи хабарга киритиш учун қўшимча тасодиғий сон r_A ни расшифровка қилади. Қатнашувчи A учинчи хабарни олганидан сўнг r_A ва r_B ларнинг қийматларини текшириш асосида айнан қатнашувчи B билан ишлаётганига ишонч ҳосил қилади.

Аутентификация жараёнида учинчи тарафни жалб этиш билан фойдаланувчиларни аутентификациялашни таъминловчи протоколларнинг машҳур намуналари сифатида Нидхэм ва Шредернинг махфий калитларни тақсимлаш протоколини ва Kerberos протоколини кўрсатиш мумкин.

Kerberos протоколи «мижоз-сервер» ва ҳам локал ва ҳам глобал тармоқларда ишловчи абонентлар орасида алоканинг химояланган каналини ўрнатишга аталган калит ахборотини алмашиш тизимларида аутентификациялаш учун ишлатилади. Бу протоколнинг Microsoft Windows 2000 ва UNIX BSD операцион тизимларига аутентификациялашнинг асосий протоколи сифатида ўрнатилганлиги алоҳида қизиқиш ўйғотади.

Kerberos ишонч қозонмаган тармоқларда аутентификациялашни таъминлайди, яъни Kerberos ишлашида нияти бўзук одамлар қуйидаги ҳаракатларни бажаришлари мумкин:

- ўзини тармок уланишининг эътироф этилган тарафларидан бири деб кўрсатиш;

- уланишда иштирок этаётган компьютерларнинг бирдан фойдалана олиш;

- ҳар қандай пакетни ушлаб қолиш, уларни модификациялаш ва ёки иккинчи марта узатиш.

Kerberos протоколида хавфсизлик таъминоти юқорида келтирилган нияти бузук одамларнинг ҳаракатлари натижасида пайдо бўладиган ҳар қандай муаммоларнинг бетарафлишини таъминлайди.

Kerberos протоколи олдинги асрнинг 80-йилларида яратилган ва шу пайтгача бешта версияда ўз аксини топган қатор жиддий ўзгаришларга дучор бўлди.

Kerberos TCP/IP тармоқлари учун яратилган бўлиб, протокол катнашчиларининг учинчи (ишонилган) тарафга ишонишлари асосига қурилган. Тармоқда ишловчи Kerberos хизмати ишонилган воситачи сифатида ҳаракат қилиб, тармок ресурсларидан мижознинг (мижоз иловасининг) фойдалинишини авторизациялаш билан тармоқда ишончли аутентификациялашни таъминлайди. Kerberos хизмати алоҳида махфий калитни тармокнинг ҳар бир субъекти билан бўлишади ва бундай махфий калитни билиш тармок субъекти ҳақиқийлигининг исботига тенг қучлидир.

Kerberos асосини Нидхем-Шредернинг учинчи ишонилган тараф билан аутентификациялаш ва калитларни тақсимлаш протоколи ташкил этади. Нидхем-Шредер протоколининг ушбу версиясини Kerberosга татбикан кўрайлик. Kerberos протоколида (5-версия) алоқа қилувчи иккита тараф ва калитларни тақсимлаш маркази KDC (Key Distribution Center) вазифасини бажарувчи ишонилган сервер KS иштирок этади.

Чакирувчи объект А орқали, чакирилувчи объект В орқали белгиланади. Сеанс катнашчилари, мос ҳолда Id_A ва Id_B ноёб идентификаторларга эга. А ва В тарафлар, ҳар бири алоҳида, ўзининг махфий калитини сервер KS билан бўлишади.

Айтайлик. А тараф В тараф билан ахборот алмашиш мақсадида сеанс калитини олмоқчи. А тараф тармок оркали сервер KSga Id_A ва Id_B идентификаторларни юбориш билан калитлар таксимланиши даврини бошлаб беради:

$$A \rightarrow KS : Id_A, Id_B$$

Сервер KS вақтий белги T , таъсир муддати L , тасодифий калит K ва идентификатор Id_A бўлган хабарни генерациялаб, бу хабарни B тараф билан бўлинган махфий калит ёрдамида шифрлайди.

Сўнгра сервер KS B тарафга тегишли вақтий белги T , таъсир муддати L , тасодифий калит K , идентификатор Id_B ни олиб уни A тараф билан бўлинган махфий калит ёрдамида шифрлайди. Бу иккала шифрланган хабарларни A тарафга жўнатади.

$$KS \rightarrow A : E_A(T, L, K, Id_B), E_B(T, L, K, Id_A)$$

A тараф биринчи хабарни ўзининг махфий калити билан расшифровка қилади ва ушбу хабар калитлар таксимотининг олдинги муолажасининг қайтарилиши эмаслигига ишонч ҳосил қилиш мақсадида вақт белгиси T ни текширади. Сўнгра A тараф ўзининг идентификатори Id_A ва вақт белгиси билан хабарни генерациялаб, уни сеанс калити K ёрдамида шифрлайди ва B тарафга узатади. Ундан гашқари, A тараф B тараф учун KS дан B тараф калити ёрдамида шифрланган хабарни жўнатади:

$$A \rightarrow B : E_K(Id_A, T), E_B(T, L, K, Id_A)$$

Бу хабарни фақат B тараф расшифровка қилиши мумкин. B тараф вақт белгиси T , таъсир муддати L , сеанс калити K ва идентификатор Id_A ни олади. Сўнгра B тараф сеанс калити K ёрдамида хабарнинг иккинчи қисмини расшифровка қилади. Хабарнинг иккала қисмидаги T ва Id_A қийматларининг мос келиши A нинг B га нисбатан ҳақиқийлигини тасдиқлайди.

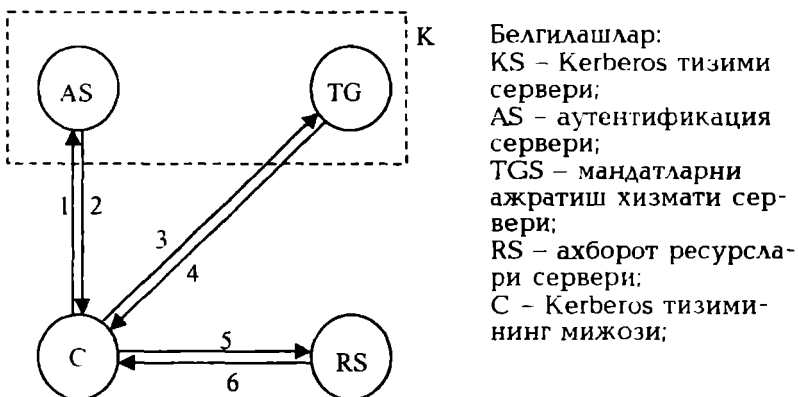
Ҳақиқийликни ўзаро тасдиқлаш мақсадида B тараф вақт белгиси T плюс 1 дан иборат хабар яратали, уни K калит ёрдамида шифрлайди ва A тарафга жўнатади.

$$B \rightarrow A : E_K(T + 1)$$

Агар бу хабар расшифровка килинганидан кейин *A* тараф кутилган натижани олса, у алоқа линиясининг бошқа тарафида хақиқатан *B* турганлигига ишонч ҳосил қилади.

Бу протокол барча қатнашувчиларнинг соатлари сервер *KS* соатлари билан синхронланганида муваффақиятли ишлайди. Таъкидлаш лозимки, бу протоколда *A* тарафнинг *B* тараф билан алоқа ўрнатишга ҳар бир хоҳишида сеанс калитини олиш учун *KS* билан алмашинув зарур бўлади. Протоколнинг *A* ва *B* объектларни ишончли улаши учун, ҳеч бир калит обрўсизланмаслиги ва сервер *KS* нинг химояланиши талаб этилади.

Умуман *Kerberos* тизимида (5 версия) фойдаланувчини идентификациялаш ва аутентификациялаш жараёнини куйидагича тавсифлаш мумкин (5.2-расм).



5.2-расм. Kerberos протоколнинг ишлаш схемаси.

Мижоз *C*, тармок ресурсидан фойдаланиш мақсадида аутентификация сервери *AS* га сўров йўллайди. Сервер *AS* фойдаланувчини унинг исми ва паролни ёрдамида идентификациялайди ва мижозга мандат ажратиш хизмати сервери *TGS*дан (*Ticket Granting Service*) фойдаланишга мандат юборади.

Ахборот ресурсларининг муайян мақсадли сервери *RS* дан фойдаланиш учун мижоз *C* *TGS* дан мақсадли сервер *RS* га мурожаат қилишга мандат сўрайди. Ҳамма нарса тартибда бўлса *TGS* керакли тармок ресурсларидан фойдаланишга рухсат бериб, мижоз *C* га мос мандатни юборади.

Kerberos тизими ишлашининг асосий кадамлари (5.2.-расмга каралсин):

1. $C \rightarrow AS$ – мижоз C нинг TGS хизматига мурожаат қилишга рухсат сўраб сервер AS дан сўрови.

2. $AS \rightarrow C$ – сервер AS нинг мижоз C га TGS хизматидан фойдаланишга рухсати (мандати).

3. $C \rightarrow TGS$ – мижоз C нинг ресурслар сервери RS дан фойдаланишга рухсат (мандат) сўраб, TGS хизматидан сўрови.

4. $TGS \rightarrow C$ – TGS хизматининг мижоз C га ресурслар сервери RS дан фойдаланишига рухсати (мандати).

5. $C \rightarrow RS$ – сервер RS дан ахборот ресурсининг (хизматнинг) сўрови.

6. $RS \rightarrow C$ – сервер RS нинг хақиқийлигини тасдиқлаш ва мижоз C га ахборот ресурсини (хизматни) тақдим этиш.

Мижоз билан сервер алоқасининг ушбу модели фақат узатиладиган бошқарувчи ахборотнинг конфиденциаллиги ва яхлилиги таъминланганида ишлаши мумкин. Ахборот хавфсизлигини катъий таъминламасдан AS , TGS ва RS серверларга мижоз C сўров юбораолмайди ва тармок хизматидан фойдаланишга рухсат ололмайди.

Ахборотнинг ушлаб қолиниши ва рухсатсиз фойдаланиши имкониятларини бартараф этиш мақсадида Kerberos тармокда ҳар қандай бошқариш ахбороти узатилганида махфий калитлар комплекси (мижознинг махфий калити, сервернинг махфий калити, мижоз-сервер жуфтнинг махфий сеанс калитлари) ёрдамида кўп марта шифрлашни ишлатади. Kerberos шифрлашнинг алмаштириш ва хэш-функциялардан фойдаланиши мумкин, ammo мададлаш учун Triple DES ва MD5 алгоритмлари ўрнатилган.

Kerberos тизимида ишонч ҳужжатларининг икки туридан фойдаланилади: мандат (ticket) ва аутентификатор (authenticator).

Мандат серверга мандат берилган мижознинг идентификацион маълумотларини хавфсиз узатиш учун ишлатилади. Унинг таркибида ахборот ҳам бўлиб, ундан сервер мандатдан фойдаланаётган мижознинг хақиқий эканлигини текширишда фойдаланиши мумкин.

Аутентификатор – мандат билан бирга кўрсатилувчи кўшимча атрибут (аломат). Қуйида Kerberos ҳужжатларида ишлатилувчи белгиланлар тизими келтирилган:

C – мижоз;

S – сервер;

a – мижознинг тармок манзили;

v – мандат таъсири вақтининг бошланиши ва охири;

m – вақт белгиси;

K_x – махфий калит x ;

$K_{x,y}$ – x ва y учун сеанс калити;

$\{m\}K_x$ – субъект x нинг махфий калити K_x билан шифрланган хабар m ;

$T_{x,y}$ – y дан фойдаланишга мандат x ;

$A_{x,y}$ – x ва y учун аутентификатор.

Kerberos мандати

Kerberos мандати қуйидаги шаклга эга:

$$T_{C,S} = S, \{C, a, v, K_{C,S}\} K_S.$$

Мандат битта мижозга катъий белгиланган сервердан фойдаланиш учун катъий белгиланган вақтга берилади. Унинг таркибида мижоз исми, унинг тармок манзили, мижоз харакатининг бошланиш ва тугаш вақти ва сервернинг махфий калити K_S шифрланган сеанс калити $K_{C,S}$ бўлади. Мижоз мандатни расшифровка қила олмайди (y сервернинг махфий калитини билмайди), аммо y мандатни шифрланган шаклда серверга кўрсатиши мумкин. Мандат тармок орқали узатилаётганда тармокдаги яширинча эшитиб турувчиларнинг бирортаси ҳам уни ўқий олмайди ва ўзгартира олмайди.

Kerberos аутентификатори

Kerberos аутентификатори қуйидаги шаклга эга:

$$A_{C,S} = \{C, t, \text{калит}\} K_{C,S}$$

Мижоз мақсадли сервердан фойдаланишни хоҳлаганида аутентификаторни яратади. Унинг таркибида мижоз ва сервер учун умумий бўлган сеанс калити $K_{C,S}$ шифрланган мижоз исми, вақт белгиси, сеанс калити бўлади. Мандатдан фаркли холда аутентификатор бир марта ишлатилади.

Аутентификаторнинг ишлатилиши иккита мақсадни кўзлайди. Биринчидан, аутентификаторда сеанс калитида шифрланган қандайдир матн бўлади. Бу калитнинг мижозга маълумлигидан далолат беради. Иккинчидан, шифрланган очик матнда вақт белгиси мавжуд. Бу вақт белгиси аутентификатор ва мандатни ушлаб

колган нияти бузук одамга улардан бирор вақт ўтганидан сўнг аутентфикациялаш муолжасини ўтишда ишлатишига имкон бермайди.

Kerberos хабарлари

Kerberosнинг 5-версиясида хабарларнинг куйидаги гурлари ишлатилади (5.2-расмга қаралсин).

1. Мижоз – Kerberos: C, tgs .
2. Kerberos – мижоз: $\{K_{C,tgs}\}K_C\{T_{C,tgs}\}K_{tgs}$.
3. Мижоз – TGS: $\{A_{C,S}\}K_{C,tgs}(T_{C,tgs})K_{tgs,S}$.
4. TGS – мижоз: $\{K_{C,S}\}K_{C,tgs}\{T_{C,S}\}K_S$.
5. Мижоз – сервер: $\{A_{C,S}\}K_{C,S}\{T_{C,S}\}K_S$.

Ушбу хабарлардан фойдаланишни батафсил кўрайлик.

Дастлабки мандатни олиш

Мижоздан шахсини исботловчи ахборотнинг қисми унинг пароли мавжуд. Мижозни паролини тармоқ орқали жўнатишига мажбур қилиб бўлмайди. Kerberos протоколи паролни обрўсизлантириш эҳтимolini минималлаштиради, агар фойдаланувчи паролни билмаса унга ўзини тўғри идентификациялашга имкон бермайди.

Мижоз Kerberosнинг аутентификация серверига ўзининг исми, сервери TGS нинг (бир нечта сервер TGS бўлиши мумкин) бўлган хабарни жўнатади. Амалда фойдаланувчи кўпинча исмини ўзини киритади, тизимга кириш дастури эса сўров юборади.

Kerberosнинг аутентификациялаш сервери ўзининг маълумотлар базасида мижоз хусусидаги маълумотларни кидиради. Агар мижоз хусусидаги ахборот маълумотлар базасида бўлса, Kerberos мижоз ва TGS орасида маълумот алмашиш учун ишлатиладиган сеанс калитини генерациялайди. Kerberos бу сеанс калитини мижознинг махфий калити билан шифрлайди. Сўнгра у TGS хизмати-га мижознинг ҳақиқийлигини исботловчи TGT (*Ticket Granting Ticket*) мандатининг ажратилиши учун мижозга мандат яратади. TGS нинг махфий калитида TGT шифрланади ва унинг таркибида мижоз ва сервер идентификатори, TGS – мижоз жуфтнинг сеанс калити ҳамда TGT таъсирининг бошланиш ва охириги вақтлари

бўлади. Аутентификациялаш сервери бу иккита шифрланган хабарни мижозга юборади.

Энди мижоз бу хабарларни қабул қилади, биринчи хабарни ўзининг махфий калити K_C билан расшифровка қилиб, сеанс калити $K_{C,TGS}$ ни хосил қилади. Махфий калит мижоз паролнинг бир томонлама хэш-функцияси бўлганлиги сабабли конуний фойдаланувчида ҳеч қандай муаммо туғилмайди. Нияти бузук одам туғри паролни билмайди ва, демак, аутентификациялаш серверининг жавобини расшифровка қила олмайди. Шу сабабли нияти бузук одам мандатни ёки сеанс калитини ола олмайди. Мижоз TGT мандатини ва сеанс калитини саклаб, парол ва хэш-кийматни, уларнинг обрўсизланиш эҳтимолликларини пасайтириш мақсадида, ўчиради. Агар нияти бузук одам мижоз хотираси таркибининг нухасини олишга ўринса, у фақат TGT ва сеанс калитини олади. Бу маълумотлар фақат TGT таъсири вақтидагина муҳим ҳисобланади. TGT таъсир муддати тугаганидан сўнг бу маълумотлар маънога эга бўлмайди. Энди мижоз TGT дан олинган мандат ёрдамида унда кўрсатилган TGT таъсирининг бутун муддати мобайнида сервер TGS да аутентификациялашдан ўтиш имкониятига эга.

Сервер мандатларини олиш

Мижоз ўзига керак бўлган ҳар бир хизмат учун алоҳида мандат олиши мумкин. Шу мақсадда мижоз TGS хизматида TGT мандати ва аутентификатордан иборат сўров юбориши лозим. (Амалда сўровни дастурий таъминот автоматик тарзда, яъни фойдаланувчига билдирмасдан юборади.) Мижоз ва TGS сервери жуфтнинг калитида шифрланган аутентификатор таркибида мижоз ва унга керакли сервернинг идентификатори, тасодифий сеанс калити ва вақт белгиси бўлади.

TGS сўровни олиб, ўзининг махфий калитида TGT ни расшифровка қилади. Сўнгра TGS TGT даги сеанс калитидан аутентификаторни расшифровка қилишда фойдаланади. Нихоясида аутентификатордаги ахборотни мандат ахбороти билан таққосланади. Аниқроғи, чиптадаги мижознинг тармок манзили сўровда кўрсатилган тармок манзили билан ҳамда вақт белгиси жорий вақт

билан солиштирилади. Агар барчаси мос келса, TGS сўровни бажаришга рухсат беради.

Вақт белгиларини текширишда барча компьютерларнинг соатлари, бўлмаганда, бир неча минут аниклигида синхронланганлиги кўзда тутилди. Агар сўровда кўрсатилган вақт жорий ондан анчагина фарк килса, TGS бундай сўровни олдинги сўровни қайтаришга уриниш деб ҳисоблайди.

TGS хизмати аутентификатор таъсири муддатининг тўғрилигини кузатиши лозим, чунки сервер хизмати битта мандат, аммо турли аутентификаторлар ёрдамида кетма-кет бир неча марта сўралиши мумкин. Ўша мандат ва аутентификаторнинг ишлатилган вақт белгиси билан қилинган бошқа сўров қайтарилди.

Тўғри сўровга жавоб тариқасида TGS мижозга мақсад сервердан фойдаланиш учун мандат тақдим этади. TGS мижоз ва мақсад сервери учун мижоз ва TGS га умумий бўлган сеанс калитида шифрланган сеанс калитини ҳам яратади. Бу иккала хабар мижозга юборилади. Мижоз хабарни расшифровка қилади ва сеанс калитини чиқариб олади.

Хизмат сўрови

Энди мижоз ўзининг ҳақиқийлигини мақсад серверига исботлаши мумкин. Мақсад серверида аутентификациядан муваффақиятли ўтиш учун мижоз таркибида ўзининг исми, тармок манзили, вақт белгиси бўлган ва сеанс калити «мижоз-сервер»да шифрланган аутентификаторни яратади ва уни TGS хизматидан олиб берилган мақсад серверининг махфий калитида шифрланган мандат билан бирга жўнатади.

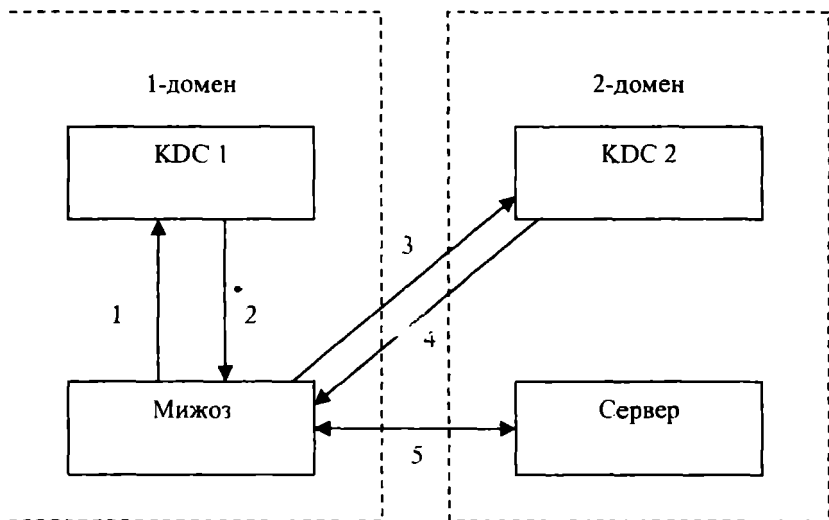
Мақсад сервери мижоздан маълумотларни олиб, аутентификаторни ўзининг махфий калитида расшифровка қилади ва ундан «мижоз-сервер» сеанс калитини чиқариб олади. Мандат ҳам текширилади. Текшириш муолажаси «мижоз-TGS» сессиясида ўтказила-диган муолажага ўхшаш, яъни тармок манзиллари ва вақт белгисининг мослиги текширилади. Агар барчаси мос келса, сервер мижознинг ҳақиқийлигига ишонч ҳосил қилади.

Агар илова ҳақиқийликнинг ўзаро текширилишини талаб этса, сервер мижозга таркибида сеанс калитида шифрланган вақт белгиси бўлган хабарни юборади. Бу серверга тўғри махфий калитининг

маълум эканлигини ва у мандат ва гувоҳномани расшифровка кила олишини исботлайди. Зарурият туғилганида миждоз ва сервер кейинги хабарларни умумий калитда шифрлашлари мумкин. Чунки бу калит фақат уларга маълум, бу калит билан шифрланган охириги хабар иккинчи тарафдан юборилганига иккала тараф ишонч ҳосил килишлари мумкин. Амалда бу барча мураккаб муолажалар автоматик тарзда бажарилади ва миждозга қандайдир ноқулайликлар етказилмайди.

Доменлараро аутентификациялаш хусусиятлари

Kerberos дан доменлараро аутентификациялашда ҳам фойдаланиш мумкин. Миждоз бошқа домендаги сервердан фойдаланиш мақсадида калитларни тақсимлаш маркази *KDC* га мурожаат қилса, *KDC* миждозга сўралаётган сервер жойлашган доменнинг *KDC* ига мурожаат этишга қайта манзиллаш мандатини (referral ticket) тақдим этади (5.3-расм).



5.3-расм. Kerberos протоколида доменлараро аутентификациялаш схемаси.

Расмда қуйидаги белгилашлар қабул қилинган:

1. Аутентификациялашга сўров.

2. *KDC1* учун *TGT*

3. *KDC2* учун *TGT*.

4. Сервердан фойдаланиш мандати.

5. Маълумотларни аутентификациялаш ва алмашиш.

Қайта манзиллаш мандати иккита домен *KDC*сининг жуфтли алоқа калитида шифрланган *TGT*дир. Бунда мижозга сервердан фойдаланишга мандатни сўралаётган сервер жойлашган *KDC* тақдим этади.

Жуда кўп доменли тармоқда аутентификациялаш учун *Kerberos*дан фойдаланиш назарий жиҳатдан мумкин бўлсада, мурожаатлар сонининг доменлар сонига муганосиб равишда ошиши сабабли, сўровларни муайян *KDC*ларга бир маънода қайта манзил-ловчи қандайдир марказий домен куришга тўғри келади.

Kerberos хавфсизлиги

Kerberos, криптографик химоялашнинг бошқа ҳар қандай дастурий воситаси каби ишончсиз дастурий муҳитда ишлайди. Ушбу муҳитнинг ҳужжатлаштирилмаган имкониятлари ёки нотўғри конфигурацияси жиддий ахборотнинг чиқиб кетишига олиб келиши мумкин. Ҳатто, калитлар фойдаланувчи ишлаш ссансида фақат оператив хотирада сақланса ҳам операцион тизимдаги бузилиш калитларнинг каттик дискда нусхаланишига олиб келиши мумкин.

Kerberos дастурий таъминоти ўрнатилган ишчи станциясидан кўпчилик фойдаланувчи режимнинг ишлатилиши ёки ишчи станциялардан фойдаланишнинг назорати бўлмаслиги дастур-закладкани киритиш ёки криптографик дастурий таъминотни модификациялаш имкониятини туғдиради.

Шу сабабли, *Kerberos* хавфсизлиги кўп жиҳатдан ушбу протокол ўрнатилган ишчи станцияси химоясининг ишончлигига боғлиқ.

Kerberos протоколининг ўзига қуйидаги қатор талаблар қуйилади:

– *Kerberos* хизмати хизмат қилишдан воз кечишга йўналтирилган ҳужумлардан химояланиши шарт;

– вақт белгиси аутентификация жараёнида қатнашиши сабабли, тизимдан фойдаланувчиларининг барчаси учун тизимли вақтни синхронлаш зарур;

– *Kerberos* паролни саралаш орқали ҳужум қилишдан химояламайди. Муаммо шундаки, *KDC* да сақланувчи фойдаланувчи ка-

лиги унинг паролни хэш-функция ёрдамида қайта ишлаш натижасидир. Паролнинг бўшлиғида уни саралаб топиш мумкин.

– Kerberos хизмати рухсатсиз фойдаланишининг барча турларидан ишончли химояланиши шарт;

мижоз олган маъдатлар ҳамда махфий калитлар рухсатсиз фойдаланишдан химояланиши шарт.

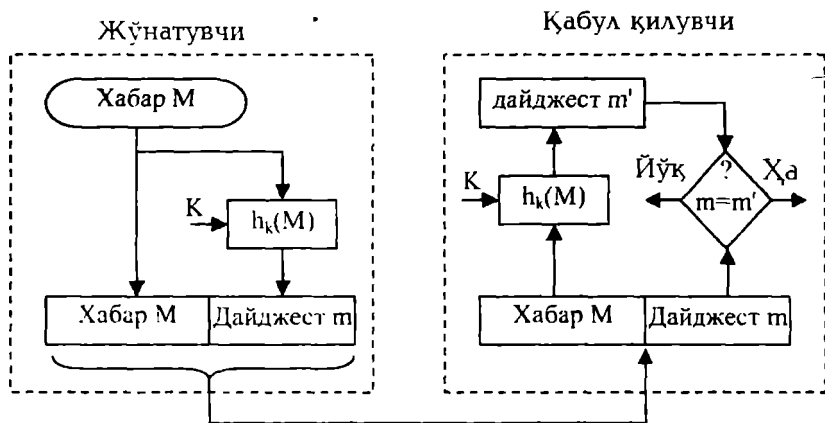
Юқорида келтирилган талабларнинг бажарилмаслиги муваффақиятли хужумга сабаб бўлиши мумкин.

Ҳозирда Kerberos протоколи аутентификациялашнинг кенг тарқалган воситаси ҳисобланади. Kerberos турли криптографик схемалар, хусусан, очик калитли шифрлаш билан биргаликда ишлатилиши мумкин.

Бир томонлама калитли хэш-функциялардан фойдаланишга асосланган протоколлар

Бир томонлама хэш-функция ёрдамида шифрлашнинг ўзига хос хусусияти шундаки, у моҳияти бўйича бир томонламадир, яъни тескари ўзгартириш-қабул қилувчи тарафда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) бир томонлама шифрлаш муолажасидан фойдаланади.

Шифрланаётган маълумот M га қўлланилган K параметр-калитли бир томонлама хэш-функция $h_k(.)$ натижада, байтларнинг белгиланган катта бўлмагани сонидан иборат хэш-қиймат (дайджест) m ни беради (5.4-расм).



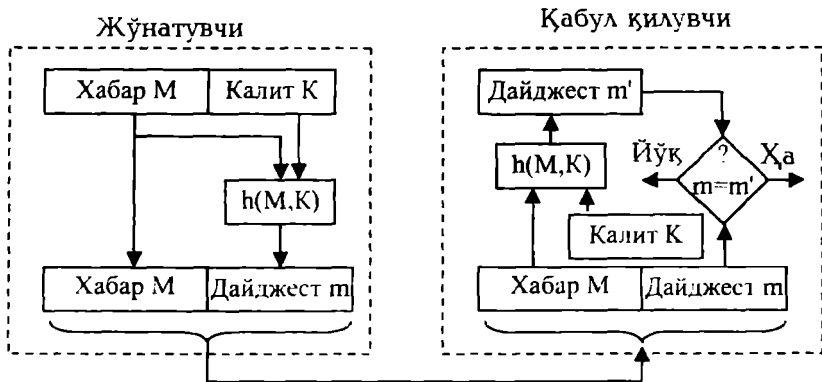
5.4-расм. Маълумотлар яхлитлигини текширишда бир томонлама хэш-функциянинг ишлатилиши (I-вариант).

Дайджест m кабул қилувчига дастлабки хабар M билан бирга узатилади. Хабарни кабул қилувчи, дайджест олинишида қандай бир томонлама хэш-функция ишлатилганлигини билган ҳолда, расшифровка қилинган хабар M дан фойдаланиб, дайджестни бошқатдан ҳисоблайди. Агар олинган дайджест билан ҳисобланган дайджест мос келса, хабар M нинг таркиби ҳеч қандай ўзгаришга дучор бўлмаганини билдиради.

Дайджестни билиш дастлабки хабарни тиклашга имкон бермайди, аммо маълумотлар яхлитлигини текширишга имкон беради. Дайджестга дастлабки хабар учун ўзига хос назорат йиғиндиси сифатида қараш мумкин. Аммо, дайджест ва оддий назорат йиғиндиси орасида жиддий фарқ ҳам мавжуд. Назорат йиғиндисидан алоканинг ишончсиз линияси бўйича узатиладиган хабарларнинг ахлитлигини текшириш воситаси сифатида фойдаланилади. Текширишнинг бу воситаси нияти бузук одамлар билан кўрашишга мўлжалланмаган. Чунки, бу ҳолда назорат йиғиндисининг янги қийматини кўшиб хабарни алмаштириб кўйишга уларга ҳеч ким халакит бермайди. Кабул қилувчи бунда ҳеч нарса сезмайди.

Дайджестни ҳисоблашда, оддий назорат йиғиндисидан фарқли равишда, махфий калитлар ишлатилади. Агар дайджест олинишида фақат жўнатувчи ва кабул қилувчига маълум бўлган параметр-калитли бир томонлама хэш-функция ишлатилса, дастлабки хабарнинг ҳар қандай модификацияси дарҳол маълум бўлади.

5.5-расмда маълумотлар яхлитлигини текширишда бир томонлама хэш-функция ишлатилишининг бошқа варианты келтирилган.



5.5-расм. Маълумотлар яхлитлигини текширишда бир томонлама хэш-функциянинг ишлатиши (II-вариант).

Бу холда бир томонлама хэш-функция $h(.)$ параметр-калитга эга эмас, аммо у махфий калит билан тўлдирилган хабарга қўлланилади, яъни жўнатувчи дайджест $m=h(M, K)$ ни ҳисоблайди. Қабул килувчи дастлабки хабарни чиқариб олиб, уни ўша маълум махфий калит билан тўлдиради. Сўнгра олинган маълумотларга бир томонлама хэш-функция $h(.)$ ни қўллайди. Ҳисоблаш натижаси – дайджест m тармоқ орқали олинган дайджест m билан таккосланади.

Асимметрик алгоритмларга асосланган қатъий аутентификациялаш

Қатъий аутентификациялаш протоколларида очик калитли асимметрик алгоритмлардан фойдаланиш мумкин. Бу холда исботловчи махфий калитни билишлигини куйидаги усулларнинг бири ёрдамида намойиш этиши мумкин:

- очик калитда шифрланган сўровни расшифровка килиш;
- сўров сўзига рақамли имзосини қўйиш.

Аутентификацияга зарур бўлган калитларнинг жуфти, хавфсизлик мулоҳазасига кўра, бошқа мақсадларга (масалан, шифрлашда) ишлатилмаслиги шарт. Очик калитли танланган тизим шифрланган матнни танлаш билан хужумларга, ҳатто бузғунчи ўзини текширувчи деб кўрсатиб ва унинг номидан ҳаракат килганда ҳам, бардош бериши лозимлигига фойдаланувчиларни огоҳлантириш керак.

Шифрлашнинг асимметрик алгоритмларидан фойдаланиб аутентификациялаш.

Шифрлашнинг асимметрик алгоритмларидан фойдаланишга асосланган протоколга мисол тариқасида аутентификациялашнинг куйидаги протоколини келтириш мумкин:

$$A \leftarrow B : h(r), B, P_A(r, B),$$

$$A \rightarrow B : r.$$

Қатнашувчи B тасодифий ҳолда r ни танлайди ва $x=h(r)$ кийматини ҳисоблайди (x киймати r нинг кийматини очмасдан туриб r ни билишлигини намойиш этади), сўнгра $y = P_A(r, B)$ кийматни ҳисоблайди. P_A орқали асимметрик шифрлаш алгоритми фараз қилинса, $h(.)$ орқали хэш-функция фараз қилинади. Қатнашувчи B ахборот хабарни қатнашувчи A га жўнатади. Қатнашувчи A $e = P_A(r, B)$ ни расшифровка қилади ва r' ва B' кийматларни олади ҳамда $x' = h(r')$ ни ҳисоблайди. Ундай кейин

$x=x'$ эканлигини ва B' идентификатор хакикатан қатнашувчи B га кўрсатаётганини тасдиқловчи қатор такқослашлар бажарилади. Такқослаш муваффақиятли ўтса қатнашувчи A га қатнашувчини B гани узатади. Қатнашувчи B r ни олганидан сўнг уни биринчи ҳабарда жўнатган қиймат эканлигини текширади.

Кейинги мисол сифатида асимметрик шифрлашга асосланган Нидхем ва Шредернинг модификацияланган протоколини келтирамыз. Фақат аутентификациялашда ишлатилувчи Нидхем ва Шредер протоколи вариантини кўришда P_B орқали қатнашувчи B нинг очик қалити ёрдамида шифрлаш алгоритми фараз қилинади. Протокол қуйидаги тузилмага эга:

$$A \rightarrow B : P_B(r_1, A)$$

$$A \leftarrow B : P_A(r_2, r_i)$$

$$A \leftarrow B : r_2$$

Рақамли имзодан фойдаланиш асосидаги аутентификациялаш:

X.509 стандартининг тавсияларида рақамли имзо, вақт белгиси ва тасодифий сонлардан фойдаланиш асосидаги аутентификациялаш схемаси спецификацияланган. Ушбу схемани тавсифлаш учун қуйидаги белгилашларни киритамиз:

- t_A, r_A ва r_B – мос ҳолда вақт белгиси ва тасодифий сонлар;
- S_A – қатнашувчи A генерациялаган имзо;
- S_B – қатнашувчи B генерациялашган имзо;
- $cert_A$ – қатнашувчи A очик қалитининг сертификати;
- $cert_B$ – қатнашувчи B очик қалитининг сертификати.

Мисол тарикасида аутентификациялашнинг қуйидаги протоколларини келтирамыз:

1. Вақт белгисидан фойдаланиб бир томонлама аутентификациялаш:

$$A \rightarrow B : cert_A, t_A, B, S_A(t_A, B)$$

Қатнашувчи B ушбу хабарни олганидан сўнг вақт белгиси t_A нинг, олинган идентификатор B нинг тўғрилигини ва сертификат $cert_A$ даги очик қалитдан фойдаланиб рақамли имзо $S_A(t_A, B)$ нинг корректлигини текширади.

2. Тасодифий сонлардан фойдаланиб бир томонлама аутентификациялаш:

$$A \leftarrow B : r_B$$

$$A \rightarrow B : cert_{A, r_A, B, S_A(r_A, r_B, B)}$$

Катнашувчи B катнашувчи A дан хабарни олиб айнан у хабарнинг манзилати эканлигига ишонч ҳосил қилади; сертификат $cert_A$ дан олинган катнашувчи A очик калитидан фойдаланиб очик кўринишда олинган r_A сони, биринчи хабарда жўнатилган r_B сони ва ўзининг идентификатори B остидаги имзо $S_A(r_A, r_B, B)$ нинг корректлигини текширади. Имзо чекилган тасодифий сон r_A очик матнни танлаш билан ҳужумни олдини олиш учун ишлатилади.

3. Тасодифий сонлардан фойдаланиб икки томонлама аутентификациялаш:

$$A \leftarrow B : r_B$$

$$A \rightarrow B : cert_{A, r_A, B, S_A(r_A, r_B, B)}$$

$$A \leftarrow B : cert_{B, A, S_B(r_A, r_B, A)}$$

Ушбу протоколдаги хабарларни ишлаш олдинги протоколдагидек бажарилади.

5.5. Фойдаланувчиларни биометрик идентификациялаш ва аутентификациялаш

Охирги вақтда инсоннинг физиологик параметрлари ва характеристикаларини, хулқининг хусусиятларини ўлчаш орқали фойдаланувчини ишончли аутентификациялашга имкон берувчи биометрик аутентификациялаш кенг тарқалмоқда.

Биометрик аутентификациялаш усуллари анъанавий усулларга нисбатан қуйидаги афзалликларга эга:

- биометрик аломатларни ноёблиги туфайли аутентификациялашнинг ишончлилик даражаси юкори;
- биометрик аломатларнинг ишга лаёқатли шахсдан ажратиб бўлмаслиги;
- биометрик аломатларни сохталаштиришнинг кийинлиги.

Фойдаланувчини аутентификациялашда фаол ишлатиладиган биометрик аломатлари қуйидагилар:

- бармок излари;
- кўл панжасининг геометрик шакли;
- юзнинг шакли ва ўлчамлари;
- овоз хусусиятлари;
- кўз ёйи ва тўр пардасининг нақши.

Аутентификациянинг биометрик қисм тизими ишлашининг намунавий схемаси қуйидагича. Тизимда рўйхатга олинмишида фойдаланувчидан ўзининг характерли аломатларини бир ёки бир неча марта намойиш қилиниши талаб этилади. Бу аломатлар

(хакикий сифатида маълум) тизим томонидан қонуний фойдаланувчининг қиёфаси сифатида рўйхатга олинади. Фойдаланувчининг бу қиёфаси тизимда электрон шаклда сақланади ва ўзини қонуний фойдаланувчи деб даъво қилган ҳар бир одамни текширишда ишлатилади. Тақдим этилган аломатлар мажмуаси билан рўйхатга олинганларининг мослиги ёки мос келмаслигига қараб қарор қабул қилинади. Истеъмолчи нуктаи назаридан биометрик аутентификациялаш тизими қуйидаги иккита параметр орқали характерланади:

- хатолик инкорлар коэффициентининг FRR (false-reject rate);
- хатолик тасдиқлар коэффициентининг FAR (false-alarm rate).

Хатолик инкор тизим қонуний фойдаланувчи шахсини тасдиқламаганда пайдо бўлади (одатда FRR қиймати тахминан 100 дан бирни ташкил этади). *Хатолик тасдиқ* тизим қонуний фойдаланувчи шахсини тасдиқлаганида пайдо бўлади (одатда, FAR қиймати тахминан 10000 дан бирни ташкил этади). Бу иккала коэффициент бир бири билан боғлиқ: хатолик инкор коэффициентининг ҳар бирига маълум хатолик тасдиқ коэффициентининг мос келади. Муқаммал биометрик тизимда иккала хатоликнинг иккала параметри нолга тенг бўлиши шарт. Афсуски, биометрик тизим идеал эмас, шу сабабли ниманидур қурбон қилишга тўғри келади. Одатда, тизимли параметрлар шундай соланадики, мос хатолик инкорлар коэффициентини аниқловчи хатолик тасдиқларнинг исталган коэффициентига эришилади.

Биометрик аутентификациялашнинг дактилоскопик тизими

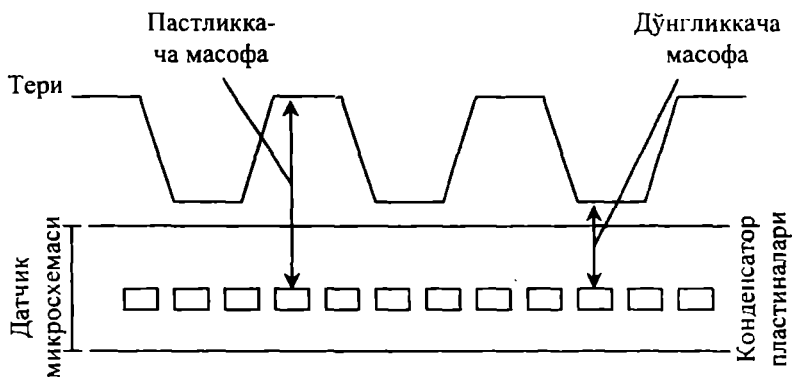
Биометрик тизимларнинг аксарияти идентификациялаш параметри сифатида бармоқ изларидан фойдаланади (аутентификациянинг дактилоскопик тизими). Бундай тизимлар содда ва қулай, аутентификациялашнинг юқори ишончлилигига эга. Бундай тизимларнинг кенг тарқалишига асосий сабаб бармоқ излари бўйича қатта маълумотлар баъзасининг мавжудлигидир. Бундай тизимлардан дунёда асосан полиция, турли давлат ва баъзи банк ташкилотлари фойдаланади.

Аутентификациянинг дактилоскопик тизими қуйидагича ишлайди. Аввал фойдаланувчи рўйхатга олинади. Одатда, сканерда бармоқнинг турли ҳолатларида сканерлашнинг бир неча варианты амалга оширилади. Табиийки, намуналар бир-биридан бир оз фарқланади ва қандайдир умумлаштирилган намуна, «паспорт» шакллантирилиши талаб этилади. Натижалар аутентификациянинг маълумотлар базасида хотирланади. Аутентификациялашда сканерланган бармоқ изи маълумотлар базасидаги «паспортлар» билан таққосланади.

Бармоқ изларининг сканерлари. Бармоқ изларини сканерловчи анъанавий қурилмаларда асосий элемент сифатида бармоқнинг характерли расмини ёзувчи кичкина оптик камера ишлатилади. Аммо, дактилоскопик қурилмаларни ишлаб чиқарувчиларнинг кўпчилиги интеграл схема асосидаги сенсорли қурилмаларга эътибор бермоқдалар. Бундай тенденция бармоқ изларига асосланган аутентификациялашни қўллашнинг янги соҳаларини очади.

Бундай технологияларни ишлаб чиқувчи компаниялар бармоқ изларини олишда турли, хусусан электрик, электромагнит ва бошқа усулларни амалга оширувчи воситалардан фойдаланадилар.

Сканерлардан бири бармоқ изи тасвирини шакллантириш мақсадида тери қисмларининг сўғим қаршилигини ўлчайди. Масалан, Veridicom компаниясининг дактилоскопик қурилмаси ярим-ўтказгичли датчик ёрдамида сўғим қаршилигини аниқлаш орқали ахборотни ййғади. Сенсор ишлашининг принципи куйидагича: ушбу асбобга қуйилган бармоқ конденсатор пластиналарининг бири вазифасини ўтайди (5.6-расм). Сенсор сиртида жойлашган иккинчи пластина конденсаторнинг 90000 сезгир пластинкали кремний микросхемасидан иборат. Сезгир сўғим датчиклари бармоқ сирти дўнгликлари ва пастликлари орасидаги электрик майдон кучининг ўзгаришини ўлчайди. Натижада, дўнгликлар ва пастликларгача бўлган масофа аниқланиб, бармоқ изи тасвири олинади.



5.6-расм. Сенсор ишлашининг принципага.

Интеграл схема асосидаги сенсорли текширишда AuthenTec компаниясида ишлатилувчи усул аниқликни яна ҳам оширишга имкон беради.

Қатор ишлаб чиқарувчилар биометрик тизимларни смартфонлар ва карта-калитлар билан комбинациялайдилар.

Интеграл схемалар асосидаги бармоқ излари датчикларининг кичик ўлчамлари ва юқори бўлмаган нархи уларни химоя тизими учун мукамал интерфейсга айлантиради. Уларни калитлар учун брелокларга ўрнатиш мумкин. Натижада, фойдаланувчи компьютердан бошлаб то кириш йўли, автомобиллар ва банкоматлар эшикларидан химояли фойдаланишни таъминлайдиган универсал калитга эга бўлади.

Қўл панжасининг геометрик шакли бўйича аутентификациялаш тизимлари. Қўл панжаси шаклини ўқувчи қуролмалар бармоқлар узунлигини, қўл панжа қалинлиги ва юзасини ўлчаш орқали қўл панжасининг ҳажмий тасвирини яратади. Масалан, Recognition Systems компаниясининг маҳсулотлари 90 дан ортиқ ўлчамларни амалга оширади. Натижада, кейинги таккослаш учун 9-хонали намуна шакллантирилади. Бу натижа қўл панжасини индивидуал сканерида ёки марказлаштирилган маълумотлар базасида сақлаши мумкин. Қўл панжасини сканерловчи қуролмалар нархининг юқорилиги ва ўлчамларининг катталиги сабабли тармоқ мухитида камдан-кам ишлатилсада, улар катъий хавфсизлик режимида ва шиддатли трафикка эга бўлган ҳисоблаш мухити (сервер хоналари ҳам бунга қиради) учун қулай ҳисобланади. Уларнинг аниқлиги юқори ва инкор коэффициентлари юқори инкор этилган қонуний фойдаланувчилар фойдаси кичик.

Юзнинг тузилиши ва овоз бўйича аутентификацияловчи тизимлар. Бу тизимлар арзонлиги туфайли энг фойдаланувчан ҳисобланадилар. Чунки аксарият замонавий компьютерлар видео ва аудио воситаларига эга. Бу синф тизимлари телекоммуникация тармоқларида масофадаги фойдаланувчи субъектни идентификациялаш учун ишлатилади. *Юз тузилишини сканерлаш технологияси* бошқа биометрик технологиялар яроқсиз бўлган иловалар учун тўғри келади. Бу ҳолда шахсни идентификациялаш ва верификациялаш учун кўз, бурун ва лаб хусусиятлари ишлатилади. Юз тузилишини аниқловчи қуролмаларни ишлаб чиқарувчилар фойдаланувчини идентификациялашда хусусий математик алгоритмлардан фойдаланадилар.

Маълум бўлишича, кўпгина ташкилотларнинг ходимлари юз тузилишини сканерловчи қуролмаларга ишонмайдилар. Уларнинг

фикрича камера уларни расмга олади, сўнгра суратни монитор экранига чиқаради. Камеранинг сифати эса паст бўлиши мумкин. Ундан ташқари юз тузилишини сканерлаш биометрик аутентификациялаш усуллари ичида ягона, текширишга рухсатни талаб қилмайдиган (яширинган камера ёрдамида амалга оширилиши мумкин) усул ҳисобланали.

Таъкидлаш лозимки, юз тузилишини аниқлаш технологияси янада такомиллаштирилишни талаб этади. Юз тузилишини аниқловчи аксарият алгоритмлар куёш ёруғлиги жадаллигининг кун бўйича тебраниши натижасидаги ёруғлик ўзгаришига таъсирчан бўладилар. Юз ҳолатининг ўзгариши ҳам аниқлаш натижасига таъсир этади. Юз ҳолатининг 45⁰ га ўзгариши аниқлашни самарасиз бўлишига олиб келади.

Овоз бўйича аутентификациялаш тизимлари. Бу тизимлар арзонлиги туфайли фойдаланувчан ҳисобланадилар. Хусусан уларни кўпгина шахсий компьютерлар стандарт комплектидаги ускуна (масалан, микрофонлар) билан бирга ўрнатиш мумкин. Овоз бўйича аутентификациялаш тизимлари ҳар бир одамга ноёб бўлган баландлиги, модуляцияси ва товуш частотаси каби овоз хусусиятларига асосланади. Овозни аниқлаш нутқни аниқлашдан фаркланади. Чунки нутқни аниқловчи технология абонент сўзини изохласа, овозни аниқлаш технологияси сўзловчининг шахсини тасдиқлайди. Сўзловчи шахсини тасдиқлаш баъзи чегараланишларга эга. Турли одамлар ўхшаш овозлар билан гапириши мумкин, ҳар қандай одамнинг овози вақт мобайнида қайфияти, ҳиссиётлик ҳолати ва ёшига боғлиқ ҳолда ўзгариши мумкин. Унинг устига телефон аппаратларнинг турли-туманлиги ва телефон орқали боғланишларнинг сифати сўзловчи шахсини аниқлашни қийинлаштиради. Шу сабабли овоз бўйича аниқлашни юз тузилишини ёки бармоқ изларини аниқлаш каби бошқа усуллар билан биргаликда амалга ошириш мақсадга мувофиқ ҳисобланади.

Кўз ёйи тўр пардасининг шакли бўйича аутентификациялаш тизими. Бу тизимларни иккита синфга ажратиш мумкин:

- кўз ёйи расмидан фойдаланиш;
- кўз тўр пардаси кон томирлари расмидан фойдаланиш.

Одам кўз пардаси аутентификация учун ноёб объект ҳисобланади. Кўз туби кон томирларининг расми ҳатто эгизакларда ҳам фаркланади. Идентификациялашнинг бу воситаларидан хавфсизликнинг юқори даражаси талаб этилганида (масалан,

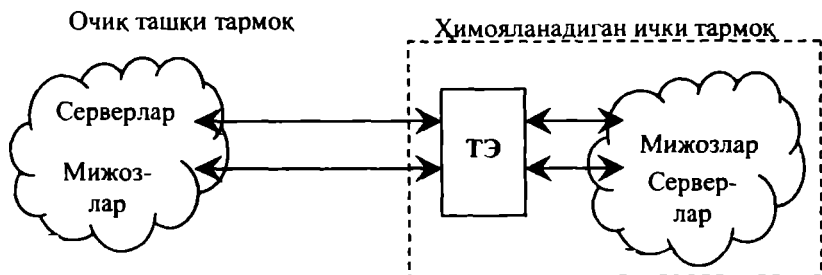
харбий ва мудофаа объектларининг режимли зоналарида) фойдаланилади.

Биометрик ёндашиш «ким бу ким» эканлигини аниқлаш жараёнини соддалаштиришга имкон беради. Дактилоскопик сканерлар ва овозни аниқловчи қурилмалардан фойдаланиш ходимларни тармоққа киришларида мураккаб паролларни эслаб қолишдан халос этади. Қатор компаниялар корхона масштабидаги бир мартали аутентификация SSO (Single Sign-On) га биометрик имкониятларни интеграциялайдилар. Бундай бириктириш тармоқ маъмурларига паролларни бир мартали аутентификациялаш хизматини биометрик технологиялар билан алмаштиришга имкон беради. Шахсни биометрик аутентификациялашнинг биринчилар қаторида кенг тарқалган соҳаларидан бири мобил тизимлари бўлди. Муаммо фақат компьютер ўғирланишидаги йўқотишларда эмас, балки ахборот тизимининг бузилиши катта зарарга олиб келиши мумкин. Ундан ташқари, ноутбуклар дастурий боғланиш (мобил компьютерларда сақланувчи пароллар ёрдамида) орқали корпоратив тармоқдан фойдаланишни тез-тез амалга оширади. Бу муаммоларни кичик, арзон ва катта энергия талаб этмайдиган бармоқ излари датчиклари ечишга имкон беради. Бу қурилмалар мос дастурий таъминот ёрдамида ахборотдан фойдаланишнинг мобил компьютерда сақланаётган тўртта сатҳи – рўйхатга олиш, экранни сақлаш режимидан чиқиш, юклаш ва файлларни дешифрациялаш учун аутентификацияни бажаришга имкон беради.

Фойдаланувчини биометрик аутентификациялаш махфий калитдан фойдаланишни модул кўринишида шифрлашда жиддий аҳамиятга эга бўлиши мумкин. Бу модул ахборотдан фақат хақиқий хусусий калит эгасининг фойдаланишига имкон беради. Сўнгра калит эгаси ўзининг махфий калитини ишлатиб хусусий тармоқлар ёки Internet орқали узатилаётган ахборотни шифрлаши мумкин.

6.1. Тармоқлараро экранларнинг ишлаш хусусиятлари

Тармоқлараро экран (ТЭ) - *брандмауэр ёки firewall системаси* деб ҳам аталувчи тармоқлараро химоянинг ихтисослаштирилган комплекси. Тармоқлараро экран умумий тармоқни икки ёки ундан кўп қисмларга ажратиш ва маълумот пакетларини чегара орқали умумий тармоқнинг бир қисмидан иккинчисига ўтиш шартларини белгиловчи қоидалар тўпламини амалга ошириш имконини беради. Одатда, бу чегара корхонанинг корпоратив (локал) тармоғи ва Internet глобал тармоқ орасида ўтказилади. Тармоқлараро экранлар гарчи корхона локал тармоғи уланган корпоратив интра тармоғидан қилинувчи хужумлардан химоялашда ишлатилишлари мумкин бўлсада, одатда, улар корхона ички тармоғини Internet глобал тармоқдан сукилиб киришдан химоялайди. Аксарият тижорат ташкилотлари учун тармоқлараро экранларнинг ўрнатилиши ички тармоқ хавфсизлигини таъминлашнинг зарурий шarti ҳисобланади.



6.1-расм. Тармоқлараро экранни улаш схемаси.

Рухсат этилмаган тармоқлараро фойдаланишга қарши таъсир кўрсатиш учун тармоқлараро экран ички тармоқ ҳисобланувчи

ташкилотнинг химояланувчи тармоғи ва ташки ганим тармок орасида жойланиши лозим (6.1-расм). Бунда бу тармоклар орасидаги барча алоқа факат тармоклараро экран орқали амалга оширилиши лозим. Ташкилий нуқтаи назаридан тармоклараро экран химояланувчи тармоқ таркибига киради.

Ички тармокнинг кўпгина узелларини бирданига химояловчи тармоклараро экран куйидаги иккита вазифани бажариши керак:

– ташки (химояланувчи тармоқка нисбатан) фойдаланувчиларнинг корпоратив тармокнинг ички ресурсларидан фойдаланишини чегаралаш. Бундай фойдаланувчилар каторига тармоклараро экран химояловчи маълумотлар базасининг серверидан фойдаланишга уринувчи шериклар, масофадаги фойдаланувчилар, хакерлар, ҳатто компаниянинг ходимлари киритилиши мумкин;

– химояланувчи тармоқдан фойдаланувчиларнинг ташки ресурслардан фойдаланишларини чегаралаш. Бу масаланинг ечилиши, масалан, сервердан хизмат вазифалари талаб этмайдиган фойдаланишни тартибга солишга имкон беради.

Ҳозирда ишлаб чиқарилаётган тармоклараро экранларнинг тавсифларига асосланган ҳолда, уларни куйидаги асосий аломатлари бўйича туркумлаш мумкин:

OSI модели сатҳларида ишлаши бўйича:

– пакетли филтър (экранловчи маршрутизатор – screening router);

– сеанс сатҳи шлюзи (экранловчи транспорт);

– татбикий шлюз (application gateway);

– эксперт сатҳи шлюзи (stateful inspection firewall).

Ишлатиладиган технология бўйича:

– протокол ҳолатини назоратлаш (Stateful inspection);

– воситачилар модуллари асосида (проху);

Бажарилиши бўйича:

– аппарат-дастурий;

– дастурий;

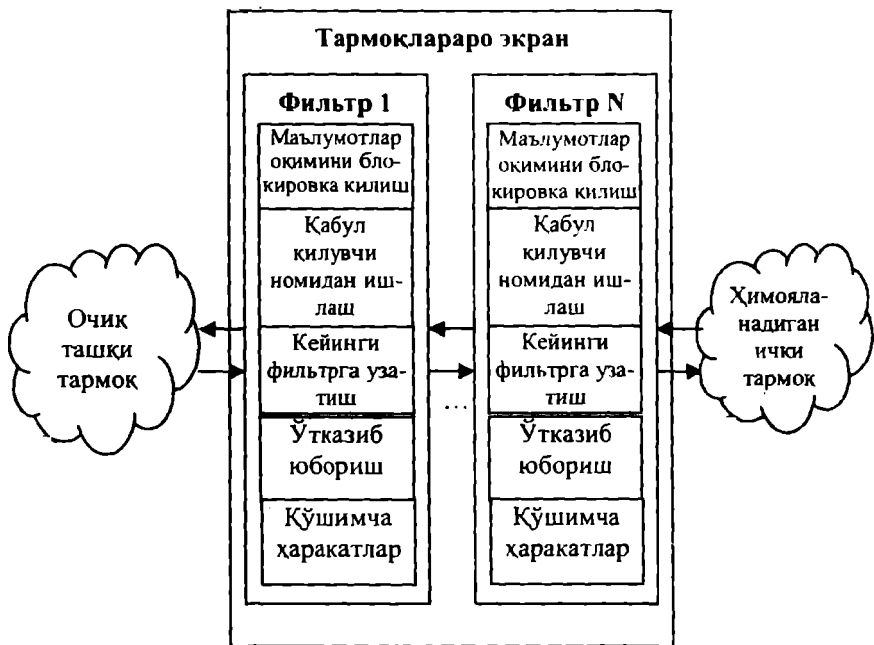
Уланиш схемаси бўйича:

– тармокни умумий химоялаш схемаси;

– тармок сегментлари химояланувчи берк ва тармок сегментлари химояланмайдиган очик схема;

– тармокнинг берк ва очик сегментларини алоҳида химояловчи схема.

Трафикларни филтрлаш. Ахборот оқимларини филтрлаш уларни экран орқали, баъзида қандайдир ўзгартиришлар билан, ўтказишдан иборат. Филтрлаш қабул қилинган хавфсизлик сиёсатига мос келувчи, экранга олдиндан юкланган қоидалар асосида амалга оширилади. Шу сабабли тармоқлараро экранни ахборот оқимларини ишловчи филтрлар кетма-кетлиги сифатида тасаввур этиш қулай (6.2-расм).



6.2-расм. Тармоқлараро экран тузилмаси.

Филтрларнинг ҳар бири қуйидаги ҳаракатларни бажариш орқали филтрлашнинг алоҳида қоидаларини изоҳлашга аталган:

1. Ахборотни изоҳланувчи қоидалардаги берилган мезонлар бўйича таҳлиллаш, масалан, қабул қилувчи ва жўнатувчи манзиллари ёки ушбу ахборот аталган илова хили бўйича.

2. Изоҳланувчи қоидалар асосида қуйидаги ечимлардан бирини қабул қилиш:

– маълумотларни ўтказмаслик;

– маълумотларни қабул қилувчи номидан ишлаш ва натижани жўнатувчига қайтариш;

– таҳлиллашни давом эттириш учун маълумотларни кейинги филътрга узатиш;

– кейинги филътрларга эътибор килмай маълумотларни узатиш.

Филътрлаш коидалари воситачилик функцияларига оид кўшимча, масалан, маълумотларни ўзгартириш, ходисаларни кайдлаш ва ҳ. каби ҳаракатларни ҳам бериши мумкин. Мас ҳолда, филътрлаш коидалари, куйидагиларнинг амалга оширилишини таъминловчи шартлар рўйхатини аниқлайди:

– маълумотларни кейинги узатишга рухсат бериш ёки рухсат бермаслик;

– химоялашнинг кўшимча функцияларини бажариш.

Ахборот оқимини таҳлиллаш мезони сифатида куйидаги параметрлардан фойдаланиш мумкин:

– таркибида тармоқ манзиллари, идентификаторлар, интерфейслар манзили, портлар рақами ва бошқа муҳим маълумотлар бўлган хабар пакетларининг хизматчи хошиялари;

– масалан, компьютер вируслари борлигига текширилувчи хабар пакетларининг бевосита таркиби;

– ахборот оқимининг ташки характеристикалари, масалан, вақт ва частота характеристикалари маълумотлар ҳажми ва ҳ.

Ишлатилувчи таҳлиллаш мезонлари филътрлашни амалга оширувчи OSI моделининг сатҳларига боғлиқ. Умумий ҳолда, пакетни филътрлашни амалга оширувчи OSI моделининг сатҳи канчалик юқори бўлса, таъминланувчи химоялаш даражаси ҳам шунчалик юқори бўлади.

Воситачилик функцияларининг бажарилиши. Тармоқлараро экран воситачилик функцияларини экранловчи агентлар ёки воситачи дастурлар деб аталувчи махсус дастурлар ёрдамида бажаради. Бу дастурлар резидент дастурлар ҳисобланади ва ташки ва ички тармоқ орасида хабарлар пакетини бевосита узатишни тақиклайди.

Ташки тармоқдан ички тармоқнинг ва аксинча фойдаланиш зарурияти туғилганда аввал тармоқлараро экран компьютерида ишловчи воситачи-дастур билан мантикий уланиш ўрнатилиши лозим. Воситачи-дастур сўралган тармоқлараро алоқанинг жоизлигини текширади ва ижобий натижада, ўзи сўралган компьютер билан алоҳида уланиш ўрнатади. Сўнгра ташки ва ички тармоқ компью-

терлари орасида ахборот алмашиш, хабарлар оқимини филтрлаш-ни ҳамда бошқа химоялаш функцияларини бажарувчи дастурий воситачи орқали амалга оширилади.

Таъкидлаш лозимки, тармоқлараро экран филтрлаш функциясини воситачи-дастур иштирокисиз амалга ошириб, ташқи ва ички тармоқ орасида ўзаро алоканинг шаффофлигини таъминлаши мумкин. Шу билан бирга воситачи дастурлар хабарлар оқимини филтрлашни амалга оширмаслиги ҳам мумкин.

Умуман, воситачи-дастурлар, хабарлар оқимини шаффоф узатилишини блокировка қилган ҳолда, қуйидаги функцияларни бажариши мумкин:

– узатилувчи ва қабул қилинувчи маълумотларнинг ҳақиқийлигини текшириш;

– ички тармоқ ресурсларидан фойдаланишни чегаралаш;

– ташқи тармоқ ресурсларидан фойдаланишни чегаралаш;

– ташқи тармоқдан сўралувчи маълумотларни кэшлаш;

– хабарлар оқимини филтрлаш ва ўзгартириш, масалан, вирусларни динамик тарзда кидириш ва ахборотни шаффоф шифрлаш;

– фойдаланувчиларни идентификациялаш ва аутентификациялаш;

– ички тармоқ манзилларини трансляциялаш;

– ходисаларни қайдлаш, ходисаларга реакция кўрсатиш ҳамда қайдланган ахборотни таҳлиллаш ва ҳисоботларни генерациялаш.

Узатишувчи ва қабул қилинувчи маълумотларнинг ҳақиқий-лигини текшириш нафақат электрон хабарларни, балки сох-талаштирилиши мумкин бўлган миграцияланувчи дастурларни (Java, Active X Controls) аутентификациялаш учун долзарб ҳисобланади. Хабар ва дастурларнинг ҳақиқийлигини текшириш уларнинг рақамли имзосини текширишдан иборатдир.

Ички тармоқ ресурсларидан фойдаланишни чегаралаш усуллари операцион тизим сатҳида мададланувчи чегаралаш усулларида фарқ қилмайди.

Ташқи тармоқ ресурсларидан фойдаланишни чегарлашда кўпинча қуйидаги ёндашишлардан бири ишлатилади:

– фақат ташқи тармоқдаги берилган манзил бўйича фойдаланишга руҳсат бериш;

– янгиланувчи ножиоз манзиллар рўйхати бўйича сўровларни филтёрлаш ва ўринсиз калит сўзлари бўйича ахборот ресурсларини кидиришни блокировка қилиш:

– маъмур томонидан ташки тармокнинг конуний ресурсларини брендмауэрнинг диски хотирасида тўплаш ва янгилаш ва ташки тармокдан фойдаланишни тўла тақиклаш.

Ташки тармокдан сўралувчи *маълумотларни хэшлаш* махсус воситачилар ёрдамида мададланади. Ички тармок фойдаланувчилари ташки тармок ресурсларидан фойдаланганларида барча ахборот, ргоху-сервер деб аталувчи брендмауэр қаттик диски маконида тўпланади. Шу сабабли, агар навбатдаги сўровда керакли ахборот ргоху-серверда бўлса, воситачи уни ташки тармокка мурожаатсиз тақдим этади. Бу фойдаланишни жиддий тезлаштиради. Маъмурга факат ргоху-сервер таркибини вақти-вақти билан янгилаб туриш вазифаси қолади.

Хэшлаш функцияси ташки тармок ресурсларидан фойдаланишни чегаралашда муваффақиятли ишлатилиши мумкин. Бу ҳолда ташки тармокнинг барча конуний ресурслари маъмур томонидан ргоху-серверда тўпланади ва янгиланади. Ички тармок фойдаланувчиларига факат ргоху-сервернинг ахборот ресурсларидан фойдаланишга рухсат берилади, ташки тармок ресурсларидан бевосита фойдаланиш эса ман қилинади.

Хабарлар оқимини филтёрлаш ва ўзгартириш воситачи томонидан қоидаларнинг берилган тўплами ёрдамида бажарилади. Бунда воситачи-дастурларнинг икки хили фарқланади:

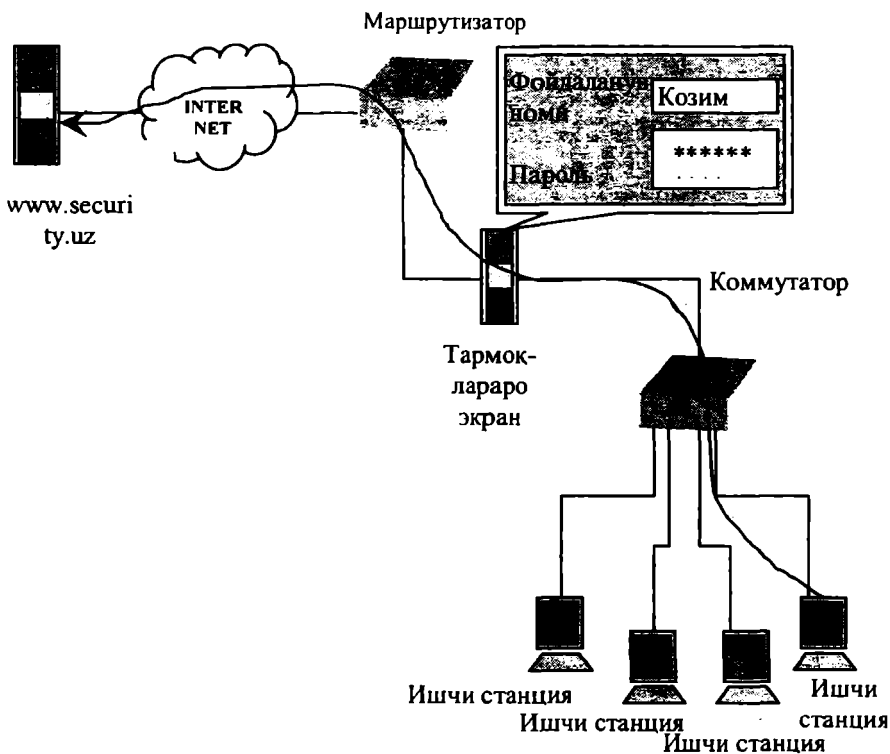
– сервис турини аниқлаш учун хабарлар оқимини таҳлиллашга мўлжалланган экранловчи агентлар, масалан, FTP, HTTP, Telnet;

– барча хабарлар оқимини ишловчи универсал экранловчи агентлар, масалан, компьютер вирусларини кидириб зарарсизлантиришга ёки маълумотларни шаффоф шифрлашга мўлжалланган агентлар.

Дастурий воситачи унга келувчи маълумотлар пакетини таҳлиллайди ва агар қандайдир объект берилган мезонларга мос келмаса, воситачи унинг кейинги силжишини блокировка қилади ёки мос ўзгаришини, масалан, ошкор қилинган компьютер вирусларни зарарсизлантиришни бажаради. Пакетлар таркибини

тахлиллашда экранловчи агентнинг ўтувчи файлли архивларни автоматик тарзда оча олиши муҳим ҳисобланади.

Фойдаланувчиларни идентификациялаш ва аутентификациялаш баъзида оддий идентификаторни (исм) ва паролни тақдим этиш билан амалга оширилади (6.3-расм). Аммо бу схема хавфсизлик нуқтаи назаридан заиф ҳисобланади, чунки паролни бегона шахс ушлаб қолиб ишлатиши мумкин. Internet тармоғидаги кўпгина можаролар қисман анъанавий кўп марта ишлатилувчи паролларнинг заифлигидан келиб чиққан.



6.3-расм. Пароль бўйича фойдаланувчини аутентификациялаш схемаси.

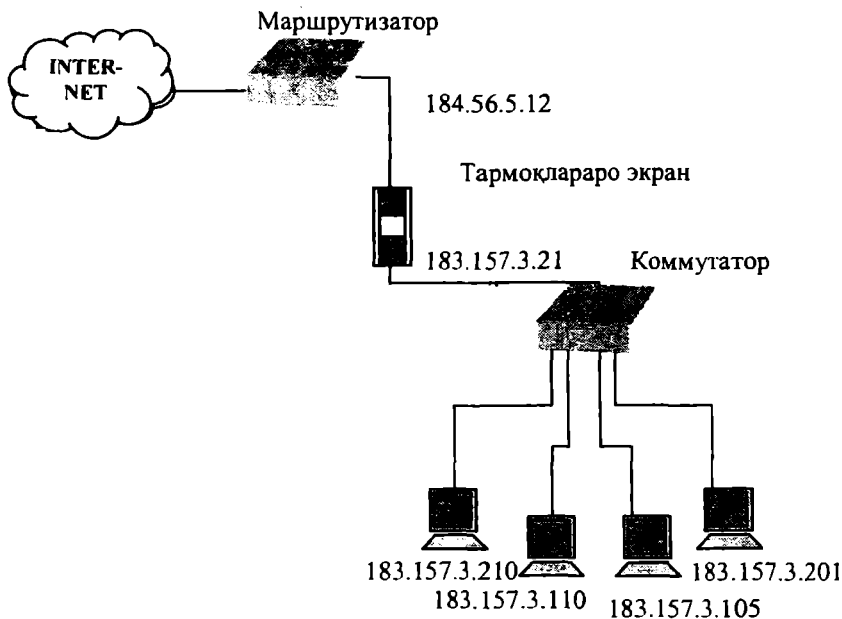
Аутентификациялашнинг ишончлироқ усули – бир марта ишлатилувчи пароллардан фойдаланишдир. Бир мартали паролларни генерациялашда аппарат ва дастурий воситалардан фойдаланилади. Аппарат воситалари компьютернинг слотига ўрнатилувчи курилма бўлиб, уни ишга тушириш учун фойдаланувчи қандайдир махфий ахборотни билиши зарур. Масалан, смарт-карта ёки фойдаланувчи токени ахборотни генерациялайди ва бу ахборотни хост аъъанавий парол ўрнида ишлатади. Смарт-карта ёки токен хостнинг аппарат ва дастурий таъминоти билан бирга ишлаши сабабли, генерацияланувчи парол ҳар бир сеанс учун ноёб бўлади.

Ишончли орган, масалан, калитларни тақсимлаш маркази томонидан берилувчи рақамли сертификатларни ишлатиш ҳам қулай ва ишончли. Кўпгина воситачи дастурлар шундай ишлаб чиқиладики, фойдаланувчи фақат тармоқлараро экран билан ишлаш сеансининг бошида аутентификациялансин. Бундан кейин маъмур белгиланган вақт мобайнида ундан кўшимча аутентификацияланиш талаб этилмайди.

Тармоқлараро экранлар тармоқдан фойдаланишни бошқаришни марказлаштиришлари мумкин. Демак, улар кучайтирилган аутентификациялаш дастурлари ва курилмаларини ўрнатишга муносиб жой ҳисобланади. Гарчи кучайтирилган аутентификация воситалари ҳар бир хостда ишлатилиши мумкин бўлсада, уларнинг тармоқлараро экранларда жойлаштириш қулай. Кучайтирилган аутентификациялаш чораларидан фойдаланувчи тармоқлараро экранлар бўлмаса, Telnet ёки FTP каби иловаларнинг аутентификацияланмаган трафиғи тармоқнинг ички тизимларига тўғридан-тўғри ўтиши мумкин.

Қатор тармоқлараро экранлар аутентификациялашнинг кенг тарқалган усулларида бири – Kerberosни мададлайди. Одатда, аксарият тижорат тармоқлараро экранлар аутентификациялашнинг гурли схемаларини мададлайди. Бу эса тармоқ хавфсизлиғи маъмурига ўзининг шароитига қараб энг мақбул схемани танлаш имконини беради.

Ички тармоқ манзилларини трансляциялаш. Кўпгина хужумларни амалга оширишда нияти бузук одамга қурбонининг манзилини билиш керак бўлади. Бу манзилларни ҳамда бутун тармоқ топологиясини беркитиш учун тармоқлараро экранлар энг муҳим вазифани – ички тармоқ манзилларини трансляциялашни бажаради (6.4-расм).



6.4-расм. Тармоқ манзилларини трансляциялаш.

Бу функция ички тармоқдан ташқи тармоққа узатилувчи барча пакетларга нисбатан бажарилади. Бундай пакетлар учун жўнатувчи компьютерларнинг IP-манзиллари битта «ишончли» IP манзилга автоматик тарзда ўзгартирилади.

Ички тармоқ манзилларини трансляциялаш иккига усул-динамик ва статик усулларда амалга оширилиши мумкин. Динамик усулда манзил узелга тармоқлараро экранга мурожаат онда ажратилади. Уланиш тугалланганидан сўнг манзил бўшайди ва уни қор-

поратив тармоқнинг бошқа узели ишлатиши мумкин. Статик усулда узел манзили барча чикувчи пакетлар узатиладиган тармоқлараро экраннинг битта манзилига доимо боғланади. Тармоқлараро экраннинг IP- манзили ташки тармоққа тушувчи ягона фаол IP- манзилга айланади. Натижада, ички тармоқдан чикувчи барча пакетлар тармоқлараро экрандан жўнатилган бўлади. Бу авторизацияланган ички тармоқ ва хавфли бўлиши мумкин бўлган ташки тармоқ орасида тўғридан-тўғри алокани истисно қилади.

Бундай ёндашишда ички тармоқ топологияси ташки фойдаланувчилардан яширинган, демак, рухсатсиз фойдаланиш масаласи кийинлашади. Манзилларни трансляциялаш тармоқ ичида ташки тармоқ, масалан, Internetдаги манзиллаш билан келишилмаган манзиллашнинг хусусий тизимига эга бўлишига имкон беради. Бу ички тармоқнинг манзил маконини кенгайтириш ва ташки манзил танқислиги муаммосини самарали ечади.

Ҳодисаларни қайдлаш, ҳодисаларга реакция кўрсатиш ҳамда қайдланган ахборотни таҳлиллаш ва ҳисоботларни генерациялаш тармоқлараро экранларнинг муҳим вазифалари ҳисобланади. Корпоратив тармоқни ҳимоялаш тизимининг жиддий элементи сифатида тармоқлараро экран барча ҳаракатларни рўйхатга олиш имкониятига эга. Бундай ҳаракатларга нафақат тармоқ пакетларини ўтказиб юбориш ёки блокировка қилиш, балки хавфсизлик маъмури томонидан фойдаланишни чегирилиши коидасини ўзгартириш ва ҳ. ҳам тааллуқли. Бундай рўйхатга олиш зарурият туғилганда (хавфсизлик можароси пайдо бўлганда ёки суд инстанцияларига ёки ички тергов учун далилларни йиғишда) яратилувчи журналларга мурожаат этишга имкон беради.

Шубҳали ходисалар (alarm) хусусидаги сигналларни қайдлаш тизими тўғри созланганида тармоқлараро экран ўзи ёки тармоқ ҳужумга дучор бўлганлиги ёки зондланганлиги тўғрисидаги батафсил ахборотни бериши мумкин. Тармоқдан фойдаланиш ва унинг зондланганлигининг исботи статистикасини йиғиш қатор сабабларга кўра муҳимдир. Аввало, тармоқлараро экраннинг зондланишга ва ҳужумларга бардошлигини аниқ билиш зарур ва тармоқлараро экранни ҳимоялаш тадбирларининг адекватлигини аниқлаш лозим. Ундан ташқари, тармоқдан фойдаланиш статистикаси тармоқ асбоб-ускуналарига ва дастурларига талабларни ифодалаш мақсадида хавф-хатарни тадқиқлаш ва таҳлиллашда дастлабки маълумотлар сифатида муҳим ҳисобланади.

Кўпгина тармоқлараро экранлар статистикани қайдловчи, йиғувчи ва таҳлилловчи қувватли тизимга эга. Миждоз ва сервер

манзили, фойдаланувчилар идентификатори, сеанс вақтлари, ула-ниш вақтлари, узатилган ва қабул қилинган маълумотлар сони, маъмур ва фойдаланувчилар ҳаракатлари бўйича ҳисоб олиб бори-лиши мумкин. Ҳисоб тизимлари статистикани таҳлиллашга имкон беради ва маъмурларга батафсил ҳисоботларни тақдим этади. Тармоқ-лараро экранлар махсус протоколлардан фойдаланиб, маълум ходисалар тўғрисида реал вақт режимида масофадан хабар беришни бажариши мумкин.

Рухсатсиз ҳаракатларни қилишга уринишларни аниқланишига бўладиган мажбурий реакция сифатида маъмурнинг хабари, яъни огоҳлантирувчи сигналларни бериш белгиланиши лозим. Хужум қилинганлиги аниқланганда огоҳлантирувчи сигналларни юбо-ришга қодир бўлмаган тармоқлараро экранни тармоқлараро химоянинг самарали воситаси деб бўлмайди.

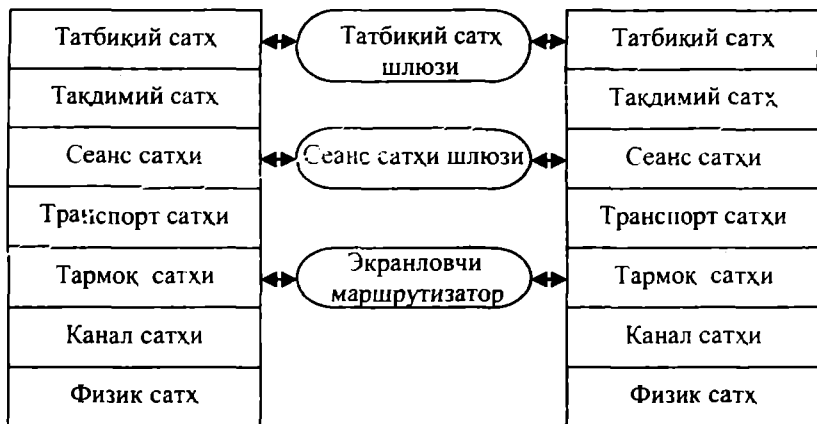
6.2. Тармоқлараро экранларнинг асосий компонентлари

Тармоқлараро экранлар тармоқлараро алоқа хавфсизлигини OSI моделининг турли сатҳларида мададлайди. Бунда эталон мо-делнинг турли сатҳларида бажариладиган химоя функциялари бир-биридан жиддий фаркланади. Шу сабабли, тармоқлараро экранлар комплексини, ҳар бири OSI моделининг алоҳида сатҳига мўлжалланган, бўлинмайдиган экранлар мажмуи кўринишида та-саввур этиш мумкин.

Экранлар комплекси кўпинча эталон моделнинг тармоқ, сеанс, татбикий сатҳларида ишлайди. Мос ҳолда, қуйидаги бўлинмайдиган брендмауэрлар фаркланади (6.5-расм).

- экранловчи маршрутизатор;
- сеанс сатҳи шлюзи (экрaнловчи транспорт);
- татбикий сатҳ шлюзи (экрaнловчи шлюз).

Тармоқларда ишлатиладиган протоколлар (TCP/IP, SPX/IPX) OSI эталон моделига батамом мос келмайди, шу сабабли санаб ўтилган экранлар хили функцияларини амалга оширишда эталон моделининг қўшни сатҳларини ҳам қамраб олишлари мумкин. Ма-салан, татбикий экран хабарларнинг ташқи тармоққа узатилишида уларни автоматик тарзда шифрлашни ҳамда қабул қилинувчи, криптографик беркитилган маълумотларни автоматик тарзда рас-шифровка қилишни амалга ошириши мумкин. Бу ҳолда бундай эк-ран OSI моделининг нафакат татбикий сатҳида, балки тақдимий сатҳида ҳам ишлайди.



6.5-рас.м. OSI моделининг алоҳида сатҳларида ишлайдиган тармоқлараро экранлар тури.

Сеанс сатҳи шлюзи ишлашида OSI моделининг транспорт ва тармоқ сатҳларини камраб олади. Экрaнловчи маршрутизатор хабарлар пакетини таҳлиллашда уларнинг нафақат тармоқ, балки транспорт сатҳи сарлавҳаларини ҳам текширади.

Ўқорида келтирилган тармоқлараро экранларнинг хиллари ўзининг афзалликлари ва камчиликларига эга. Ишлатиладиган брандмауэрларнинг кўпчилиги ёки татбикий шлюзлар ёки экранловчи маршрутизаторлар бўлиб, тармоқлараро алоканинг тўлиқ хавфсизлигини таъминламайди. Ишончли ҳимояни эса фақат ҳар бири экранловчи маршрутизатор, сеанс сатҳи шлюзи ҳамда татбикий шлюзни бирлаштирувчи тармоқлараро экранларнинг комплекси таъминлайди.

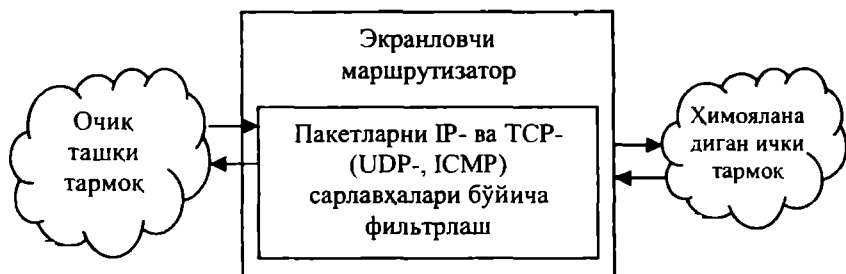
Экрaнловчи маршрутизатор (screening router) (пакетли фильтр packet filter деб ҳам аталади) хабарлар пакетини филтрлашга аталган ва ички ва ташқи тармоқлар орасида шаффоф алокани таъминлайди. У OSI моделининг тармоқ сатҳида ишлайди, ammo ўзининг айрим функцияларини бажаришида эталон моделининг транспорт сатҳини ҳам камраб олиши мумкин.

Маълумотларни ўтказиш ёки яроқсиз ҳолга чиқариш хусусидаги қарор филтрлашнинг берилган қоидаларига биноан ҳар бир пакет учун мустақил қабул қилинади. Қарор қабул қилишда тармоқ ва

транспорт сатхлари пакетларининг сарлавҳалари таҳлил этилади (6.6-расм).

Ҳар бир пакетнинг IP- ва TCP/UDP – сарлавҳаларининг таҳлилланувчи хошиялари сифатида куйидагилар ишлатилиши мумкин:

- жўнатувчи манзили;
- қабул килувчи манзили;
- пакет хили;
- пакетни фрагментлаш байроғи;
- манба порти рақами;
- қабул килувчи порт рақами.



6.6-расм. Пакетли филтрни ишлаш схемаси.

Биринчи тўртга параметр пакетнинг IP-сарлавҳасига, кейингилари эса TCP-ёки UDP сарлавҳасига тааллуқли. Жўнатувчи ва қабул килувчи манзиллари IP-манзиллар ҳисобланади. Бу манзиллар пакетларни шакллантиришда тўлдирилади ва уни тармоқ бўйича узатганда ўзгармайди.

Пакет хили хошиясида тармоқ сатҳига мос келувчи ICMP протокол коди ёки таҳлилланувчи IP-пакет тааллуқли бўлган транспорт сатҳи протоколининг (TCP ёки UDP) коди бўлади.

Пакетни фрагментлаш байроғи IP-пакетлар фрагментлашининг борлиги ёки йўқлигини аниқлайди. Агар таҳлилланувчи пакет учун фрагментлаш байроғи ўрнатилган бўлса, мазкур пакет фрагментланган IP-пакетнинг қисм пакети ҳисобланади.

Манба ва қабул килувчи портлари рақамлари TCP ёки UDP драйвер томонидан ҳар бир жўнатиловчи хабар пакетларига қўшилади ва жўнатувчи иловасини ҳамда ушбу пакет аталган ило-

вани бир маънода идентификациялайди. Портлар номерлари бўйича филтрлаш имконияти учун юқори сатҳ протоколларига порт ракамларини ажратиш бўйича тармоқда қабул қилинган келишувни билиш лозим.

Ҳар бир пакет ишланишида экранловчи маршрутизатор берилган коидалар жадвалини, пакетнинг тўлиқ ассоциациясига мос келувчи коидани топгунича, кетма-кет кўриб чиқади. Бу ерда ассоциация деганда берилган пакет сарлавҳаларида кўрсатилган параметрлар мажмуи тушунилади. Агар экранловчи маршрутизатор жадвалдаги коидаларнинг бирортасига ҳам мос келмайдиган пакетни олса, у, хавфсизлик нуктаи назаридан, уни яроксиз холга келтирилади.

Пакетли филтрлар аппарат ва дастурий амалга оширилиши мумкин. Пакетли филтр сифатида оддий маршрутизатор ҳамда кирувчи ва чиқувчи пакетларни филтрлашга мослаштирилган, серверда ишловчи дастурдан фойдаланиш мумкин. Замонавий маршрутизаторлар ҳар бир порт билан бир неча ўнлаб коидаларни боғлаши ва киришда, ҳам чиқишда пакетларни филтрлаши мумкин.

Пакетли филтрларнинг камчилиги сифатида қуйидагиларни кўрсатиш мумкин. Улар хавфсизликнинг юқори даражасини таъминламайди, чунки фақат пакет сарлавҳаларини текширадилар ва кўпгина керакли функцияларни мададламайди. Бу функцияларга, масалан, охириги узелларни аутентификациялаш, хабарлар пакетларини криптографик беркитиш ҳамда уларнинг яхлитлигини ва ҳақиқийлигини текшириш киради. Пакетли филтрлар дастлабки манзилларни алмаштириб қўйиш ва хабарлар пакети таркибини рухсатсиз ўзгартириш каби кенг тарқалган тармоқ хужумларига заиф ҳисобланадилар. Бу хил бренд-мауэрларни «алдаш» кийин эмас – филтрлашга рухсат берувчи коидаларни кондирувчи пакет сарлавҳаларини шаклантириш кифоя.

Аммо, пакетли филтрларнинг амалга оширилишининг соддалиги, юқори унумдорлиги, дастурий иловалар учун шаффофлиги ва нарҳининг пастлиги, уларнинг ҳамма ерда тарқалишига ва тармоқ хавфсизлиги тизимининг мажбурий элементи каби ишлатилишига имкон яратди.

Сеанс сатҳи шлюзи, (экрaнловчи транспорт, деб ҳам юритилади) виртуал уланишларни назоратлашга ва ташки гармок билан ўзаро алоқа қилишда IP-манзилларни трансляциялашга аталган. У

OSI моделининг сеанс сатҳида ишлайди ва ишлаш жараёнида эталон моделнинг транспорт ва тармоқ сатҳларини ҳам камраб олади. Сеанс сатҳи шлюзининг химоялаш функциялари воситачилик функцияларига тааллуқли.

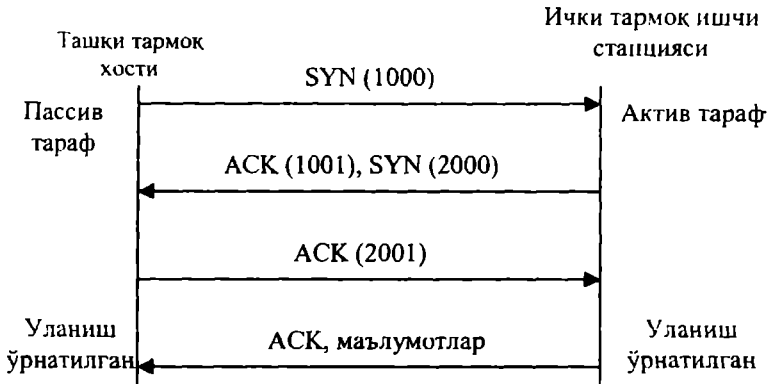
Виртуал уланишларнинг назорати алокани квитирилашни кузатишдан ҳамда ўрнатилган виртуал каналлар бўйича ахборот узатилишининг назоратлашдан иборат. Алокани квитирилашнинг назоратида сеанс сатҳида шлюз ички тармоқ ишчи станцияси ва ташқи тармоқ компьютери орасида виртуал уланишни кузатиб, сўралаётган алоқа сеансининг жоизлигини аниқлайди.

Бундай назорат TCP протоколининг сеанс сатҳи пакетларининг сарлавҳасидаги ахборотга асосланади. Аммо TCP-сарлавҳаларни таҳлиллашда пакетли фильтр факат манба ва қабул қилувчи портларининг рақамини текширса, экранловчи транспорт алокани квитирилаш жараёнига тааллуқли бошқа ҳошияларни таҳлиллайди.

Алоқа сеансига сўровнинг жоизлигини аниқлаш учун сеанс сатҳи шлюзи қуйидаги ҳаракатларни бажаради. Ишчи станция (мижоз) ташқи тармоқ билан боғланишни сўраганида, шлюз бу сўровни қабул қилиб унинг филтёрлашнинг базавий мезонларини каноатлантиришини, масалан, сервер мижоз ва у билан ассоциацияланган исмнинг IP-манзилни аниқлай олишини текширади. Сўнгра шлюз, мижоз исмидан ҳаракат қилиб, ташқи тармоқ компьютери билан уланишни ўрнатади ва TCP протоколи бўйича квитирилаш жараёнининг бажарилишини кузатади.

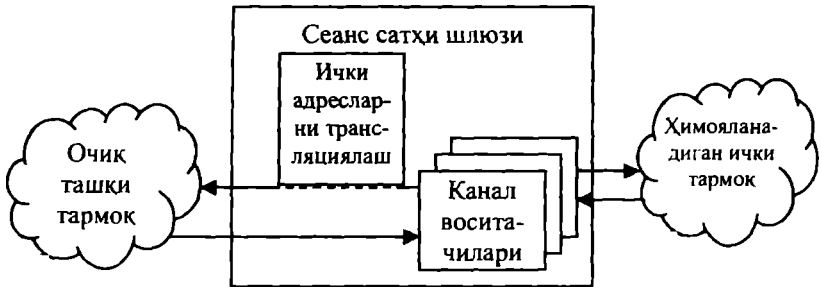
Бу муолажа SYN (синхронлаш) ва ACK (тасдиқлаш) байроқлари орқали белгиланувчи TCP-пакетларни алмашишдан иборат (6.7-расм).

SYN байроқ билан белгиланган ва таркибида ихтиёрий сон, масалан, 1000, бўлган TCP сеансининг биринчи пакети мижознинг сеанс очишга сўрови ҳисобланади. Бу пакетни олган ташқи тармоқ компьютери жавоб тариқасида ACK байроқ билан белгиланган ва таркибида олинган пакетдагидан биттага катта (бизнинг ҳолда 1001) сон бўлган пакетни жўнатади. Шу тариқа, мижоздан SYN пакети олинганлиги тасдиқланади. Сўнгра, тесқари муолажа амалга оширилади: ташқи тармоқ компьютери ҳам мижозга узатилувчи маълумотлар биринчи байтининг тартиб рақами билан (масалан, 2000) SYN пакетини жўнатади, мижоз эса уни олганлигини, таркибида 2001 сони бўлган пакетни узатиш орқали тасдиқлайди. Шу билан алокани квитирилаш жараёни тугалланади.



6.7-расм. TCP протоколи бўйича алоқани квитишлаш схемаси.

Сеанс сатҳи шлюзи (6.8-расм) учун сўралган сеанс жоиз ҳисобланади, қачонки алоқани квитишлаш жараёни бажарилишида SYN ва ACK байроқлар ҳамда TCP-пакетлари сарлавҳаларидаги сонлар ўзаро мантикий боғланган бўлса.



6.8-расм. Сеанс сатҳи шлюзи ишлаш схемаси.

Ички тармоқнинг ички станцияси ва ташқи тармоқнинг компютери TCP сеансининг авторизацияланган қатнашчилари эканлиги ҳамда ушбу сеансининг жоизлиги тасдиқланганидан сўнг шлюз

улашишни ўрнатади. Бунда шлюз улашишларининг махсус жадвалига мос ахборотни (жўнатувчи ва қабул қилувчи манзиллари, улашиш ҳолати, кетма-кетлик рақами хусусидаги ахборот ва х.) кирилади.

Шу ондан бошлаб шлюз пакетларни нусхалайди ва иккала томонга йўналтириб, ўрнатилган виртуал канал бўйича ахборот узатилишини назорат қилади. Ушбу назорат жараёнида сеанс сатҳи шлюзи пакетларни филтрламайди. Аммо у узатиувчи ахборот сонини назорат қилиши ва қандайдир чегарадан ошганида улашишни узиши мумкин. Бу эса, ўз навбатида, ахборотнинг рухсатсиз экспорт қилинишига тўсик бўлади. Виртуал улашишлар хусусидаги қайдлаш ахборотининг тўпланиши ҳам мумкин.

Сеанс сатҳи шлюзларида виртуал улашишларни назоратлашда канал *воситачилари* (pipe proxy) деб юритилувчи махсус дастурлардан фойдаланилади. Бу воситачилар ички ва ташқи тармоқлар орасида виртуал каналларни ўрнатади, сўнгра TCP/IP иловалари генерациялаган пакетларнинг ушбу канал орқали узатилишини назоратлайди.

Канал воситачилари TCP/IPнинг муайян хизматларига мўлжалланган. Шу сабабли ишлаши муайян иловаларнинг воситачи-дастурларига асосланган татбиқий сатҳ шлюзлари имкониятларини кенгайтиришда сеанс сатҳ шлюзларидан фойдаланиш мумкин.

Сеанс сатҳи шлюзи ташқи тармоқ билан ўзаро алоқада тармоқ сатҳи ички манзилларини (IP-манзилларини) трансляциялашни ҳам таъминлайди. Ички манзилларни трансляциялаш ички тармоқдан ташқи тармоққа жўнатиувчи барча пакетларга нисбатан бажарилади.

Амалга оширилиши нуктаи назаридан сеанс сатҳи шлюзи етарлича оддий ва нисбатан ишончли дастур ҳисобланади. У экранловчи маршрутизаторни виртуал улашишларни назоратлаш ва ички IP-манзилларни трансляциялаш функциялари билан тўлдиради.

Сеанс сатҳи шлюзининг камчиликлари – экранловчи маршрутизаторларнинг камчиликларига ўхшаш. Ушбу технологиянинг яна бир жиддий камчилиги маълумотлар хошиялари таркибини назоратлаш мумкин эмаслиги. Натижада, нияти бузук одамларга зарар келтирувчи дастурларни ҳимояланувчи тармоққа узатиш имконияти туғилади. Ундан ташқари, TCP-сессиясининг (TCP hijacking)

ушлаб қолিনিшида нияти бузук одам хужумларини хатто рухсат берилган сессия доирасида амалга ошириши мумкин.

Амалда аксарият сеанс сатҳ шлюзлари мустақил маҳсулот бўлмай, татбиқий сатҳ шлюзлари билан комплекта тақдим этилади.

Татбиқий сатҳ шлюзи (экранловчи шлюз деб ҳам юритилади) OSI моделининг татбиқий сатҳида ишлаб, тақдимий сатҳни ҳам камраб олади ва тармоқлараро алоканинг энг ишончли химоясини таъминлайди. Татбиқий сатҳ шлюзининг химоялаш функциялари, сеанс сатҳи шлюзига ўхшаб, воситачилик функцияларига тааллуқли. Аммо, татбиқий сатҳ шлюзи сеанс сатҳи шлюзига караганда химоялашнинг анча кўп функцияларини бажариши мумкин:

- брандмауэр орқали уланишни ўрнатишга уринишда фойдаланувчиларни идентификациялаш ва аутентификациялаш;

- шлюз орқали узатилувчи ахборотнинг хақиқийлигини текшириш;

- ички ва ташқи тармоқ ресурсларидан фойдаланишни чегаралаш;

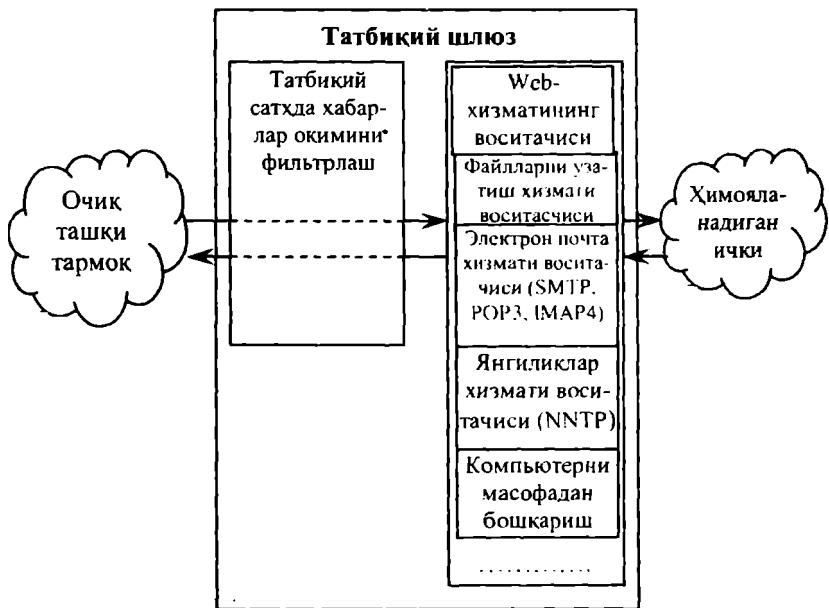
- ахборотлар оқимини филтрлаш ва ўзгартириш, масалан, вирусларни динамик тарзда кидириш ва ахборотни шаффоф шифрлаш;

- ходисаларни қайдлаш, ходисаларга реакция кўрсатиш ҳамда қайдланган ахборотни таҳлиллаш ва ҳисоботларни генерациялаш;

- ташқи тармоқдан сўралувчи маълумотларни кэшлаш.

Татбиқий сатҳ шлюзи функциялари воситачилик функцияларига тааллуқли бўлганлиги сабабли, бу шлюз универсал компьютер ҳисобланади ва бу компьютерда ҳар бир хизмат кўрсатилувчи татбиқий протокол (HTTP, FTP, SMTP, NNTP ва х.) учун битгадан воситачи дастур (экранловчи агент) ишлатилади. TCP/IPнинг ҳар бир хизматининг воситачи дастури (application proxy) айнан шу хизматга тааллуқли хабарларни ишлашга ва химоялаш функцияларини бажаришга мўлжалланган.

Татбиқий сатҳ шлюзи мос экранловчи агентлар ёрдамида кичувчи ва чиқувчи пакетларни ушлаб қолади, ахборотни нусха тайди ва қайта жўнатади, яъни ички ва ташқи тармоқлар орасидаги тўғридан-тўғри уланишни истисно қилган ҳолда, сервер-воситачи функциясини бажаради (6.9-расм).



6.9-расм. Татбикий шлюз ишлаш схемаси.

Татбикий сатҳ шлюзи ишлатадиган воситачилар сеанс сатҳи шлюзларининг канал воситачиларидан жиддий фаркланади. Биринчидан, татбикий сатҳ шлюзлари муайян иловалар (дастурий серверлар) билан боғланган, иккинчидан улар OSI моделининг татбикий сатҳида хабарлар оқимини филтрлашлари мумкин.

Татбикий сатҳ шлюзлари воситачи сифатида мана шу мақсадлар учун махсус ишлаб чиқилган TCP/IPнинг муайян хизматларининг дастурий серверлари – HTTP, FTP, SMTP, NNTP ва х. – серверларидан фойдаланади. Бу дастурий серверлар брандмауэрларда резидент режимда ишлайди ва TCP/IPнинг мос хизматларига тааллуқли химоялаш функцияларини амалга оширади. UDP трафигига UDP-пакетлар таркибининг махсус транслятори хизмат кўрсатади.

Ички тармок ишчи сервери ва ташқи тармок компьюттери орасида иккита уланиш амалга оширилади: ишчи станциядан брандмауэргача ва брандмауэрдан белгиланган жойгача. Канал воситачиларидан фарқли холда, татбикий сатҳ шлюзининг воситачилари факат ўзлари хизмат килувчи иловалар генерациялаган пакетларни

ўтказди. Масалан, HTTP хизмагининг воситачи-дастури фақат шу хизмат генерациялаган графикани ишлайди.

Агар қандайдир иловада ўзининг воситачиси бўлмаса, татбикий сатҳдаги шлюз бундай иловани ишлай олмайди ва у блокировка қилинади. Масалан, агар татбикий сатҳдаги шлюз фақат HTTP, FTP ва Telnet воситачи-дастурларидан фойдаланса, у фақат шу хизматларга тегишли пакетларни ишлайди ва қолган хизматларнинг пакетларини блокировка қилади.

Татбикий сатҳ шлюзи воситачилари. канал воситачиларидан фарқли ҳолда, ишланувчи маълумотлар таркибини текширишни таъминлайди. Улар ўзлари хизмат кўрсатадиган татбикий сатҳ протоколларидаги командаларнинг алоҳида хилларини ва хабарлардаги ахборотларни филтрлашлари мумкин.

Татбикий сатҳ шлюзини сошлашда ва хабарларни филтрлаш қондаларини тавсифлашда қуйидаги параметрлардан фойдаланилади: сервис номи, ундан фойдаланишнинг жойиз вақт оралиғи, ушбу сервисга боғлиқ хабар таркибига чегаралашлар, сервис ишлатадиган компьютерлар, фойдаланувчи идентификатори, аутентификациялаш схемалари ва ҳ.

Татбикий сатҳ шлюзи қуйидаги афзалликларга эга:

- аксарият воситачилик функцияларини бажара олиши туфайли локал тармоқ химоясининг юқори даражасини таъминлайди;

- иловалар сатҳида химоялаш кўпгина қўшимча текширишларни амалга оширишга имкон беради, натижада, дастурий таъминот камчиликларига асосланган муваффақиятли хужумлар ўтказиш эҳтимоллиги камаяди;

- татбикий сатҳ шлюзининг ишга даёқатлиги бузилса, бўлинувчи тармоқлар орасида пакетларнинг тўппа-тўғри ўтиши блокировка қилинади, натижада, рад қилиниши туфайли химояланувчи тармоқнинг хавфсизлиги пасаймайди.

Татбикий сатҳ шлюзининг камчиликларига қуйидагилар қиради:

- нархининг нисбатан юқорилиги;
- брандмауэрнинг ўзи ҳамда уни ўрнатиш ва конфигурациялаш муолажаси етарлича мураккаб;
- компьютер платформаси унумдорлигига ва ресурслари ҳажмига қўйиладиган талабларнинг юқорилиги;

– фойдаланувчилар учун шаффофликнинг йўқлиги ва тармоқлараро алоқа ўрнатилишида ўтказиш қобилиятининг сусайиши.

Охирги камчиликка батафсил тўхталамиз. Воситачилар сервер ва мижоз орасида пакетлар узатилишида оралик ролини бажаради. Аввал воситачи билан уланиш ўрнатилади, сўнгра воситачи манзилат билан уланишни яратиш ёки яратмаслик хусусида қарор қабул қилади. Мас ҳолда татбиқий сатҳ шлюзи ишлаши жараёнида ҳар қандай рухсат этилган уланишни қайталайди. Натижада, фойдаланувчилар учун шаффофлик йўқолади ва уланишга хизмат қилишга кўшимча харажат сарфланади.

Эксперт сатҳи шлюзи. Татбиқий сатҳ шлюзининг фойдаланувчилар учун шаффофлигининг йўқлиги ва тармоқлараро алоқа ўрнатилишида ўтказиш қобилиятининг сусайиши каби жиддий камчиликларини бартараф этиш мақсадида пакетларни филтрлашнинг янги технологияси ишлаб чиқилган. Бу технологияни баъзида уланиш ҳолатини назоратлашли филтрлаш (stateful inspection) ёки эксперт сатҳидаги филтрлаш деб юритишади. Бундай филтрлаш пакетлар ҳолатини кўп сатҳли тахлиллашнинг махсус усуллари (SMLT) асосида амалга оширилади.

Ушбу гибрид технология тармоқ сатҳида пакетларни ушлаб қолиш ва ундан уланишни назорат қилишда ишлатилувчи татбиқий сатҳ ахборотини чиқариб олиш орқали уланиш ҳолатини кузатишга имкон беради.

Ишлаши асосини ушбу технология ташкил этувчи тармоқлараро экран *эксперт сатҳ брандмауэри* деб юритилади. Бундай брандмауэрлар ўзида экранловчи маршрутизаторлар ва татбиқий сатҳ шлюзлари элементларини уйғунлаштиради. Улар ҳар бир пакет таркибини берилган хавфсизлик сиёсатиға мувофиқ баҳолайдилар.

Шундай қилиб эксперт сатҳидаги брандмауэрлар куйидагиларни назоратлашга имкон беради:

– мавжуд қондалар жадвали асосида ҳар бир узатилувчи пакетни;

– ҳолатлар жадвали асосида ҳар бир сессияни;

– ишлаб чиқилган воситачилар асосида ҳар бир иловани.

Эксперт сатҳ тармоқлараро экранларининг афзалликлари сифатида уларнинг фойдаланувчилар учун шаффофлигини, ахборот

окимини ишлашининг юкори тезкорлигини ҳамда улар оркали ўтувчи пакетларнинг IP-манзилларини ўзгартирмаслигини кўрсатиш мумкин. Охирги афазаллик. IP-манзилдан фойдаланувчи татбикий сатҳнинг ҳар қандай протоколининг бундай брендмауэрлардан ҳеч қандай ўзгаришсиз ёки махсус дастурлашсиз бирга ишлай олишини англатади.

Бундай брендмауэрларнинг авторизацияланган мижоз ва ташқи тармок компютери орасида тўғридан-тўғри уланишга йўл кўйиши, ҳимоянинг унчалик юкори бўлмаган даражасини таъминлайди. Шу сабабли амалда эксперт сатҳини филтрлаш технологиясидан комплекс брендмауэрлар ишлаши самарадорлигини оширишда фойдаланилади. Эксперт сатҳнинг филтрлаш технологиясини ишлатувчи комплекс брендмауэрларга мисол тарикасида Fire Wall-1 ва ON Guard ларни кўрсатиш мумкин.

6.3. Тармоқлараро экранлар асосидаги тармок ҳимоясининг схемалари

Тармоқлараро алоқани самарали ҳимоялаш учун брендмауэр тизими тўғри ўрнатилиши ва конфигурацияланиши лозим. Ушбу жараён қуйидагиларни ўз ичига олади:

- тармоқлараро алоқа сиёсатини шакллантириш;
- брендмауэрни улаш схемасини танлаш ва параметрларини сошлаш.

Тармоқлараро алоқа сиёсатини шакллантириш

Тармоқлараро алоқа сиёсатини шакллантиришда қуйидагиларни аниқлаш лозим:

- тармок сервисларидан фойдаланиш сиёсати;
- тармоқлараро экран ишлаши сиёсати.

Тармок сервисларидан фойдаланиш сиёсати ҳимояланувчи компютер тармокнинг барча сервисларини тақдим этиш ҳамда улардан фойдаланиш қоидаларини белгилайди. Ушбу сиёсат доирасида тармок экрани орқали тақдим этилувчи барча сервислар ва ҳар бир сервис учун мижозларнинг жоиз манзиллари берилиши лозим. Ундан ташқари, фойдаланувчилар учун қачон ва қайси фойдаланувчилар қайси сервисдан ва қайси компютерда фойдаланишларини тавсифловчи қоидалар кўрсатилиши лозим. Фойдаланиш усулларига чегаралашлар ҳам берилади. Бу чегаралашлар фойдаланувчиларнинг Internet нинг ман этилган сервисларидан айланма йўл

орқали фойдаланишларига йўл кўймаслик учун зарур. Фойдаланувчилар ва компьютерларни аутентификациялаш қодалари ҳамда ташкилот локал тармоғи ташқарисидаги фойдаланувчиларнинг ишлаш шароитлари алоҳида белгиланиши лозим.

Тармоқлараро экран ишлаши сиёсатида тармоқлараро алокани бошқаришнинг брандмауэр ишлаши асосидаги базавий принципи берилади. Бундай принципларнинг қуйидаги иккитасида» бири танланиши мумкин:

- ошқора рухсат этилмагани ман қилинган;
- ошқора ман этилмаганига рухсат берилган.

«Ошқора рухсат этилмагани ман қилинган» принципи танланганида тармоқлараро экран шундай созланадики, ҳар қандай рухсат этилмаган тармоқлараро алоқалар блокировка қилинади. Ушбу принцип ахборот хавфсизлигининг барча соҳаларида ишлатилувчи фойдаланишнинг мумтоз моделига мос келади. Бундай ёндашиш, имтиёزلарни минималлаштириш принципини адекват амалга оширишга имкон бериши сабабли, хавфсизлик нуқтаи назаридан яхшироқ ҳисобланади. Моҳияти бўйича «ошқора рухсат этилмагани ман қилинган» принципи билмаслик зарар келтириши фактини эътироф этишдир. Таъқидлаш лозимки, ушбу принципга асосан таърифланган фойдаланиш қодалари фойдаланувчиларга маълум ноқулайликлар туғдириши мумкин.

«Ошқора ман этилмаганига рухсат берилган» принципи танланганида тармоқлараро экран шундай созланадики, фақат ошқора ман этилган тармоқлараро алоқалар блокировка қилинади. Бу ҳолда, фойдаланувчилар томонидан тармоқ сервисларидан фойдаланиш қулайлиги ошади, аммо тармоқлараро алоқа хавфсизлиги пасаяди. Фойдаланувчиларнинг тармоқлараро экранни четлаб ўтишларига имкон туғилади, масалан улар сиёсат ман қилмаган (ҳатто, сиёсатда кўрсатилмаган) янги сервисларидан фойдаланишлари мумкин. Ушбу принцип амалга оширилишида ички тармоқ хакерларнинг ҳужумларидан камроқ химояланган бўлади. Шу сабабли, тармоқлараро экранларни ишлаб чиқарувчи-лари одатда, ушбу принципдан фойдаланмайдилар.

Тармоқлараро экран симметрик эмас. Унга ички тармоқнинг ташқи тармоқдан ва аксинча фойдаланишни чегараловчи қодалар алоҳида берилади. Умумий ҳолда, тармоқлараро экраннинг иши қуйидаги иккита гуруҳ функцияларни динамик тарзда бажаришга асосланган:

- у орқали ўтаётган ахборот окимини филтрлаш;
- тармоқлараро алоқа амалга оширилишида воситачилик.

Оддий тармоқлараро экранлар бу функцияларнинг бирини бажаришга мўлжалланган. Комплекс тармоқлараро экранлар химоялашнинг кўрсатилган функцияларининг биргаликда бажарилишини таъминлайди.

Тармоқлараро экранларни улашнинг асосий схемалари.

Корпоратив тармоқни глобал тармоқларга улаганда химояланувчи тармоқнинг глобал тармоқдан ва глобал тармоқнинг химояланувчи тармоқдан фойдаланишини чегаралаш ҳамда уланувчи тармоқдан глобал тармоқнинг масофадан рухсатсиз фойдаланишидан химоялашни таъминлаш лозим. Бунда ташкилот ўзининг тармоғи ва унинг компонентлари хусусидаги ахборотни глобал тармоқ фойдаланувчиларидан беркитишга манфаатдор. Масофадаги фойдаланувчилар билан ишлаш химояланувчи тармоқ ресурсларидан фойдаланишнинг катъий чегараланишини талаб этади.

Ташкилотдаги корпоратив тармоқ таркибида кўпинча химояланишнинг турли сатхли бир неча сегментларга эга бўлиши эҳтиёжи туғилади:

- бемалол фойдаланилувчи сегментлар (масалан, реклама WWW-серверлари);
- фойдаланиш чегараланган сегментлар (масалан, ташкилотнинг масофадаги узеллари ходимларининг фойдаланиши учун);
- ёпик сегментлар (масалан, ташкилотнинг молия локал қисм тармоғи).

Тармоқлараро экранларни улашда турли схемалардан фойдаланиш мумкин. Бу схемалар химояланувчи тармоқ ишлаши шароитига ҳамда ишлатиладиган брендмауэрларнинг тармоқ интерфейслари сонига ва бошқа характеристикаларига боғлиқ. Тармоқлараро экранни улашнинг қуйидаги схемалари кенг тарқалган:

- экранловчи маршрутизатордан фойдаланилган химоя схемалари;
- локал тармоқни умумий химоялаш схемалари;
- химояланувчи ёпик ва химояланмайдиган очик қисм тармоқли схемалар;
- ёпик ва очик қисм тармоқларни алоҳида химояловчи схемалар.

Экранловчи маршрутизатордан фойдаланилган химоя схемаси.

Пакетларни филтрлашга асосланган тармоқлараро экран кенг таркалган ва амалга оширилиши осон. У химояланувчи тармоқ ва бўлиши мумкин бўлган ганим очик тармоқ орасида жойлашган экранловчи маршрутизатордан иборат (6.10-расм).



6.10-расм. Тармоқлараро экран – экранловчи маршрутизатор.

Экранловчи маршрутизатор (пакетли филтр) кирувчи ва чиқувчи пакетларни уларнинг манзиллари ва портлари асосида блокировка қилиш ва филтрлаш учун конфигурацияланган.

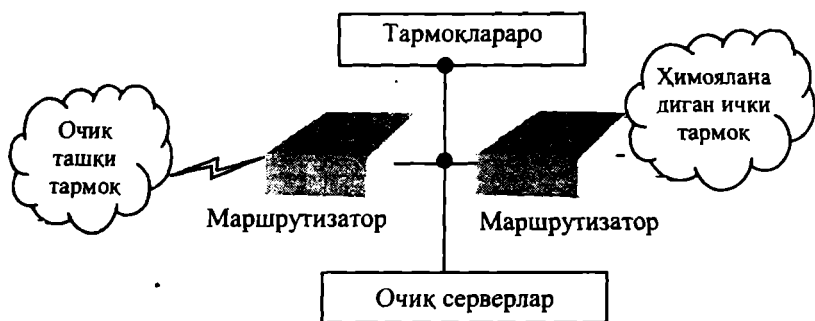
Химояланувчи тармоқдаги компьютерлар Internetдан тўғридан-тўғри фойдаланаолади, Internetнинг улардан фойдаланишининг кўп қисми эса блокировка қилинади. Умуман, экранловчи маршрутизатор юқорида тавсифланган химоялаш сиёсатидан исталганини амалга ошириши мумкин. Аммо, агар маршрутизатор пакетларни манба порти ва кириш йўли ва чиқиш йўли портлари рақами бўйича филтрламаса, «ошқора рухсат этилмагани ман қилинган» сиёсатини амалга ошириш қийинлашади.

Пакетларни филтрлашга асосланган тармоқлараро экраннинг камчиликлари куйидагилар:

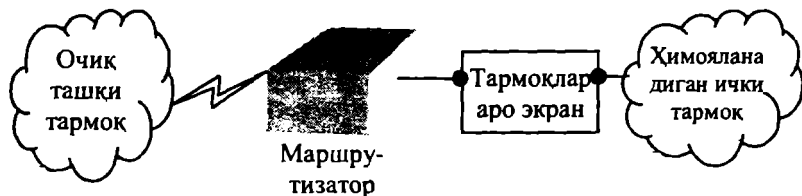
- филтрлаш коидаларининг мураккаблиги; баъзи ҳолларда бу коидалар мажмуи бажарилмаслиги мумкин;
- филтрлаш коидаларини тўлиқ тестлаш мумкин эмаслиги; бу тармоқни тестланмаган хужумлардан химояланмаслигига олиб келади;
- ҳодисаларни рўйхатга олиш имкониятининг йўқлиги; натижада маъмурга маршрутизаторнинг хужумга дуч келганлигини ва обрўсизлантирилганлигини аниқлаш қийинлашади.

Локал тармоқни умумий химоялаш схемалари. Битта тармоқ интерфейсли брендмауэрлардан фойдаланилган химоялаш схема-

лари (6.11-расм) хавфсизлик ва конфигурациялашнинг қулайлиги нуктаи назаридан самарасиз ҳисобланади. Улар ички ва ташқи тармоқларни физик ажратмайдилар, демак, тармоқлараро алоқанинг ишончли ҳимоясини таъминлай олмайдилар.



6.11-расм. Битта тармоқ интерфейсли firewall ёрдамида локал тармоқни ҳимоялаш.



6.12-расм. Локал тармоқни умумий ҳимоялаш схемаси.

Локал тармоқни умумий ҳимоялаш схемаси энг оддий ечим бўлиб, унда брандмауэр локал тармоқни ташқи ғаним тармоқдан бутунлай экранлайди (6.12-расм). Маршрутизатор ва брандмауэр орасида фақат битта йўл бўлиб, бу йўл орқали бутун трафик ўтади. Брандмауэрнинг ушбу варианти «ошқора рухсат этилмагани ман қилинган» принципига асосланган ҳимоялаш сиёсатини амалга оширади. Одатда, маршрутизатор шундай созиладики, брандмауэр ташқаридан кўринадиган ягона машина бўлади.

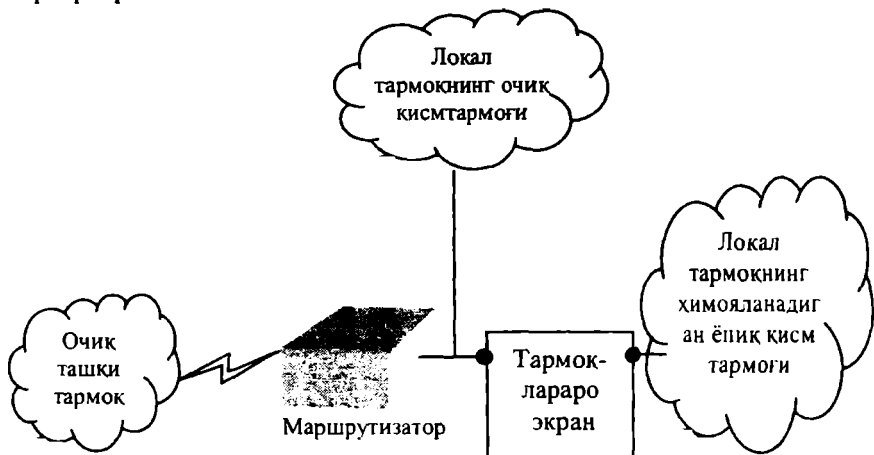
Локал тармоқ таркибидаги очик серверлар ҳам тармоқлараро экранлар томонидан ҳимояланади. Аммо, ташқи тармоқ фойдалана оладиган серверларни ҳимоялашувчи локал тармоқларнинг бошқа

ресурслари билан бирлаштириш тармоқлараро алоқа хавфсизлигини жиддий пасайтиради.

Тармоқлараро экран фойдаланадиган хостга фойдаланувчиларни кучайтирилган аутентификациялаш учун дастур ўранатилиши мумкин.

Ҳимояланувчи ёпиқ ва ҳимояланмайдиган очик қисм тармоқли схемалар. Агар локал тармоқ таркибида умумфойдаланувчи очик серверлар бўлса уларни тармоқлараро экрандан олдин очик қисм тармоқ сифатида чиқариш мақсадга мувофиқ ҳисобланади (6.13-расм).

Ушбу усул локал тармоқ ёпиқ қисмининг кучли ҳимояланишини, аммо тармоқлараро экрангача жойлашган очик серверларнинг пасайган ҳимояланишини таъминлайди.

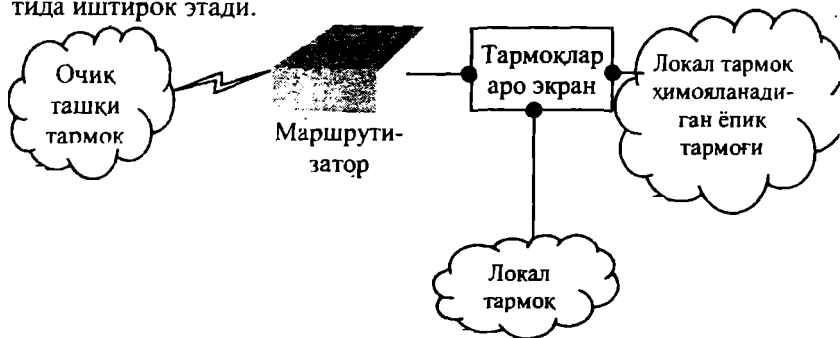


6.13-расм. Ҳимояланадиган ёпиқ ва ҳимояланмайдиган очик қисм тармоқли схема.

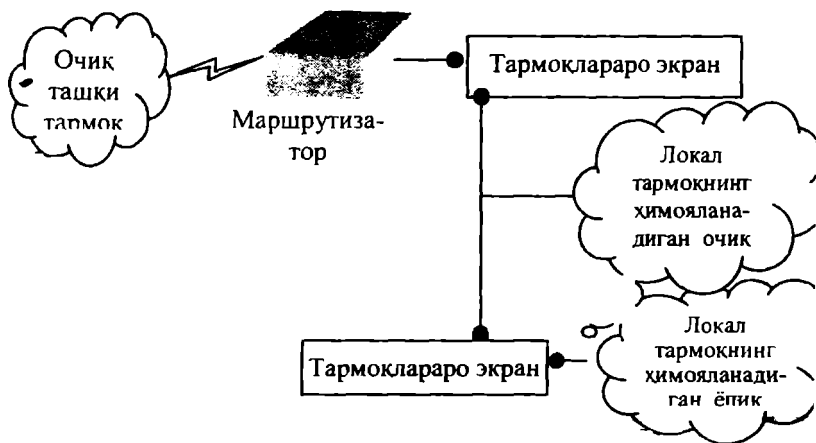
Баъзи брандмауэрлар бу серверларни ўзида жойлаштиради. Аммо бу брандмауэрнинг хавфсизлиги ва компьютернинг юкланиши нуқтаи назаридан яхши ечим ҳисобланмайди. Ҳимояланувчи ёпиқ ва ҳимояланмайдиган очик қисм тармоқли схемани очик қисм тармоқ хавфсизлигига қўйиладиган талабларнинг юқори бўлмаган ҳолларида ишлатилиши мақсадга мувофиқ ҳисобланади. Агар очик сервер хавфсизлигига юқори талаблар қўйилса, ёпиқ ва очик қисм тармоқларни алоҳида ҳимоялаш схемаларидан фойдаланиш зарур.

Ёпик ва очик қисм тармоқларни алоҳида ҳимояловчи схемалар. Бундай схемалар учта тармоқ интерфейсли битта брандмауэр (6.14-расм) ёки иккита тармоқ интерфейсли иккита брандмауэр (6.15-расм) асосида қурилиши мумкин. Иккала ҳолда ҳам очик ва ёпик қисм тармоқлардан фақат тармоқлараро экран орқали фойдаланиш мумкин. Бунда очик қисм тармоқдан фойдаланиш ёпик қисм тармоқдан фойдаланишга имкон бермайди.

Иккита брандмауэрли схема тармоқлараро алоқа хавфсизлигининг юқори даражасини таъминлайди. Бунда ҳар бир брандмауэр ёпик тармоқни ҳимоялашнинг алоҳида эшелонини ҳосил қилади, ҳимояланувчи очик қисм тармоқ эса экранловчи қисм тармоқ сифатида иштирок этади.



6.14 -расм. Учта тармоқ интерфейсли бир брандмауэр асосида ёпик ва очик қисм тармоқларни алоҳида ҳимоялаш схемаси.



6.15-расм. Иккита тармоқ интерфейсли иккита брандмауэр асосида ёпик ва очик қисм тармоқларни алоҳида ҳимоялаш схемаси.

Одатда, экранловчи қисм тармоқ шундай конфигурацияланадики, қисм тармоқ компютеридан ғаним ташқи тармоқ ва локал тармоқнинг ёпик қисм тармоғи фойдалана олсин. Аммо ташқи тармоқ ва ёпик қисм тармоқ орасида тўғридан-тўғри ахборот пакетларини алмашиш мумкин эмас. Экранловчи қисм тармоқли тизимни хужум қилишда, бўлмаганида химоянинг иккита мустақил қизигини босиб ўтишга тўғри келади. Бу эса жуда мураккаб масала ҳисобланади. Тармоқлараро экран ҳолатларини мониторинглаш воситалари бундай уринишни доимо аниқлаши ва тизим маъмури ўз вақтида руҳсатсиз фойдаланишга қарши зарурий чоралар кўриши мумкин.

Таъкидлаш лозимки, алоканинг коммутацияланувчи линияси орқали уланувчи масофадаги фойдаланувчиларнинг иши ҳам ташкилотда ўтказилувчи хавфсизлик сиёсатиға мувофиқ назорат қилиниши шарт. Бундай масаланинг намунавий ҳал этилиши – зарурий функционал имкониятларға эга бўлган масофадан фойдаланиш серверини (терминал серверни) ўрнатиш. Терминал сервер бир неча асинхрон портларға ва локал тармоқнинг битта интерфейсиға эга бўлган тизим ҳисобланади. Асинхрон портлар ва локал тармоқ орасида ахборот алмашиш фақат ташқи фойдаланувчини аутентификациялашдан кейин амалға оширилади.

Терминал серверни улаш шундай амалға ошириш лозимки, унинг иши фақат тармоқлараро экран орқали бажарилсин. Бу масофалаги фойдаланувчиларнинг ташкилот ахборот ресурслари билан ишлаш хавфсизлигининг керакли даражасини таъминлашға имкон беради.

Терминал серверни очик қисм тармоқ таркибига киритилганида бундай уланиш жоиз ҳисобланади. Терминал сервернинг дастурий таъминоти коммутацияланувчи каналлар орқали алоқа сеансларини маъмурлаш ва назоратлаш имкониятини таъминлаши лозим. Замонавий терминал серверларни бошқариш модуллари серверни ўзини хавфсизлигини таъминлаш ва мижозларнинг фойдаланишини чегаралаш бўйича етарлича ривожланган имкониятларға эга ва қуйидаги функцияларни бажаради:

- кетма-кет портлардан, PPP протоколи бўйича масофадан, ҳамда маъмур консолидан фойдаланишда локал паролни ишлатиш;
- локал тармоқнинг қандайдир машинасининг аутентификациялашға сўровидан фойдаланиш;

– аутентификациялашнинг ташки воситаларидан фойдаланиш;
– терминал сервери портларидан фойдаланишни назоратловчи рўйхатни ўрнатиш;

– терминал сервер оркали алоқа сеансларини протоколлаш.

Шахсий ва тақсимланган тармоқ экранлари. Охириги бир неча йил мобайнида корпоратив тармоқ тузилмасида маълум ўзгаришлар содир бўлди. Агар илгари бундай тармоқ чегараларини аниқ белгилаш мумкин бўлган бўлса, ҳозирда бу мумкин эмас. Яқиндаёқ бундай чегара барча маршрутизаторлар ёки бошқа қурилмалар (масалан, модемлар) оркали ўтар ва улар ёрдамида ташки тармоқларга чиқилар эди. Аммо ҳозирда тармоқлараро экран оркали ҳимояланувчи тармоқнинг тўла ҳужукли эгаси – ҳимояланувчи периметр ташқарисидаги ходим ҳисобланади. Бундай ходимлар сирасига уйдаги ёки меҳнат сафараридаги ходимлар киради. Шубҳасиз, уларга ҳам ҳимоя зарур. Аммо барча анъанавий тармоқлараро экранлар шундай қурилганки, ҳимояланувчи фойдаланувчилар ва ресурслар уларнинг ҳимоясида корпоратив ёки локал тармоқнинг ички томонида бўлишлари шарт. Бу эса мобил фойдаланувчилар учун мумкин эмас.

Бу муаммони ечиш учун қуйидаги ёндашишлар тақлиф этилган:

– тақсимланган тармоқлараро экранлардан (distributed firewall) фойдаланиш;

– виртуал хусусий тармоқ VPNлар имкониятидан фойдаланиш.

Тақсимланган тармоқлараро экран тармоқнинг алоҳида компьютерини ҳимояловчи марказдан бошқарилувчи тармоқ мини-экранлар мажмуидир.

Тақсимланган брандмауэрларнинг катор функциялари (масалан, марказдан бошқариш, хавфсизлик сиёсатини тарқатиш) шахсий фойдаланувчилар учун ортиқча бўлганлиги сабабли, тақсимланган брандмауэрлар модификацияланди. Янги ёндашиш *шахсий тармоқли экранлаш технологияси* номини олди. Бунда тармоқли экран ҳимояланувчи шахсий компьютерда ўрнатилади. Компьютернинг шахсий экрани (personal firewall) ёки тармоқли экранлаш тизими деб аталувчи бундай экран, бошқа барча тизимли ҳимоялаш воситаларига боғлиқ бўлмаган ҳолда бугун чиқувчи ва

кирувчи трафикни назоратлайди. Алоҳида компьютерни экранлашда тармок сервисдан фойдаланувчанлик мададланади, аммо ташки фаолликнинг юкланиши пасаяди. Натижада, шу тарика химояланувчи компьютер ички сервисларининг заифлиги пасаяди, чунки четки нияти бузук одам олдин, химоялаш воситалари синчиклаб ва катъий конфигурацияланган, экранни босиб ўтиши лозим.

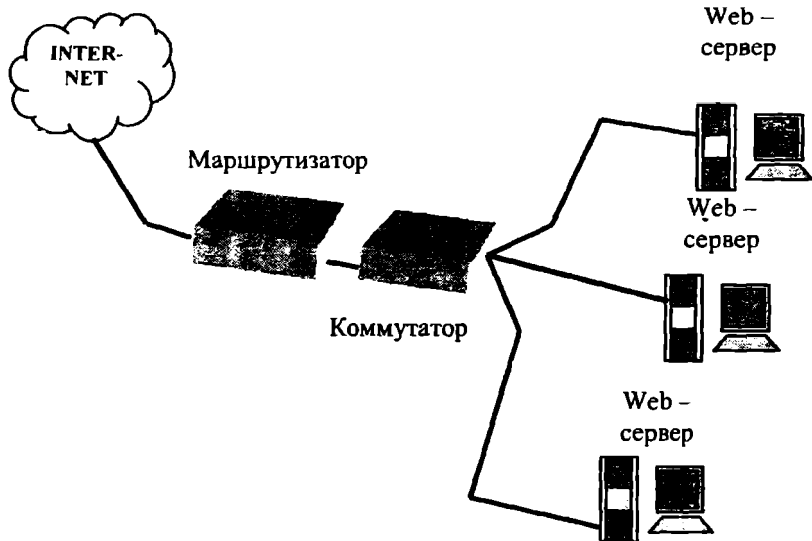
Таксимланган тармоқлараро экраннинг шахсий экрандан асосий фарқи-таксимланган тармоқлараро экранда марказдан бошқариш функциясининг борлиги. Агар шахсий тармоқли экранлар улар ўрнатилган компьютер орқали бошқарилса (уй шаронтида қўлланишга жуда мос), таксимланган тармоқлараро экранлар ташкилотнинг бош офисида ўрнатилган бошқаришнинг умумий консоли томонидан бошқарилиши мумкин.

Корпоратив тармок рухсатсиз фойдаланишдан хақиқатан ҳам химояланган ҳисобланади, қачонки, унинг Internetдан кириш нуктасида химоя воситалари ҳамда ташкилот локал тармоғи фрагментларини, корпоратив серверларини ва алоҳида компьютерлар хавфсизлигини таъминловчи ечимлар мавжуд бўлса. Таксимланган ёки шахсий тармоқлараро экран асосидаги ечимлар алоҳида компьютерлар, корпоратив серверлар ва ташкилот локал тармок фрагментлари хавфсизлигини таъминлашни аъло даражада бажаради.

Таксимланган тармоқлараро экранлар, аънавий тармоқлараро экранлардан фарқли равишда, кўшимча дастурий таъминот бўлиб, хусусан корпоратив серверларни, масалан, Internet-серверларни ишончли химоялаши мумкин. Корпоратив тармоқни химоялашнинг оқилона ечими – химоялаш воситасини у химоя килувчи сервери билан бир платформада жойлаштиришдир. 6.16-расмда корпоратив серверларни таксимланган тармоқлараро экранлар ёрдамида химоялаш схемаси келтирилган.

Аънавий ва таксимланган тармоқлараро экранларни куйидаги кўрсаткичлари бўйича таққослайлик.

Самарадорлик. Аънавий брандмауэр кўпинча тармок периметри бўйича жойлаштирилади, яъни у химоянинг бир катламини таъминлайди ҳолос. Агар бу ягона қатлам бузилса, тизим ҳарқандай хужумга бардош бераолмайди. Шахсий брандмауэр операция тизимнинг ядро сатҳида ишлайди ва барча кирувчи ва чикувчи пакетларни текшириб корпоратив серверларни ишончли химоялайди.



6.16 -расм. Таксимланган тармоқлараро экранлар ёрдамида корпоратив серверларни химоялаш.

Таксимланган брандмауэр дастурий таъминот бўлиб, санокли дақиқаларда ўрнатилади ва олиб ташланади.

Бошқариш. Анъанавий брандмауэр тармоқ маъмури томонидан бошқарилади. Таксимланган брандмауэр тармоқ маъмури ёки локал тармоқ фойдаланувчиси томонидан бошқарилиши мумкин.

Унумдорлик. Анъанавий брандмауэр тармоқлараро алашашишни таъминловчи қурилма бўлиб, унумдори (пакет/дақиқа бўйича) белгиланган чегараланишга эга. У бир-бири билан коммутацияланувчи маҳаллий тармоқ орқали боғланган ўсувчи сервер парклари учун тўғри келмайди. Таксимланган брандмауэр қабул қилинган хавфсизлик сиёсатига зиён етказмасдан сервер паркларини ўсишига имкон беради.

Нархи. Анъанавий брандмауэр, одатда, функциялари белгиланган, нархи етарлича юкори гизим ҳисобланади. Брандмауэрнинг таксимланган маҳсулотлари дастурий таъминот бўлиб, анъанавий тармоқлараро экранлар нархининг 1/5 ёки 1/10 га тенг.

VII боб. ҲИМОЯЛАНГАН ВИРТУАЛ ХУСУСИЙ ТАРМОҚЛАР

7.1. Ҳимояланган виртуал хусусий тармоқларни куриш концепцияси

Internet нинг гуриллаб ривожланиши нагижасида дунёда ахборотни тарқатиш ва фойдаланишда сифатий ўзгариш содир бўлди. Internet фойдаланувчилари арзон ва қулай коммуникацияга эга бўлдилар. Корхоналар Internet каналларидан жиддий тижорат ва бошқарув ахборотларини узатиш имкониятларига қизиқиб қолдилар. Аммо Internetнинг қурилиши принципи нияти бузук одамларга ахборотни ўғирлаш ёки атайин бузиш имкониятини яратди. Одатда, TCP/IP протоколлар ва стандарт Internet-иловалар (e-mail, Web, FTP) асосида қурилган корпоратив ва идора тармоқлари сукилиб киришдан қафолатланмаганлар.

Internetнинг ҳамма ерда тарқалишидан манфаат кўриш мақсадида тармоқ ҳужумларига самарали қаршилиқ кўрсатувчи ва бизнесда очик тармоқлардан фаол ва хавфсиз фойдаланишга имкон берувчи виртуал хусусий тармоқ VPN яратиш устида ишлар олиб борилди. Натижада, 1990 йилнинг бошида виртуал хусусий тармоқ VPN концепцияси яратилди. «Виртуал» ибораси VPN атамасига иккита узел ўртасидаги уланишни вақтинча деб кўрилишини таъкидлаш мақсадида киритилган. Ҳақиқатан, бу уланиш доимий, қатъий бўлмай, фақат очик тармоқ бўйича трафик ўтганида мавжуд бўлади.

Виртуал тармоқ VPNларни куриш концепцияси асосида етарлича оддий ғоя ётади: агар глобал тармоқда ахборот алмашинувчи иккита узел бўлса, бу узеллар орасида очик тармоқ орқали узатилаётган ахборотнинг конфиденциаллигини ва яхлитлигини таъминловчи виртуал химояланган туннел куриш зарур ва бу виртуал туннелдан барча мумкин бўлган ташқи фаол ва пассив кузатувчиларнинг фойдаланиши ҳаддан ташқари қийин бўлиши лозим.

Шундай қилиб, VPN туннели очик тармоқ орқали ўтказилган уланиш бўлиб, у орқали виртуал тармоқнинг криптографик химояланган ахборот пакетлари узатилади. Ахборотни VPN туннели бўйича узатилиши жараёнидаги химоялаш қуйидаги вазифаларни бажаришга асосланган:

- ўзаро алоқадаги тарафларни аутентификациялаш;
- узатилувчи маълумотларни криптографик беркитиш (шифрлаш);
- етказиладиган ахборотнинг ҳақиқийлигини ва яхлитлигини текшириш.

Бу вазифалар бир-бирига боғлиқ бўлиб, уларни амалга оширишда ахборотни криптографик химоялаш усулларидан фойдаланилади. Бундай химоялашнинг самарадорлиги симметрик ва асимметрик криптографик тизимларнинг биргаликда ишлатилиши эвазига таъминланади. VPN қурилмалари томонидан шакллантирилувчи VPN туннели химояланган ажратилган линия хусусиятларига эга бўлиб, бу химояланган ажратилган линиялар умумфойдаланувчи тармоқ, масалан, Internet доирасида, сафланади. VPN қурилмалари виртуал хусусий тармоқларда VPN-мижоз, VPN-сервер ёки VPN хавфсизлиги шлюзи вазифасини ўташи мумкин.

VPN-мижоз одатда шахсий компьютер асосидаги дастурий ёки дастурий-аппарат комплекси бўлиб, унинг тармоқ дастурий таъминоти у бошқа VPN-мижоз, VPN-сервер ёки VPN хавфсизлиги шлюзлари билан алмашинадиган трафикни шифрлаш ва аутентификациялаш учун модификацияланади. Одатда, VPN-мижознинг амалга оширилиши стандарт операцион тизим – Windows NT/2000 ёки Unixни тўлдирувчи дастурий ечимдан иборат бўлади.

VPN-сервер сервер вазифасини ўтовчи, компьютерга ўрнатилувчи дастурий ёки дастурий-аппарат комплексидан иборат. VPN-сервер ташқи тармоқларнинг рухсатсиз фойдаланишидан серверларни химоялашни ҳамда алоҳида компьютерлар ва мос VPN-маҳсулотлари орқали химояланган локал тармоқ сегментларидаги компьютерлар билан химояланган уланишларни ташкил этишни таъминлайди. VPN-сервер VPN-мижознинг сервер платформалари учун функционал аналог ҳисобланади. У аввало, VPN-мижозлар билан кўпгина уланишларни мададловчи кенгайтирилган ресурслари билан ажралиб туради. VPN-сервер мобил фойдаланувчилар билан уланишларни ҳам мададлаши мумкин.

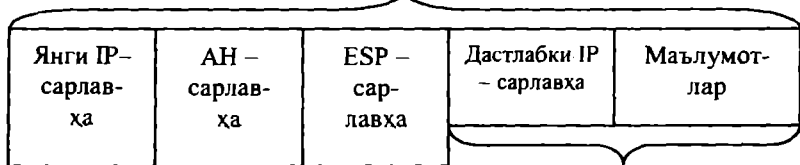
VPN хавфсизлик шлюзи. (Security gateway) иккита тармоққа уланувчи тармоқ қурилмаси бўлиб, ўзидан кейин жойлашган кўп сонли хостлар учун шифрлаш ва аутентификациялаш вазифаларини бажаради. VPN хавфсизлиги шлюзи шундай жойлаштириладики, ички корпоратив тармоққа аталган барча трафик у орқали ўтади. VPN хавфсизлиги шлюзининг манзили кирувчи туннелланувчи пакетнинг ташқи манзили сифатида кўрсатилади, пакетнинг ички манзили эса шлюз орқасидаги муайян хост манзили ҳисобланади. VPN хавфсизлиги шлюзи алоҳида дастурий ечим, алоҳида аппарат қурилмаси ҳамда VPN вазифалари билан гўлдирилган маршрутизаторлар ёки тармоқлараро экран кўринишида амалга оширилиши мумкин.

Ахборот узатишнинг очик ташқи муҳити маълумот узатишнинг тезкор каналларини (Internet муҳити) ва алоқанинг секин ишлайдиган умумфойдаланувчи каналларини (масалан, телефон тармоғи каналларини) ўз ичига олади. Виртуал хусусий тармоқ VPNнинг самарадорлиги алоқанинг очик каналлари бўйича айланувчи ахборотнинг химояланиш даражасига боғлиқ. Очик тармоқ орқали маълумотларни хавфсиз узатиш учун инкапсуляциялаш ва туннеллаш кенг ишлатилади. Туннеллаш усули бўйича маълумотлар пакети умумфойдаланувчи тармоқ орқали худди оддий икки нуктали уланиш бўйича узатилганидек узатилади. Ҳар бир «жўнатувчи-қабул қилувчи» жуфтлиги орасига бир протокол маълумотларини бошқасининг пакетига инкапсуляциялашга имкон берувчи ўзига хос туннел-манتيкий уланиш ўрнатилади.

Туннеллашга биноан, узатилувчи маълумотлар порцияси хизматчи хошиялар билан бирга янги «конверт»га «жойлаш» амалга оширилади. Бунда пастрок сатҳ протоколи пакети юкорирок ёки худди шундай сатҳ протоколи пакети маълумотлари майдонига жойлаштирилади. Таъкидлаш лозимки, туннеллашнинг ўзи маълумотларни руҳсатсиз фойдаланишдан ёки бузишдан химояламайди, аммо туннеллаш туфайли инкапсуляцияланувчи дастлабки пакетларни тўла криптографик химоялаш имконияти пайдо бўлади. Узатилувчи маълумотлар конфиденциаллигини таъминлаш мақсадида жўнатувчи дастлабки пакетларни шифрлайди, уларни, янги IP-сарлавҳа билан ташқи пакетга жойлайди ва транзит тармоқ бўйича жўнатади (7.1-расм).

Очик тармоқ бўйича маълумотларни ташишда ташқи пакет сарлавҳасининг очик каналларидан фойдаланилади.

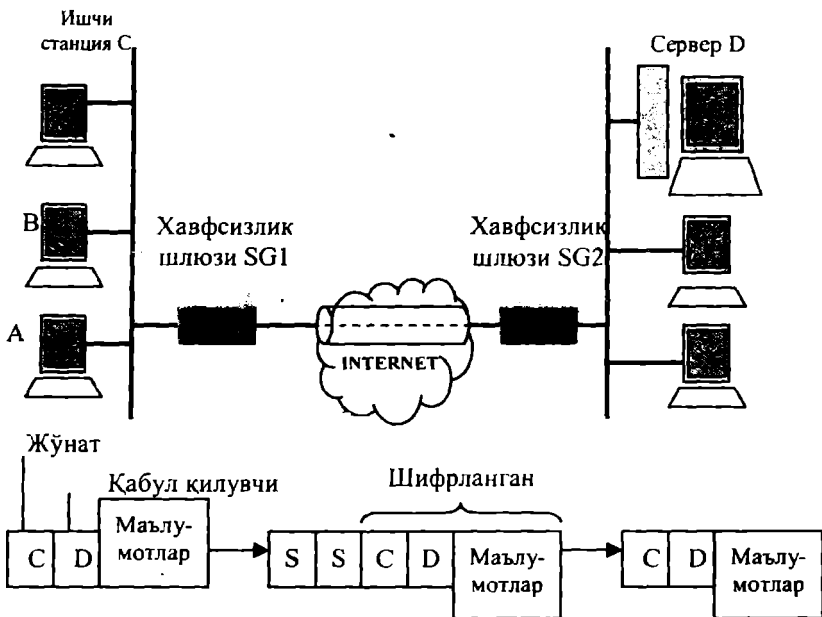
Янги пакет



Даствабки пакет

7.1-расм. Туннеллашга тайёрланган пакет мисоли.

Ташки пакет химояланган каналнинг охириги нуктасига келиши билан ундан ички даствабки пакет чиқариб олиниб, расшифровка қилинади ва унинг тикланган сарлавхаси ички тармоқ бўйича кейинги узатиш учун ишлатилади (7.2-расм).



7.2-расм. Виртуаль химояланган туннел схемаси.

Туннеллашдан пакет таркибини нафақат конфиденциаллигини, балки унинг яхлитлигини ва аутентлигини таъминлашда фойдала-

нилади. Бунда электрон рақамли имзони пакетнинг барча хошияларига таркатиш мумкин.

Internet билан боғланмаган локал тармоқ яратилганда компания ўзининг тармоқ қурилмалари ва компьютерлари учун хоҳлаган IP-манзилдан фойдаланиши мумкин. Олдин яққаланган тармоқларни бирлаштиришда бу манзиллар бир-бирлари ва Internetда ишлатилаётган манзиллар билан тўқнашишлари мумкин. Пакетларни инкапсуляциялаш бу муаммони ечади, чунки у дастлабки манзилларни беркитишга ва Internet IP - манзиллари мақонидаги ноёб манзилларни қўшишга имкон беради. Бу манзиллар кейин маълумотларни ажратилувчи тармоқлар бўйича узатишда ишлатилади. Бунга локал тармоққа уланувчи мобил фойдаланувчиларнинг IP-манзилларини ва бошқа параметрларини сошлаш масаласи ҳам киради.

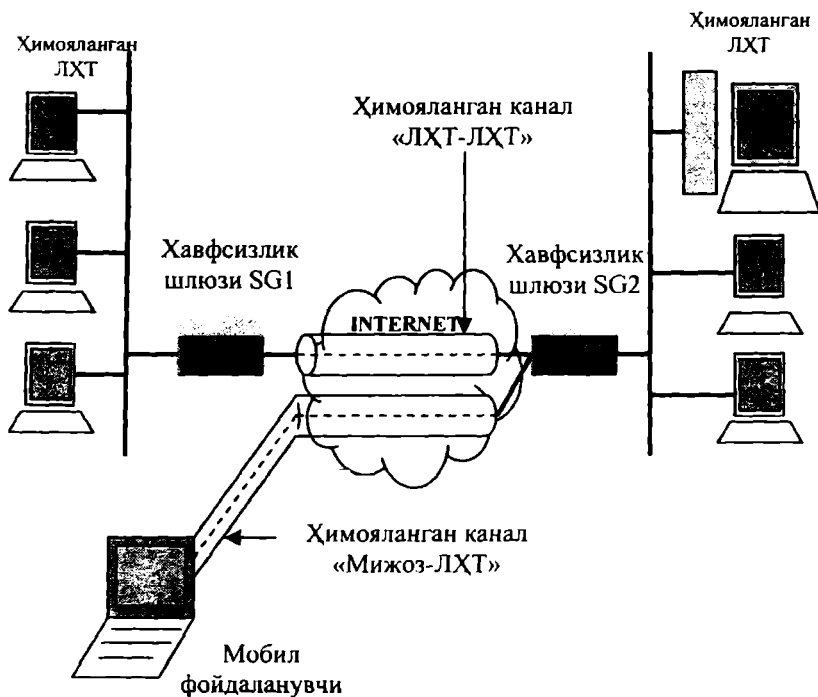
Туннеллаш механизми ҳимояланувчи канални шакллантирувчи турли протоколларда кенг қўлланилади. Одатда, туннел фақат маълумотларнинг конфиденциаллиги ва яхлитлигининг бузилиши хавфи мавжуд бўлган очик тармоқ қисмида, масалан, очик Internet ва корпоратив тармоқ кириш нукталари орасида, яратилади. Бунда ташки пакетлар учун ушбу икки нуктада ўрнатилган чегара маршрутизаторларининг манзилларидан фойдаланилса, охириги узелларнинг ички манзиллари ички дастлабки пакетларда ҳимояланган ҳолда сақланади. Таъкидлаш лозимки, туннеллаш механизмининг ўзи қандай мақсадларда туннеллаш қўлланилаётганига боғлиқ эмас. Туннеллаш нафақат узатилаётган барча маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлашда, балки турли протоколли (масалан, IPv4 ва IPv6) тармоқлар орасида ўтишни ташкил этишда ҳам қўлланилади. Туннеллаш бир протокол пакетини бошқа протоколдан фойдаланувчи мантикий муҳитда узатишни ташкил этишга имкон беради. Натижада, бир неча турли хил тармоқларнинг ўзаро алоқалари муаммосини ҳал этиш имконияти пайдо бўлади.

Туннеллаш механизмини амалга оширилишига уч хил протоколлар: протокол-«йўловчи», протокол элтувчи ва туннеллаш протоколи ишлаши натижаси деб қараш мумкин. Масалан, протокол – «йўловчи» сифатида битта корхона филиалларининг локал тармоқларида маълумотларни ташувчи транспорт протоколи IPX ишлатилиши мумкин. Элтувчи протоколнинг энг кўп тарқалган варианты Internet тармоғининг IP-протоколи ҳисобланади. Туннеллаш протоколи сифатида канал сатхи протоколари PPTP ва L2TP,

хамда тармоқ сатҳи протоколи IPSec ишлатилиши мумкин. Туннеллаш туфайли Internet инфратузилмасини VPN-иловалардан беришиш мумкин бўлади.

VPN туннеллари турли фойдаланувчилар учун яратилиши мумкин. Булар хавфсизлик шлюзи бўлган локал тармоқ LAN ёки масофадаги ва мобил фойдаланувчиларнинг алоҳида компьютерлари бўлиши мумкин. Йирик корхонанинг виртуал хусусий тармоғини яратиш учун VPN-шлюзлар, VPN-серверлар ва VPN-мижозлар керак бўлади. VPN-шлюзларни корхона локал тармоқларини химоялаш учун ишлатиш мақсадга мувофиқ бўлса, VPN-серверлар ва VPN-мижозлардан масофадаги ва мобил фойдаланувчиларни Internet орқали корпоратив тармоқ билан химояланган уланишини ташкил этишда фойдаланилади.

Виртуал химояланган каналларни қуриш вариантлари. VPN ни лойиҳалашда одатда, иккита асосий схема кўрилади (7.3-расм):



7.3-расм. «ЛХТ-ЛХТ» ва «Мижоз-ЛХТ» ҳилидаги виртуал химояланган каналлар

– локал тармоқлар орасидаги виртуал химояланган канал («ЛХТ-ЛХТ» канал);

– узел ва локал тармоқ орасидаги виртуал химояланган канал («мижоз-ЛХТ» канали).

Уланишнинг биринчи схемаси алоҳида офислар орасидаги кимматли ажратилган линиялар ўрнига ўтади ва улар орасида доимо фойдаланувчан, химояланган каналларни яратади. Бу ҳолда хавфсизлик шлюзи туннел ва локал тармоқ орасида интерфейс вазифасини ўтайди ва локал тармоқ фойдаланувчилари бир-бирлари билан мулоқот қилишда туннелдан фойдаланадилар. Аксарият компаниялар VPNнинг бу ҳилидан глобал тармоқнинг мавжуд Frame Relay каби уланишларни алмаштириш учун ёки уларга қўшимча сифатида фойдаланадилар.

VPN химояланган каналнинг иккинчи схемаси масофадаги ёки мобил фойдаланувчилар билан уланишни ўрнатишга аталган. Туннелни яратишни мижоз (масофадан фойдаланувчи) бошлаб беради. Масофадаги тармоқни химояловчи шлюз билан боғланиш учун у ўзининг компютерида махсус мижоз дастурий таъминотини ишга туширади. VPNнинг бу тури коммутацияланувчи уланишларни ўрнига ўтади ва масофадан фойдаланишнинг анъанавий усуллари билан бир қаторда ишлатилиши мумкин.

Виртуал химояланган каналларнинг қатор вариантлари мавжуд. Умуман, орасида виртуал химояланган канал шакллантирилувчи корпоратив тармоқнинг ҳар қандай иккита узели химояланувчи ахборот оқимининг охириги ва оралиқ нуктасига гааллукли бўлиши мумкин. Ахборот хавфсизлиги нуктаи назаридан химояланган туннел охириги нукталарининг химояланувчи ахборот оқимининг охириги нукталарига мос келиши варианты маъқул ҳисобланади. Бу ҳолда каналнинг ахборот пакетлари ўтишининг барча йўллари бўйлаб химояланиши таъминланади. Аммо бу вариант бошқаришнинг децентрализацияланишига ва ресурс сарфининг ошишига олиб келади. Агар виртуал тармоқдаги локал тармоқ ичида трафикни химоялаш талаб этилмаса, химояланган туннелнинг охириги нуктаси сифатида ушбу локал тармоқнинг тармоқлараро экрани ёки чегара маршрутизатори танланиши мумкин. Агар локал тармоқ ичидаги ахборот оқими химояланиши шарт бўлса, бу тармоқ охириги нуктаси вазифасини химояланган алоқада иштирок этувчи компютер бажаради.

Локал тармоқдан масофадан фойдаланилганида фойдаланувчи компьютери виртуал химояланган каналнинг охириги нуктаси бўлиши шарт. Фақат пакетларни коммутациялашли очик тармоқ, масалан Internet ичида ўтказилувчи химояланган туннел варианты етарлича кенг тарқалган. Ушбу вариант ишлатилиши қулайлиги билан ажралиб турсада, нисбатан паст хавфсизликка эга. Бундай туннелнинг охириги нукталари вазифасини одатда, Internet провайдерлари ёки локал тармоқ чегара маршрутизаторлари (тармоқлараро экранлар) бажаради.

Локал тармоқлар бирлаштирилганида туннел фақат Internetнинг чегара провайдерлари ёки локал тармоқнинг маршрутизаторлари (тармоқлараро экранлари) орасида шакллантирилади. Локал тармоқдан масофадан фойдаланилганида туннел Internet провайдерининг масофадан фойдаланиш сервери ҳамда Internetнинг чегара провайдери ёки локал тармоқ маршрутизатори (тармоқлараро экран) орасида яратилади. Ушбу вариант бўйича қурилган корпоратив тармоқлар яхши масштабланувчанлик ва бошқарилувчанликка эга бўлади. Шакллантирилган химояланган туннеллар ушбу виртуал тармоқдаги миждоз компьютерлари ва серверлари учун тўла шаффоф ҳисобланади. Ушбу узелларнинг дастурий таъминоти ўзгармайди. Аммо бу вариант ахборот алоқасининг нисбатан паст хавфсизлиги билан характерланади, чунки трафик қисман очик алоқа канали бўйича химояланмаган ҳолда ўтади. Агар шундай VPNни яратиш ва эксплуатация қилишни провайдер ISP ўз зиммасига олса, барча виртуал хусусий тармоқ унинг шлюзларида, локал тармоқлар ва корхоналарнинг масофадаги фойдаланувчилари учун шаффоф ҳолда қурилиши мумкин. Аммо бу ҳолда провайдерга ишонч ва унинг хизматига доимо тўлаш муаммоси пайдо бўлди.

Химояланган туннел, орасида туннел шакллантирилувчи узеллардаги виртуал тармоқ компонентлари ёрдамида яратилади. Бу компонентларни туннел инициаторлари ва туннел терминаторлари деб юритиш қабул қилинган.

Туннел инициатори дастлабки пакетни янги пакетга, жўнатувчи ва қабул қилувчи хусусидаги ахбороти бўлган янги сарлавҳали пакетга инкапсуляциялайди. Инкапсуляцияланган пакетлар ҳар қандай протокол турига, жумладан, маршрутланмайдиган протоколларга (масалан, Net BEUI) мансуб бўлишлари мумкин. Туннел бўйича узатиладиган барча пакетлар IP пакетлари

ҳисобланади. Туннелнинг инициатори ва терминатори орасидаги маршрутни одатда, Internetдан фарқлиниши мумкин бўлган, оддий маршрутланувчи тармоқ IP аниқлайди.

Туннелни инициаллаш ва узиш турли тармоқ қурилмалари ва дастурий таъминот ёрдамида амалга оширилиши мумкин. Масалан, туннел масофадан фойдаланиш учун улашни таъминловчи модем ва мос дастурий таъминот билан жихозланган мобил фойдаланувчининг ноутбуки томонидан инициалланиши мумкин. Инициатор вазифасини мос функционал имкониятларга эга бўлган локал тармоқ маршрутизатори ҳам бажариши мумкин. Туннел одатда, тармоқ коммутатори ёки хизматлар провайдери шлюзи билан тугалланади.

Туннел терминатори инкапсуляциялаш жараёнига тескари жараёни бажаради. Терминатор янги янги сарлавҳаларни олиб ташлаб, ҳар бир дастлабки пакетни локал тармоқдаги манзилга йўллайди.

Инкапсуляцияланувчи пакетларнинг конфиденциаллиги уларни шифрлаш, яхлитлиги ва ҳақиқийлиги эса электрон рақамли имзони шакллантириш йўли билан таъминланади. Маълумотларни криптографик химоялашнинг жўда кўп усуллари ва алгоритмлари мавжуд бўлганлиги сабабли, туннел инициатори ва терминатори химоянинг бир хил усулларида фойдаланишга ўз вақтида келишиб олишлари мақсадга мувофиқ ҳисобланади. Маълумотларни расшифровка қилиш ва рақамли имзони текшириш имкониятини таъминлаш учун туннел инициатори ва терминатори қадгларни хавфсиз алмашиш вазифасини ҳам мададлашлари зарур. Ундан ташқари, VPN туннеларини ваколатли фойдаланувчилар томонидан яратилишини кафолатлаш мақсадида ахборот алоқасининг асосий тарафлари аутентификациялашдан ўтишлари лозим. Корпорациянинг мавжуд тармоқ инфратузилмалари VPNдан фойдаланишга ҳам дастурий, ҳам аппарат таъминот ёрдамида тайёрланишлари мумкин.

7.2. Химояланган виртуал хусусий тармоқларнинг туркумланиши

Химояланган виртуал хусусий тармоқлар VPNни туркумлашни турли вариантлари мавжуд. Кўпинча туркумлашнинг қуйидаги учта аломати ишлатилади:

- OSI моделининг иш сатҳи;
- VPN техник ечимининг архитектураси;
- VPNни техник амалга ошириш усули.

OSI моделининг иш сатҳи бўйича VPNнинг туркумланиши.

Ушбу туркумлаш анчагина кизиқиш тўғдиради, чунки амалга оширилувчи VPNнинг функционаллиги ва унинг корпоратив ахборот тизимлари иловалари ҳамда химоянинг бошқа воситалари билан биргаликда ишлатилиши кўп ҳолларда танланган OSI сатҳига боғлиқ бўлади.

OSI моделининг иш сатҳ аломати бўйича канал сатҳидаги VPN, тармоқ сатҳидаги VPN ва сеанс сатҳидаги VPN фарқланади. Демак, VPNлар одатда, OSI моделининг пастки сатҳларида қурилади. Бунинг сабаби шуки, химояланган канал воситалари қанчалик пастки сатҳда амалга оширилса, уларни иловаларга ва татбиқий протоколларга шунчалик шаффоф қилиш соддалашади. Тармоқ ва канал сатҳларида иловаларнинг химоя протоколларига боғлиқлиги умуман йўқолади. Шу сабабли, фойдаланувчилар учун универсал ва шаффоф химояни фақат OSI моделининг пастки сатҳларида қуриш мумкин. Аммо, бунда биз бошқа муаммога-химоя протоколининг муайян тармоқ технологиясига боғлиқлиги муаммосига дуч келамиз.

Каналь сатҳидаги VPN. OSI моделининг канал сатҳида ишлатилувчи VPN воситалари учинчи (ва юқорирок) сатҳнинг турли хил трафигини инкапсуляциялашни таъминлашга ва «нукта-нукта» тилидаги виртуал туннелларни (маршрутизатордан маршрутизаторга ёки шахсий компьютердан локал ҳисоблаш тармоғининг шлюзига) қуришга имкон беради. Бу гуруҳга L2F (Layer 2 Forwarding) ва PPTP (Point-to-Point Tunneling Protocol) протоколлари ҳамда Cisco Systems и MicroSoft фирмаларининг бирга ишлаб чиққан L2TP(Layer 2 Tunneling Protocol) стандартидан фойдаланувчи VPN-маҳсулотлар тааллуқли.

Химояланган каналнинг протоколи PPTP «нукта-нукта» ула-нишларида, масалан, ажратилган линияларда ишлаганда кенг қўлланилувчи PPP протокоliga асосланган. PPTP протоколи иловалари ва татбиқий сатҳ хизматлари учун химоя воситаларининг шаффофлигини таъминлайди ва тармоқ сатҳида ишлатилувчи протоколга боғлиқ эмас. Хусусан, PPTP протоколи ҳам IP тармоқларида, ҳам IPX, DECnet ёки NetBEUL протоколлари асосида ишловчи тармоқларда пакетларни ташиши мумкин. Аммо, PPP

протоколи ҳамма тармоқларда ҳам ишлатилмаслиги сабабли (аксарият локал тармоқларида канал сатҳида Ethernet протоколи ишласа, глобал тармоқларда ATM, Frame Relay протоколлари ишлайди), уни универсал восита деб бўлмайди. Йирик бирикма тармоқнинг турли қисмларида, умуман айтганда, турли канал протоколлари ишлатилади. Шу сабабли бу гетероген муҳит орқали канал сатҳининг ягона протоколи ёрдамида химояланган канални ўтказиш мумкин эмас.

L2TP протоколи, эҳтимол, локал ҳисоблаш тармоқларидан фойдаланишни ташкил этишда устунлик қилувчи ечим бўлиб қолиши мумкин (чунки у, асосан, Windows операцион тизимида таянади.)

Тармоқ сатҳидаги VPN. Тармоқ сатҳидаги VPN-маҳсулотлар IPни IPга инкапсуляциялашни бажаради. Бу сатҳдаги кенг тарқалган протоколлардан бири SKIP протоколидир. Аммо бу протоколни аутентификациялаш, туннеллаш ва IP-пакетларни шифрлаш учун аталган IPSec(IPSecurity) протоколи аста-секин сўриб чиқармоқда.

Тармоқ сатҳида ишловчи IPSec протоколи мурасага асосланган вариант ҳисобланади. Бир томондан у иловалар учун шаффоф, иккинчи томондан кенг тарқалган IP протоколига асосланганлиги сабабли барча тармоқларда ишлаши мумкин. Шу орада эсдан чиқармаслик лозимки, IPSecнинг спецификацияси IPга мўлжалланганлиги сабабли у тармоқ сатҳининг бошқа протоколлари трафиғи учун тўғри келмайди. IPSec протоколи L2TP протоколи билан биргаликда ишлаши мумкин. Натижада, бу икки протокол ишончли идентификациялашни, стандартланган шифрлашни ва маълумотлар яхлитлигини таъминлайди. Иккита локал тармоқ орасидаги IPSec туннели маълумотлар узатувчи яқка тармоқлар тўпламини мададлаши мумкин. Натижада, бу хилдаги иловалар масштабланиш нуқтаи назаридан иккинчи сатҳ технологияларига нисбатан устунликка эга бўлади.

IPSec протоколи билан масофадаги қурилмалар орасида криптографик қалитларни хавфсиз бошқариш ва алмашиш масалаларини ечувчи IKE (Internet Key Exchange) протоколи боғланган. IKE протоколи қалитларни алмашишни автоматлаштиради ва химояланган уланишни ўранатади, IPSec эса пакетларни кодлайди ва «имзо чекади». Ундан ташқари, IKE ўрнатилган уланиш учун

калитни ўзгартириш имкониятига эга. Бу узатиловчи ахборотнинг конфиденциаллигини оширади.

Сеанс сатҳидаги VPN. Баъзи VPNлар «канал воситачилари» (circuit proxy) деб аталувчи усулдан фойдаланади. Бу усул транспорт сатҳи устида ишлайди ва ҳар бир сокет учун алоҳида трафикни ҳимояланган тармоқдан умумфойдаланувчи Internet тармоғига ретрансляциялайди. (IP сокети TCP-уланишнинг ва муайян порт ёки берилган порт UDP комбинацияси орқали идентификацияланади. TCP/IP стекида бешинчи-сеанс сатҳи бўлмайди, аммо сокетларга мўлжалланган амалларни кўпинча сеанс сатҳи амаллари деб юритишади.)

Туннелнинг инициатори ва терминатори орасида узатиловчи ахборотни шифрлаш транспорт сатҳи TLS(Transport Layer Security) ёрдамида амалга оширилади. Тармоқлараро экран орқали аутентификацияланган ўтишни стандартлаш учун SOCKS деб аталувчи протокол аниқланган ва ҳозирда SOCKS протоколининг 5-версияси канал воситачиларини стандарт амалга оширилишида ишлатилади.

SOCKS протоколининг 5-версиясида мижоз компьютери воситачи (proxy) вазифаларини бажарувчи сервер билан аутентификацияланган сокет (ёки сеанс) ўрнатади. Бу воситачи-тармоқлараро экран орқали боғланишнинг ягона усули. Воситачи, ўз навбатида, мижоз томонидан сўралган ҳар қандай амални бажаради. Воситачига сокет сатҳидаги трафик маълумлиги сабабли, у синчиклаб назорат қилиши, масалан, муайян иловаларни, агар улар зарурий ваколатларга эга бўлмаса, блокировка қилиши мумкин.

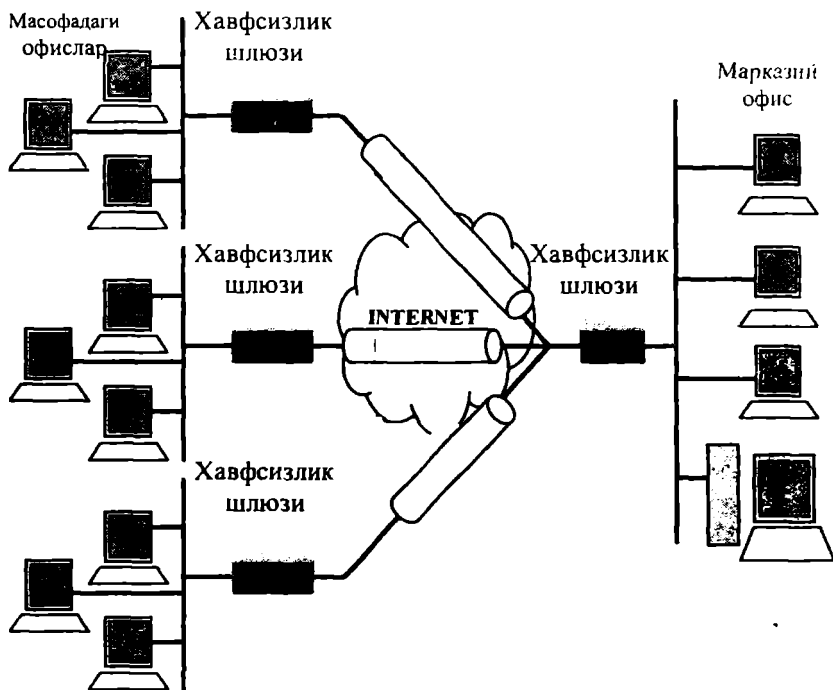
Агар IPSec протоколи моҳияти бўйича, IP тармоқни ҳимояланган туннелга таркатса, SOCKS протоколи асосидаги маҳсулотлар уни алоҳида ҳар бир илова ва ҳар бир сокетга кенгайтиради. Иккинчи ва учинчи сатҳнинг яратилган туннеллари иккала йўналишда бирдай ишласа, 5 сатҳнинг VPN тармоғи ҳар бир йўналишда узатишни мустақил бошқаришга руҳсат беради. IPSec протоколга ва иккинчи сатҳ протоколларига ўхшаб 5 сатҳнинг VPN тармоқлари виртуал хусусий тармоқларнинг бошқа турлари билан бирга ишлатилиши мумкин, чунки бу технологиялар бир-бирини инкор қилмайди.

Техник ечимининг архитектураси бўйича VPNнинг туркумланиши. Ушбу туркумлаш бўйича виртуал хусусий тармоқлар қуйидаги уч турга бўлинади:

- корпорация ичидаги VPN тармоқ;

- масофадан фойдаланилувчи VPN тармоқ;
- корпорациялараро VPN тармоқ.

Корпорация ичидаги VPN тармоқ. Корпорация ичидаги VPN тармоқлар (Intranet VPN) корхона ичидаги бўлинмалар ёки алоқанинг корпорация тармоқлари (шу жумладан, ажратилган линиялар) ёрдамида бирлаштирилган корхоналар гуруҳи орасида химояланган алоқани ташкил этиш учун ишлатилади. Ўзининг филиллари ва бўлимлари учун ахборотнинг марказлаштирилган омборидан фойдаланишга эҳтиёж сезган компаниялар масофадаги узелларни ажратилган линиялар ёки frame relay технологияси ёрдамида улайдилар. Аммо ажратилган линияларнинг ишлатилиши эгалланадиган ўтказиш полосасининг ва объектлар орасидаги масофанинг катталашгани сари жорий сарф-харажатларнинг ошишига сабаб бўлади. Буларни камайтириш учун компания узелларини виртуал хусусий тармоқ ёрдамида улаши мумкин (7.4-расм).



7.4-расм. VPN intranet технологияси ёрдамида тармоқ узелларини улаш.

Intranet VPN тармоқлар Internetдан ёки сервис-провайдерлар томонидан тақдим этилувчи бўлинувчи тармоқ инфратузилмаларидан фойдаланган ҳолда қурилади. Компания нархи қиммат ажратилган линиялардан воз кечиб, уларни арзонроқ Internet орқали алоқа билан алмаштиради. Бу ўтказиш полосасидан фойдаланишдаги сарф-харажатни жиддий камайтиради, чунки Internetда масофа уланиш нархига ҳеч таъсир этмайди.

Intranet VPN учун қуйидаги афзалликлар ҳарактерли:

- конфиденциал ахборотни ҳимоялаш учун шифрлашнинг қучли криптографик протоколларидан фойдаланиш;
- автоматлаштирилган савдо тизими ва маълумотлар базасини бошқариш тизими каби жиддий иловаларни бажаришда ишлашнинг ишончилиги;
- сони тез ўсаётган фойдаланувчилар, янги офислар ва янги дастурий иловаларни самаралироқ жойлаштириш учун бошқаришнинг мослашувчанлиги.

Internetдан фойдаланиб Intranet VPNни қуриш VPN-технологияни амалга оширувчи энг рентабел усули ҳисобланади. Аммо Internetда сервис даражаси умуман қафолатланмайди. Қафолатланган сервис даражасини хоҳловчи компаниялар ўзларининг VPNларини сервер-провайдерлари томонидан тақдим этилувчи бўлинувчи тармоқ инфратузилмаларидан фойдаланиб сафлаш имкониятларини қўришлари шарт.

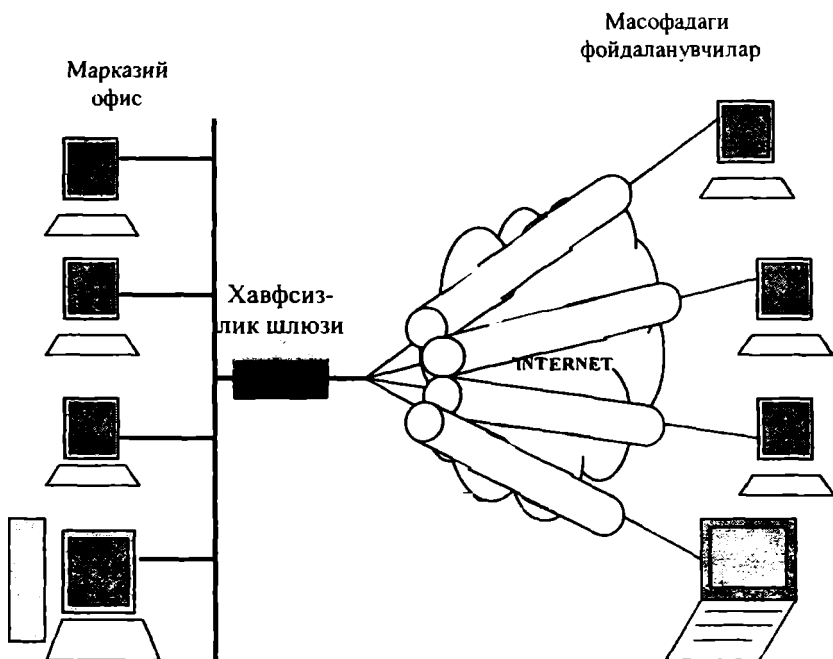
Масофадан фойдаланилувчи VPN тармоқ. Масофадан фойдаланилувчи виртуал хусусий тармоқлар VPN (Remote Access VPN) корпорациянинг мобил ёки масофадаги ходимларига (компания раҳбарияти, меҳнат сафаригадаги ходимлар, қасаначилар ва ҳ.) корхона ахборот ресурсларидан ҳимояланган масофадан фойдаланишни таъминлайди.

Масофадан фойдаланувчи виртуал хусусий тармоқларнинг (7.5-расм) коммутацияланувчи ва ажратилган линиялардан фойдаланишнинг ҳар ойдаги сарф-харажатларини анчагина камайтиришга имкон бериши, уларнинг умумий эътироф этилишига сабаб бўлди. Уларнинг ишлаш принципи оддий: фойдаланувчилар глобал тармоқдан фойдаланишнинг маҳаллий нуқтаси билан уланишларни ўрнатади. Сўнгра уларнинг сўровлари Internet орқали туннелланади. Бу шаҳарлараро ва халқаро алоқа учун тўловдан қутилишга имкон беради. Ундан кейин барча сўровлар мос узелларда тўпланади ва корпорация тармоқларига узатилади.

Хусусий бошқарилувчи тармоқлардан (dial networks) масофадан фойдаланилувчи VPN тармоқларга (Remote Acces VPN) ўтиш куйидаги афзалликларни беради:

– шаҳарлараро ракамлар ўрнига маҳаллий ракамлардан фойдаланиш имконияти шаҳарлараро телекоммуникацияга сарф-харажатларни анчагина камайтиради;

– аутентификациялаш жараёнини ишончли ўтказишни таъминловчи масофадаги ва мобил фойдаланувчилар ҳақиқийлигини аниқлаш тизимининг самарадорлиги;



7.5-расм. Масофадан фойдаланишли виртуаль хусусий тармоқ.

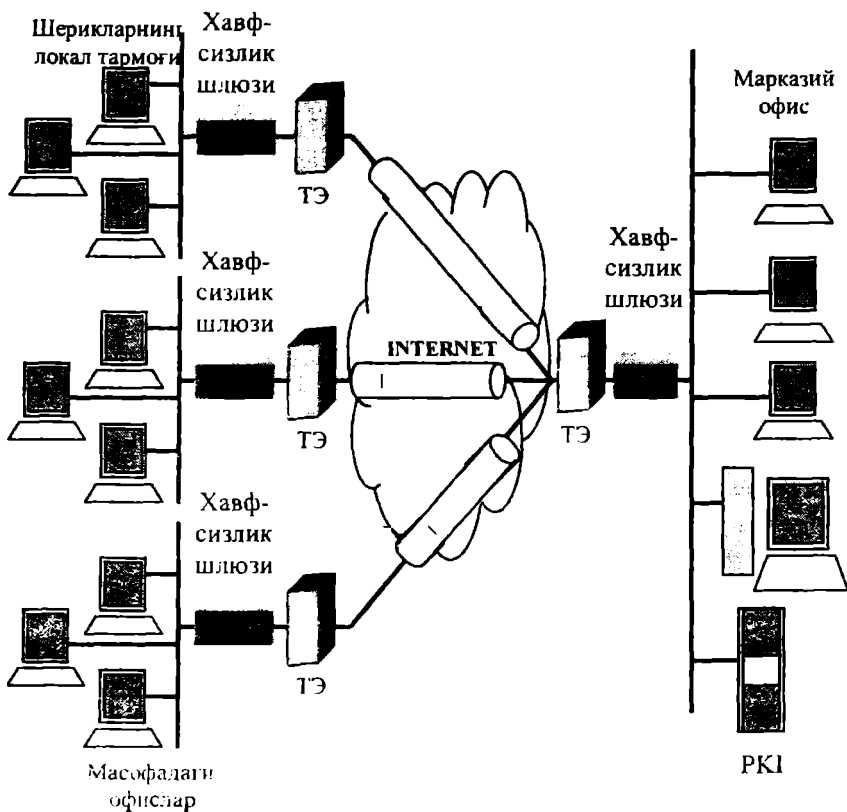
– масштабланишнинг янада юқорилиги ва тармоққа кўшилувчи янги фойдаланувчилар сафланишининг оддийлиги;

– компания эътиборини тармоқ ишлаши муаммолари ўрнига корпорациянинг асосий бизнес-мақсадларига қаратиш.

Таъкидлаш лозимки, сезувчан корпорация трафигини ташишда очик тармоқ Internet нинг бирлаштирувчи магистрал сифатида иш-

латилишининг кўлами ошиб бормоқда. Бу ахборот химояси механизмини ушбу технологиянинг энг муҳим элементига айлантиради.

Корпорациялараро VPN тармоқ. Корпорациялараро VPN тармоқлардан (Extranet VPN) бизнес бўйича стратегик шериклар, таъминотчилар, йирик буюртмачилар, мижозлар ва х. билан самарали алокани ва ахборотни химояланган алмашинувини ташкил этишда фойдаланилади (7.6-расм). Extranet – бир компания тармоғидан иккинчи компания тармоғининг тўғридан-тўғри фойдаланишини таъминлаш орқали иш юзасидан ҳамкорлик жараёнида алоқа ишончилигини оширишга имкон берувчи технологиядир.



7.6-расм Корпорациялараро extranet VPN тармоғи.

Extranet VPN тармоқлари умуман корпорация ичидаги виртуал хусусий тармоқларга ўхшаш, фарқи шундаки, корпорациялараро виртуал хусусий тармоқлар учун ахборот химояси муаммоси кескинроқдир. Extranet VPN учун ишбилармон шериклар ўзларининг тармоқларида қўллашлари мумкин бўлган турли VPN-счимлар билан алоқа қилиш имкониятларини кафолатловчи стандартлаштирилган VPN-махсулотлардан фойдаланиш характерлидир.

Бир неча компаниялар бирга ишлашга келишиб, бир-бирларига тармоқларини очишганида, улар янги шерикларининг факат маълум ахборотдан фойдаланишларига йўл қўйишлари лозим. Бунда конфиденциал ахборот рухсатсиз фойдаланишдан ишончли химояланиши зарур. Айнан, шу сабабли корпорациялараро тармоқларда очик тармоқ томонидан тармоқлараро экран (бранд-мауэр) ёрдамида назоратга катта аҳамият берилади. Ахборотдан хақиқий фойдаланувчининг фойдаланишини кафолатловчи аутентификациялаш ҳам муҳим ҳисобланади. Шу билан бир қаторда рухсатсиз фойдаланишдан химоялашнинг сафланган тизими ўзига эътиборни жалб қилмаслиги шарт.

Extranet VPN уланишлари intranet VPN ва remote access VPN лар амалга оширилишидаги ишлатилган архитектура ва протоколлардан фойдаланиб сафланади. Асосий фарқ шундан иборатки, extranet VPN фойдаланувчиларига бериладиган фойдаланишга рухсат улар шеригининг тармоғи билан боғлиқ.

Баъзида VPN тармоғининг локал варианты (Localnet VPN) алоҳида гуруҳга ажратилади. Localnet VPN локал тармоғи компания локал тармоғи ичида (одагда, марказий офис) айланувчи ахборотлар оқимидан компаниядан ишловчи «ортикча кизикувчи» ходимларнинг рухсатсиз фойдаланишидан химоялашни таъминлайди. Таъкидлаш лозимки, ҳозирда VPNни амалга оширувчи турли усулларнинг конвергенцияси ғояси кўзга ташланмоқда.

Техник амалга ошириш бўйича VPNнинг туркумланиши. Виртуал хусусий тармоқнинг конфигурацияси ва характеристикалари кўп жihatдан ишлатиладиган VPN-қурилмаларининг турига боғлиқ.

Техник амалга ошириш бўйича VPNнинг қуйидаги гуруҳлари фаркланади:

- маршрутизаторлар асосидаги VPN;
- тармоқлараро экранлар асосидаги VPN;

– дастурий таъминот асосидаги VPN;

– ихтисослаштирилган аппарат воситалари асосидаги VPN.

Маршрутизаторлар асосидаги VPN. VPN куришининг ушбу усулига биноан химояланган каналларни яратишда маршрутизаторлардан фойдаланилади. Локал тармоқдан чиқувчи барча ахборот маршрутизатор орқали ўтганлиги сабабли, унга шифрлаш вазифасини юклаш табиий. Маршрутизатор асосидаги VPN асбоб-ускуналарига мисол тариқасида Cisco-Systems компаниясининг курилмаларини кўрсатиш мумкин.

Тармоқлараро экранлар асосидаги VPN. Аксарият ишлаб чиқарувчиларнинг тармоқлараро экранни туннеллаш ва маълумотларни шифрлаш вазифаларини мададлайди. Тармоқлараро экранлар асосидаги ечимга мисол тариқасида Check Point Software Technologies компаниясининг Fire Wall-1 маҳсулотини кўрсатиш мумкин. Шахсий компьютер асосидаги тармоқлараро экранлар фақат узатишчи ахборот ҳажми нисбатан кичик бўлган тармоқларда қўлланилади. Ушбу усулнинг камчилиги – битта ишчи ўрнига ҳисобланганда ечим нархининг юқорилиги ва унумдорликнинг тармоқлараро экран ишлайдиган аппарат таъминотига боғлиқлиги.

Дастурий таъминот асосидаги VPN. Дастурий усул бўйича амалга оширилган VPN маҳсулотлар унумдорлик нуқтани назаридан ихтисослаштирилган курилмадан қолишсада, VPN-тармоқларни амалга оширилишида етарли қувватга эга. Таъкидлаш лозимки, масофадан фойдаланишда зарурий ўтказиш полосасига талаблар катта эмас. Шу сабабли, дастурий маҳсулотларнинг ўзи масофадан фойдаланиш учун етарли унумдорликни таъминлайди. Дастурий маҳсулотларнинг шубҳасиз афзаллиги-қўлланилишининг мосланувчанлиги ва қулайлиги ҳамда нархининг нисбатан юқори эмаслиги.

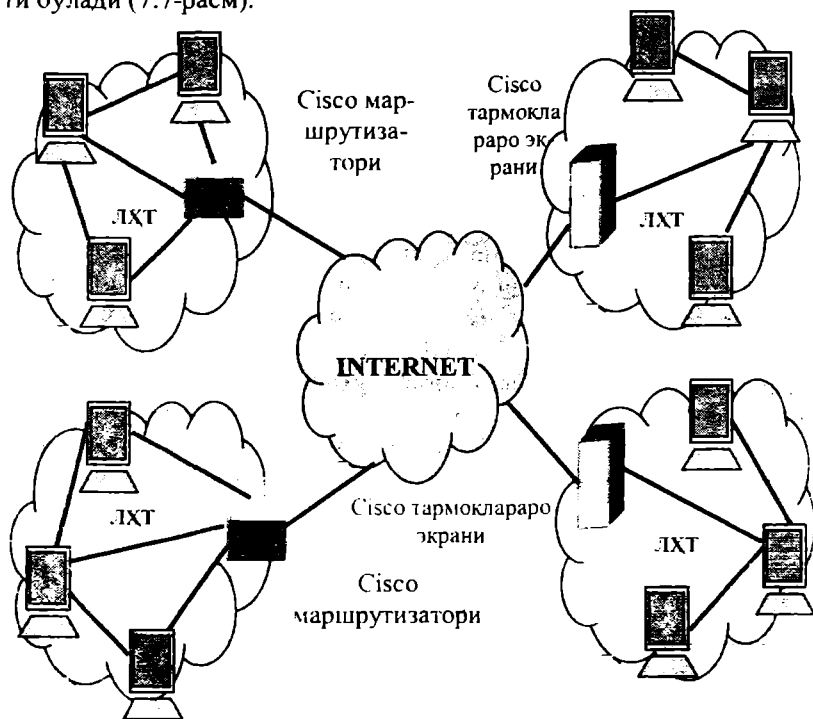
Ихтисослаштирилган аппарат воситалари асосидаги VPN
Ихтисослаштирилган аппарат воситалари асосидаги VPNларнинг эни муҳим афзаллиги унумдорлигининг юқорилигидир. Ихтисослаштирилган аппарат воситалари асосидаги VPN тизимларда шифрлашнинг микросхемаларда амалга оширилиши тезкорликнинг таъминланишига сабаб бўлади. Ихтисослаштирилган VPN-курилмалар хавфсизликнинг юқори даражасини таъминлайди, ammo уларнинг нархи анчагина юқори.

7.3. Химояланган корпоратив тармоқларни қуриш учун VPN ечимлар

Маршрутизаторлар асосидаги VPN. Ташқи дунё билан локал тармоқ алмашадиган барча ахборот маршрутизатор орқали ўтади. Бу маршрутизаторларни чиқувчи пакетларни шифрловчи ва кирувчи пакетларни расшифровка қилувчи габиий платформага айлантиради. Бошқача айтганда, маршрутизатор, умуман, маршрутлаш вазифасини VPN вазифасини мададлаш билан бирга олиб бориши мумкин. Бундай ечим ўзининг афзалликлари ва камчиликларига эга. Афзаллиги – маршрутлаш ва VPN вазифаларини биргаликда маъмурлаш кўлайлигидир. Корхона тармоқлараро экранни ишлатмасдан корпоратив тармоқ химоясини фақат ҳам тармоқдан фойдаланиш бўйича, ҳам узатиладиган трафикни шифрлаш бўйича химоялаш вазифаларини биргаликда ҳал этувчи маршрутизатор ёрдамида ташкил этган ҳолларда маршрутизаторларни VPNни мададлашда ишлатилиши айниқса фойдалидир. Ушбу ечимнинг камчилиги маршрутлаш бўйича асосий амалларнинг кўп меҳнат сарфини талаб этувчи трафикни шифрлаш ва аутентификациялаш амаллари билан бирга олиб борилиши натижасида маршрутизатор унумдорлигига қуйиладиган талабларнинг ошиши билан боғлиқ. Маршрутизаторларнинг унумдорлигини оширишга шифрлаш вазифаларини аппарат мададлаш орқали эришилади. Ҳозирда барча маршрутизатор ва бошқа тармоқ қурилмаларини етакчи ишлаб чиқарувчилари ўзларининг махсулотларида турли VPN-протоколларини мададлайдилар. Бу соҳада Cisco Systems ва 3Com компаниялари лидер ҳисобланадилар. Cisco Systems компанияси ўзлари ишлаб чиққан маршрутизаторларга энг кенг тарқалган стандартлар асосида VPNларни қуришга имкон берувчи канал сатҳи протоколларини мададловчи IOS 11.3(Internetwork Operation System 11.3) ва тармоқ сатҳи протоколи IPSecни киритди. L2F протоколи аввалроқ IOS операцион тизимнинг компонентига айланди ва Cisco ишлаб чиқарадиган барча тармоқлараро алоқа ва масофадан фойдаланиш қурилмаларида мададланади.

Cisco маршрутизаторларида VPN вазифалари бутунлай дастурий йўл билан ёки шифрлаш сопроцессори бўлган махсус кенгайтириш платасидан фойдаланилган ҳолда амалга оширилиши мумкин. Охириги вариант VPN амалларида маршрутизатор унумдорлигини анчагина оширади. Cisco Systems компанияси томонидан иш-

лаб чиқилган VPN қуриш технологияси юқори унумдорлиги ва мосланувчанлиги билан ажралиб туради. Унда «тоза» ёки инкапсуляция қилинган кўринишда узатилувчи ҳар қандай IP-оқим учун шифрлаш билан туннеллаш таъминланади. Cisco компаниясининг маршрутизаторлари асосида VPN-каналларини қуриш операцион-тизимининг воситалари ёрдамида Cisco IOS 12.х. версиясидан бошлаб амалга оширилади. Агар мазкур операцион тизим компаниянинг бошқа бўлимларидаги Cisco чегара маршрутизаторларида ўрнатилган бўлса, бир маршрутизатордан иккинчисига «нукта нукта» туридаги виртуал химояланган туннеллар мажмуасида иборат бўлган корпоратив VPN тармоқни шакллантириш имконияти бўлади (7.7-расм).



Маршрутизаторлар асосида VPNларни куришда эсда тутиш лозимки, бундай ёндашишнинг ўзи компаниянинг умумий ахборот хавфсизлигини таъминлаш муаммосини ҳал этмайди. Чунки барча ички ахборот ресурслар барибир ташқаридан хужум қилиш учун очик қолади. Бу ресурсларни химоялаш учун, одатда, чегара маршрутизаторларидан кейин жойлашган тармоқлараро экранлардан фойдаланилади.

Cisco 1720 VPN Access Router маршрутизатори катта бўлмаган ва ўртача корхоналарда химояланган фойдаланишини ташкил этишга агадган. Бу маршрутизатор Internet ва интратаармоқлардан фойдаланишни ташкил этишга зарур бўлган имкониятларни таъминлайди ва Cisco IOS дастурий таъминот асосидаги виртуал хусусий тармоқларни ташкил этиш вазибаларини мададлайди. Cisco IOS операцион тизими маълумотларни химоялаш, хизмат сифагини бошқариш ва юқори ишончилиликни таъминлаш бўйича VPN вазибаларининг жуда кенг тўпламини таъминлайди.

Cisco 1720 маршрутизатори маълумотлар химоясинини куйидаги вазибаларини бажаради:

- *тармоқлараро экранлаш.* Cisco IOS Firewall компонента локал тармоқларни хужумлардан химоялайди. *Фойдаланишининг контекстли назорати* CBAC (Context-based access control) функцияси маълумотларни динамик ёки ҳолатларга асосланган, иловалар бўйича дифференциалланган филтрлашни бажаради. Бу функция самарали тармоқлараро экранлаш учун жуда муҳим ҳисобланади. Cisco IOS Firewall компонента қатор бошқа фойдали вазибаларни ҳам, хусусан, «хизмат қилишдан воз кечиш» каби хужумларни аниқлаш ва олдини олиш, Javaни блокировка этиш, аудит ва вакнинг реал масшабида огоҳлантиришларни тарқатиш вазибаларини бажаради:

- *шифрлаш.* IPSec протоколидаги DES ва Triple DES шифрлаш алгоритмларини мададлаш маълумотларни конфиденциаллиги ва яхлитлигини ва маълумотлар манбаини аутентификациялашни (маълумотлар глобал тармоқдан ўтганидан сўнг) таъминлаш мақсадида ишончли ва стандарт шифрлайди;

туннеллаш. Туннеллашнинг IPSec, GRE (Generic Routing Encapsulation), L2F ва L2TP стандартлари ишлатилади. L2F ва L2TP стандартлари масофадаги фойдаланувчиларнинг корхона локал тармоғида ўрнатилган Cisco 1720 маршрутизаторигача виртуал туннел ўтказганларида ишлатилади. Бундай қўлланишда корхонада

масофадан фойдаланиш серверига эҳтисж қолмайди ва шакарлараро ёки халқаро кўнгилроқлар учун тўлови тежаллади;

– *қурilmаларни аутентификациялаш ва қалитларни бошқариш*. IPSec қатта тармоқларда маълумотлар ва қурilmаларни масштабланувчи аутентификациялашни таъминловчи қалитларни бошқариш протоколи IKE, рақамли сертификатлар X.509 версия 3, сертификатларни бошқарувчи протокол СЕР, ҳамда Verisign ва Entrust компания сертификат серверлари мададланади;

– *VPNнинг шижоз дастурий таъминоти*. IPSec ва L2TP протоколларининг стандарт версиялари билан ишловчи ҳар қандай шижоз Cisco IOS билан ўзаро алоқа қилиши мумкин;

– *фойдаланувчиларни аутентификациялаш*. Бунинг учун PAP, CHAP протоколлари, TACACS⁺ ва RADIUS тизимлари, фойдаланиш токенлари каби воситалардан фойдаланилади.

Виртуал химояланган тармоқлар нафақат маълумотларни химоялаш, балки химоялашнинг юқори савияси QoSни (Quality of Service) таъминлаши лозим. Cisco 1720 маршрутизатори QoSни куйидаги бошқариш механизмларини мададлайди:

– *фойдаланишнинг келишмаган тезлиги CAR (Committed Access Rate) иловалар ёки фойдаланувчилар базисида куйидаги учта муҳим вазифани бажаради:*

- график турини туркумайди;
- берилган иловага руҳсат этилган ўтказиш қобилиятининг максимал даражасини ўрнатади;
- трафикнинг ҳар бир турини устуворлигини белгилайди;

– *сиёсат асосида маршрутлаш (Policy Routing) ҳам трафикни туркумайди ва устуворлайди ҳамда трафикнинг қайси турини маршрутизаторнинг мос чиқиб йўли портига жўнатиш лозимлигини ҳал этади:*

– *мулоҳазали одилона навбат WFQ (Weighted Fair Queuing) трафикни ҳисобга олган ҳолда мақбул жавоб вақтини таъминлайди: протокол RSVP иловаларга йўлнинг бошидан охиригача қафолатланган ўтказиш қобилиятини резервлашга имкон беради.*

Маршрутизаторнинг мослашувчанлиги модулли конструкция ва иккита слотда ўрнатиловчи интерфейс WAN-карталари тўплами орқали таъминланади. Cisco 1720 моделида Cisco 1600, 2800, ва 3600 моделларда ишлатиладиган WAN-карталардан фойдаланилади.

Компания 3Com VPN технологияни амалга оширишда бошқадан стандартларни кўзга тутган эди. VPN ни маддадлаш учун Net-Builder II, Super Stack II NetBuilder маршрутизаторларига Office Connect Net Builder Platform платформаларига ўрнатилган.

3Com компанияси PPTP ва L2TP протоколларни маддадловчи масофадан фойдаланиувчи концентраторларни йирик ишлаб чиқарувчиларидан биридир. 3Com компаниясининг VPN тармоқлари IPsec билан бирга ишлатилади ва ташқи каталоглар, жумладан, Novell NDS ва Windows NT Directory Servicesлар билан ўзаро алоқа қилиш учун ишлаб чиқилган.

Компания Web-технологияга асосланган ва VPN юкланганлигини назоратлашга ҳамда юз берувчи ходисалар асосида статистика ва ахборотни йиғишга аталган дастурий илова Transcend Ware Secure VPN Manager ни ҳам ишлаб чиқди. Ундан ташқари, 3Com криптохимояланган туннелларни осонгина яратишга имкон берувчи Web асосидаги инструментарийни ишлаб чиқаради.

Internet Devices компаниясининг Fort Knox маршрутизаторларида тезлик ва қувват уйғунлашган. Ундаги тармоқни химоялашни таъминлашга йўналтирилган IP-трафикни ишлаш вазифалари рўйхатининг кенглиги унинг афзаллигидир. Fort Knox маршрутизатори тармоқлараро экран режимида ишлаши, NAT стандарти бўйича манзилларни трансляциялаши, хавфсизлик сиёсатини бошқариши, Web-саҳифалар ва DNS жадвал ёзувларини кўшлаши, аудитни бажариши мумкин. Одатда, Fort Knox корпоратив тармоқ чегарасида, корпоратив тармоқни глобал тармоқ билан уловчи маршрутизатордан кейин ўрнатилади. Демак, у бошқа локал тармоқлар билан VPN-алокани ўрнатиш ва тармоқлараро экранлар каби фойдаланишни назоратлашнинг турли қондаларини шакллантириши мумкин. Fort Knoxда NAT манзилларини трансляциялаш функциясининг мавжудлиги, унга ички IP-манзилларни беркитиш ва маршрутизаторлар трафигини қайта йўналтириш имконини беради. Бу корпоратив тармоқ маъмурларини VPNни куришда маршрутизаторларни янгидан конфигурациялашдан озод этади. Fort Knox функциялари тўпламининг кенглигига карамай унинг нархи оддий маршрутизатор нархига тенг.

Тармоқлараро экранлар асосидаги VPN. Локал тармоқнинг тармоқлараро экрани орқали, худди маршрутизатордагидек, бутун трафик ўтади. Шу сабабли, тармоқлараро экран ҳам чикувчи трафикни шифрлаш, қирувчи графикни расшифровка қилиш вазифа-

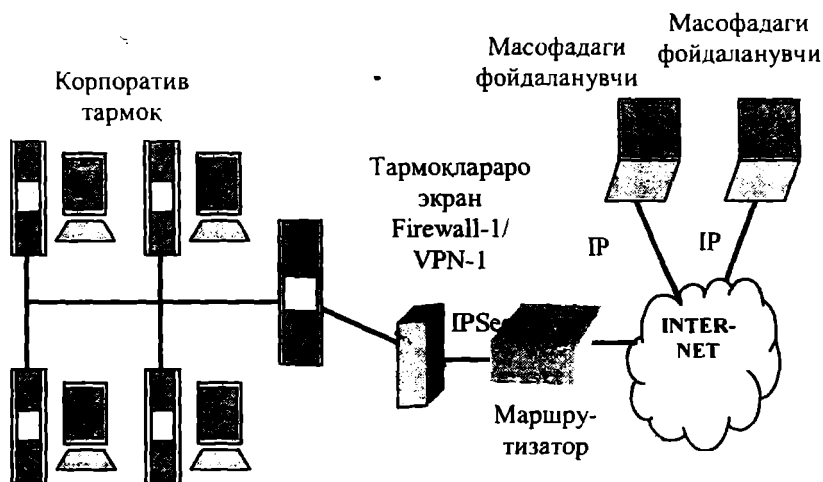
сини бажариши мумкин. Ҳозирди қатор VPN-ечимлар тармоқлараро экранларни VPNнинг қўшимча мадад функциялари билан тўлдирилишига таянади. Бу Internet орқали бошқа тармоқлараро экранлар билан шифрланган уланишни ўрнатишга имкон беради. Ахборот хавфсизлиги бўйича қатор мутахассисларнинг фикрича VPNни тармоқлараро экранлар асосида қуриш, корпоратив тармоқларни очик тармоқлар ҳужумларидан комплекс химоялаш нуқтан назаридан, тўла асосланган ечимдир. Ҳақиқатан, тармоқлараро экран ва VPN-шлюз функциялари бир нуқтада, ягона бошқариш ва аудит тизими назоратида бирлаштирилса, корпоратив тармоқни химоялаш функциялари битта қурилмада тўпланади. Натижанда, химоя воситаларини маъмурлаш сифати ошади.

Аммо, химоялаш воситаларининг бундай универсаллаштирилиши, ҳисоблаш воситаларининг мавжуд имкониятлари даражасида нафақат ижобий, балки салбий томонига ҳам эга. Шифрлаш ва аутентификациялаш амалларини ҳисоблаш мураккаблиги тармоқлараро экран учун анъанавий бўлган пакетларни филтрлаш амалларига нисбаган анча юқори. Шу сабабли, VPNнинг қўшимча вазифаларини амалга оширишда мураккаблиги катта бўлмаган амалларни бажаришга мўлжалланган тармоқлараро экран кўпинча керакли унумдорликни таъминламайди. Корпоратив тармоқ тезқоқ канал орқали очик тармоққа уланганида сифатли химояни таъминлаш учун алоҳида аппарат, дастурий ёки комбинацияланган қурилма кўринишидаги VPN-шлюздан фойдаланиш лозим.

Аксарият тармоқлараро экранлар сервер дастурий таъминоти дан иборат, шу сабабли унумдорликни ошириш муаммоси юқори унумдорликка эга бўлган компьютер платформасидан фойдаланиш эвазига ечилиши мумкин.

Check Point Software Technologies компанияси Internet билан ишлаганда ахборот хавфсизлигини комплекс таъминлаш маҳсулотларини ишлаб чиқариш соҳасидаги етакчилардан бири ҳисобланади. Check Point Fire Wall-1 тармоқлараро экран корпоратив ахборот ресурслари учун ягона комплекс доирасида химоянинг чуқур эшелонланган чегарасини қуришга имкон беради. Бундай комплекс таркибига Check Point FW-1 нинг ўзи ва корпоратив VPN тармоқ (химояланган туннелларни шакллантирувчи қисм тизим) қуриш учун маҳсулотлар тўплами Check Point VPN-1 ҳамда сукилиб киришни пайкаш воситалари Flood Gate ва х. қиради.

Дастурий таъминотлар Check Point Fire Wall-1/VPN-1 асосида корпоратив тармоқ куриш мисоли 7.8-расмда келтирилган.



7.8-расм. Check Point FW-1/VPN-1 асосида корпоратив VPN тармоғини куриш схемаси.

Check Point VPN-1 қисм тизим таркибидаги барча маҳсулотлар ҳам ўзаро, ҳам оммавий брандмауэр Fire Wall-1 билан узвий интеграцияланган. Check Point компанияси «тармоқ-тармоқ» (VPN-1 Gateway) ва «тармоқ-масофадаги фойдаланувчи» (VPN-1 Gateway+VPN-1 Secu Remote) типидagi ҳимояланган тармоқларни ташкил этиш учун воситаларни тақдим этади.

Check Point VPN-1 маҳсулотлари очик стандартлар (IPSec) асосида амалга оширилган, фойдаланувчиларни аутентификациялашнинг ривожланган тизимига эга, очик калитларни (PKI) тақсимлашнинг ташқи тизимлари билан ўзаро алокани мададлайди, бошқариш ва аудитнинг марказлаштирилган тизимини куришга имкон беради ва ҳ.

Check Point Fire Wall-1/VPN-1 нафакат очик, балки криптоҳимояланган трафикни ҳам назоратлайди. Тармоқлараро экран FW-1га келган маълумотлар VP-1 воситалари ёрдамида расшифровка қилинади, сўнгра ахборотлар пакети яна шифрланади ва ўтказиб юборилади.

VPN-1 қисм тизими трафикни нафақат криптографик беркитади, балки ахборотлар пакетини аутентификациялайди ҳам. Check Point Fire Wall-1/VPN-1 каналларида трафикни шифрлашда махшур DES, 3-Des, CAST, IDEA, FWZ1 ва ҳ. крптоалгоритмлардан фойдаланилади. FWZ1 криптотизими Check Point компаниясининг ишланмасидир. Ахборот пакетларини аутентификациялашда MD5, SHA-1, CBC DES ва MAC алгоритмлари ишлатилади.

VPN-Gateway шлюзи – шифрлашнинг дастурий модули тармоқлараро экран Fire Wall – 1 билан узвий интеграцияланган. Бу махсулот корхонага узатилувчи маълумотларнинг тўла конфиденциаллигини, аутентификацияланганлиги ва яхлитлигини кафолатлаган ҳолда Internet орқали алоқа каналларини куришга имкон беради. VPN функциялари корхонанинг умумий хавфсизлик сиёсати-га тўла интеграцияланганлиги сабабли, брандмауэр ва VPN-махсулотларни алоҳида бошқаришга эҳтиёж қолмайди.

VPN Gateway шлюзи химояланган VPN-туннелни ўрнатган ҳолда тармоқлар орасида Internet орқали узатилаётган конфиденциал маълумотларни шифрлайди. Бу шлюз уни жавобгарлик доирасига, яъни унинг доменига кирувчи компьютерлардан келадиган маълумотлар оқимини шифрлайди. Бу локал тармоқ ёки ушбу шлюз орқасидаги оддий хостлар гуруҳи бўлиши мумкин. Бу маълумотлар тармоқнинг оммавий қисми бўйича шифрланган кўринишда узатилади, ички тармоқ бўйича узатилганда шифрланмайди. VPN-амалларининг барчаси охириги фойдаланувчи ва барча иловалар учун шаффофдир.

VPN-1 Gateway шлюзи шифрлашнинг бир неча алгоритмини ва бир неча қалитларни бошқариш протоколини мададлайди. Бу шлюз IKE (Internet Key Exchange) каби индустриал стандарт VPN-протоколларни мададлаши сабабли, экстратармоқларни ташкил этишда қўллаш қулай ҳисобланади. Экстратармоқларда VPN бизнес-шериклар орасида хавфсиз алоқани таъминлайди. Check Point компаниясининг VPN-махсулотлари IKE стандартига амал қилади. Шу сабабли улар қарши томон билан музокаралар жараёнида автоматик тарзда шифрлашнинг энг криптобардош алгоритмини (DES ва Triple DES) ва аутентификациялашнинг энг катъий алгоритмини (SHA-1 ва MD5) танлайди. Ундан ташқари, шифрлашнинг махфий қалитлари, максимал химояланишни кафолатлаган ҳолда, тез-тез янгиланади.

VPN-1 Gateway шлюзи виртуал хусусий тармоқдаги иккита охириги узелларга ҳам шифрланган, ҳам шифрланмаган маълумотларни алмашишга имкон берувчи шифрлашнинг танлов режимини мададлайди. Бунинг учун тармоқ маъмури трафиги учун химоялашнинг алоҳида шартлари таъминланадиган иловаларни беради. Сўнгра VPN-1 Gateway ушбу иловалар маълумотларини шифрланган, колган конфиденциал бўлмаган маълумотларни очик кўринишда узатишни бошлайди. Бундай мосланувчанлик VPN-1 Gateway шлюзининг унумдорлигини оширади.

VPN-1 Gateway шлюзи калитларни бошқаришнинг куйидаги механизмларини мададлайди: IPSec учун стандарт бўлган IKE, калитларни бошқаришнинг саноат стандарти FWZ, оммавий протокол SKIP ва калитларни қўл билан тарқатиладиган усули. У X.509 сертификатлари ва Entrus Technologies компаниясининг сертификатлар серверлари технологияси асосида очик PKI калитларни бошқариш инфратузилмасини мададлайди.

VPN-1 Secu Remote мижоз дастурий таъминоти VPN-1 Gateway Шлюзи ёрдамида «тармоқ-масофадаги фойдаланувчи» хилидаги химояланган уланишларни ташкил этишда ишлатилади. Windows 98/XP/NT/2000 бошқарувида ишловчи масофадаги компьютерларга VPN-1Secu Remotening ўрнатилиши мобил ходимларнинг ёки телекомпьютерларнинг корхона бош тармоғи билан Internet орқали химояланган боғланишини таъминлайди. VPN-1 Secu Remotening маълумотларни OSI моделининг тармоқ сатҳида шифрлаши ва расшифровка қилиши ушбу амалларнинг барча иловалар учун шаффофлигини, мавжуд иловаларга ўзгартириш киритишни талаб қилмаган холда, таъминлайди. SecuRemote фойдаланувчиларга VPN-воситалар ўрнатилган бир неча турли тармоқлар билан боғланишига имкон беради.

VPN-1 Accelator Card қурилмаси Chrysalis-ITS компанияси томонидан ишлаб чиқилган аппарат криптографик тезлатгичдир. VPNнинг химояланган каналларида трафикни шифрлаш ва калитларни генерацияловчи амаллар анчагина ҳисоблаш мураккаблигига эга ва VPN орқали узатилувчи трафикнинг ҳажми ошган сари компьютернинг процессори ва хотирасининг хаддан ортиқ юкланиши рўй бериши мумкин. VPN-1 Accelator махсулоти бу муаммони ҳал этиши мумкин.

VPN-1 Accelator Card тезлатгичи VPN-1 Gateway шлюзи билан биргаликда ишлашга аталган ва IKE ва IPSecлар талаб этадиган

барча криптографик амалларни бажаради. VPN-I Accelerator Card бевосита шлюз орқали маъмурланади.

VPN функциялари ўрнатилган SecureZone тармоқлараро экранни Secure Computing компанияси томонидан ишлаб чиқилган ва асосий характеристикалари қуйидагича:

- VPNни мададлаш функциялари – IPSec стандарти, DES ва Triple DES, PKI бошқариш ва Netscape, Entrust ва Verisign компаниялардан X.509 сертификатлари;

- ихтисослаштирилган операцион тизими Secure OS (Unixнинг химояланган варианты) бошқарувида ишлайди;

- қуйидагиларни каноатлантирувчи аппарат платформалар: процессор Intel Pentium, Pentium Pro, ёки Pentium II; RAM-камида 64Мбайт; ташқи қурилмалар қаттиқ диск 4 Гбайт SCSI-2, қайишқоқ дисклар 3,5, СО КОМ. стриммер DAT; SVGA video, PS/2- билан бирга ишлай олувчи сичқон;

- стандарт тармоқ интерфейслари: 2-4 Ethernet, FAST Ethernet, Token Ring ёки FDDI;

- бузилишга бардошлик хоссасига эга.

Secure Computing компанияси MicroSoft Windows муҳитида ишловчи, алоҳида фойдаланувчиларга TCP/IP протоколлари бўйича телефон тармоғи ёки пакетларни коммутацияловчи, оммавий тармоқдан химояланган масофавий фойдаланишни таъминловчи, IPSec билан бирга ишлай олувчи мижоз дастурий таъминотини (SecureClient) ҳам тавсия этади.

VPN функциялари ўрнатилган Raptor Firewall 5.0 тармоқлараро экранни Axent Technologies компанияси томонидан ишлаб чиқилган ва Eagle Firewallнинг модификацияланган маҳсулоти ҳисобланади. Бу тармоқлараро экраннинг характеристикалари қуйидагича:

- VPN мадади тармоқлараро экранга ўрнатилган;

- IPSec стандарти мададланади, дастурий шифрлаш IP (текин тарқатилувчи шифрлаш усули swIPe);

- хавфсизликнинг умумий сиёсати тармоқлараро экран функцияларига ва VPN функцияси ёрдамида туннелланувчи трафикка гааллуқли;

- Windows NT/2000 ва Solaris операцион тизимлар бошқарувида ишлайди.

Axent компанияси масофадаги фойдаланувчилар учун VPNнинг мижоз дастурий таъминотини ҳам тақдим этади. Raptor

Firewall 5.0 версияси IPSec протоколи бўйича химояланган виртуал тармок курилишини таъминлайди.

Gauntlet Global VPN маҳсулоти Network Associates компанияси таркибига кирувчи Trusted Information Systems компаниясининг Gauntlet Firewall тармоклараро экрани учун, ушбу тармоклараро экран муҳитида узвий интеграцияланувчи, кўшимча дастурий маҳсулот ҳисобланади.

IPSec протоколига асосланган Gauntlet Global VPN қисм тизими трафикни криптографик химоялашнинг куйидаги иккита режими мададлайди:

- Smart Gate шлюзлари ёрдамида амалга оширилувчи тармоклараро экрандан тармоклараро экрангача;

- масофадаги миждо дастурий таъминоти Gauntlet PC Extender ёрдамида амалга оширилувчи тармоклараро экрандан масофадаги фойдаланувчи компьютеригача.

Gauntlet Global VPNда шифрлашнинг DES алгоритми ишлатилади. Gauntlet Global VPN сертификация марказининг дастурий таъминоти билан ҳам тақдим этилади. Ушбу дастурий таъминот ёрдамида ташкилотлар X.509 стандартига мос келувчи рақамли сертификатларни генерациялаши ва текшириши мумкин.

VPN куриш функциясини мададловчи BorderManager тармоклараро экрани Novell компаниясининг маҳсулоти бўлиб, нафақат VPN куриш имкониятини, балки фойдаланишни чегаралашни, пакетларни филтрлаш ва тармок манзилларини трансляциялашни таъминлайди, воситачи HTTPнинг хизматларини тавсия этади, Web саҳифаларини кешлайди, канал сатҳида шлюзларга эга, кўп протоколли маршрутлашни бажаради ва масофадан фойдаланишни мададлайди.

Border Manager тармоклараро экраннинг NDS (Novell Directory Service) каталоглари хизмати билан узвий интеграцияси химояланган виртуал тармокларни самарали бошқаришга имкон беради. Шифрлаш калитининг тақсимоти RSA криптотизими ва Диффи-Хеллман алгоритми бўйича амалга оширилади. Ахборот пакетларини криптографик беркитиш ва аутентификациялашда RC2 ва RSA криптотизимлардан фойдаланилади. Border Managerнинг бир версиясида IPSec протоколи мададланади. Border Manager тармоклараро экран асосида курилган химояланган виртуал тармокларда браундмаўэрлардан бирининг асосий бўлиши, бошқариш маркази ролини бажариши лозим.

Ихтисослаштирилган дастурий таъминот асосидаги VPN.

VPN куришда ихтисослаштирилган дастурий воситалар кенг қўлланилади. VPN куришнинг дастурий воситалари химояланган туннелларни факат дастурий шакллантиришга имкон беради ва улар ишлайдиган компьютерни TCP/IP маршрутизаторига айлантиради. Бу маршрутизатор шифрланган пакетларни қабул қилади, расшифровка қилади ва локал тармоқ орқали тайинланган нуктага узатади. Охири вақтда бундай маҳсулотларнинг етарлича сони пайдо бўлди. Ихтисослаштирилган дастурий таъминот кўринишида VPN-шлюзлар, VPN-серверлар ва VPN-мижозлар бажарилиши мумкин.

Дастурий усул бўйича амалга оширилган VPN-маҳсулотлар унумдорлик нуктаи-назаридан ихтисослаштирилган аппарат курилмалардан қолишсада, дастурий маҳсулотлар масофадаги фойдаланувчиларга етарли унумдорликни осонгина таъминлайди. Дастурий маҳсулотларнинг шубҳасиз афзаллиги ишлатилишида мосланувчанлиги ва қолайлиги ҳамда нисбатан юкори бўлмаган нархидир. Аппарат шлюзларни ишлаб чиқарувчи кўпгина компаниялар (масалан, Time Step, VPNet, Shiva) ўзларининг маҳсулотларига стандарт операцион тизимда ишлашга мўлжалланган VPN-мижознинг дастурий амалга оширилишини кўшадилар.

Microsoft компаниясининг RAS ва RRAS дастурий маҳсулотлари. Microsoft компаниясининг масофадан фойдаланувчи дастурий сервери RAS (Remote Access Service) машхур PPP (Point to Point Protocol) протоколнинг кенгайтирилган варианты-химояланган канал протоколи PPTPни (Point-to-Point Tunneling Protocol) ўрнатилиши эвазига VPN технологияни мададлайди. Трафикни туннеллаш очик IP-тармоқ бўйича узатиладиган стандарт PPP- фреймларни IP-датаграммаларга инкапсуляциялаш ва кейин шифрлаш орқали амалга оширилади.

RASнинг асосий афзаллиги – тежамлилиги, камчилиги – унумдорлигининг пастлиги. Ҳозирда бу маҳсулотнинг такомиллаштирилган версияси – RRAS (Routing and Remote Acces Service) пайдо бўлди. RRAS таркибидаги такомиллаштирилган дастурий кўп протоколли маршрутизатор маршрутлашнинг RIP (Routing Information Protocol) ва OSFP (Open Shortest Path First) протоколларини мададлайди. RRASнинг бу хусусиятлари ундан VPN шлюзи каби «тармоқ-тармоқ» ўзаро алоқасида фойдаланишга имкон яратади.

RAS хизмати масофадан фойдаланувчиларнинг кўпчилигига (256 тагача) битта Windows NT серверига уланиш ва локал тармоқ ресурсларидан IPX ва TCP/IP протоколлари бўйича фойдаланиш имкониятини беради.

Alta Vista Tunnel 98 маҳсулотлари оиласи учта маҳсулотни ўз ичига олади: Telecommuter Server, Extranet Server, AltaVista Tunnel Client. Telecommuter Server сервери Internet корпоратив фойдаланувчилар орасида химояланган туннеларни Internet оркали ташкил этишга аталган. Extranet Server сервери ёрдамида тармоқлар орасида химояланган канал ҳосил қилинади. Бу иккала сервер умумий Alta Vista Tunnel Server номига эга. Alta Vista Tunnel Client VPN клиентнинг дастурий таъминотидир.

Alta Vista Tunnel 98 оиласининг барча маҳсулотлари фойдаланувчиларни аутентификациялашда ва RSA криптографик тизимнинг сессия калитларини алмашишда ишлатилади. Фойдаланувчиларни аутентификациялашда Security Dynamics компаниясининг аппарат калити SecurID ҳам ишлатилиши мумкин. Мижоз ва сервер янги сессия калитлари билан ҳар 30 минутда алмашишади.

Маълумотларни шифрлашда RC4 алгоритмидан фойдаланилади. Маҳсулотларнинг халқаро версияси RC4 алгоритми бўйича шифрлашда 56 ёки 40 битли калитлардан фойдаланади. Маълумотларни аутентификациялаш ва яхлитлигини таъминлаш учун MD5 хэш-функцияси ишлатилади. Alta Vista Tunnel 98 оиласининг маҳсулотлари LZO алгоритми бўйича маълумотларни зичлаштириши мумкин.

Ушбу оила маҳсулотлари аксарият замонавий операцион тизимлар – Windows NT/2000, Unix BSD/OS, Unix Free BSD ва Digital UNIX бошқарувида ишлаши мумкин. Windows NT/2000 операцион муҳитда Alta Vista Tunnel Server маҳсулоти бир вақтнинг ўзида 200 туннел уланишларини, UNIX операцион муҳитда эса 2000 гача туннел уланишларни мададлайди.

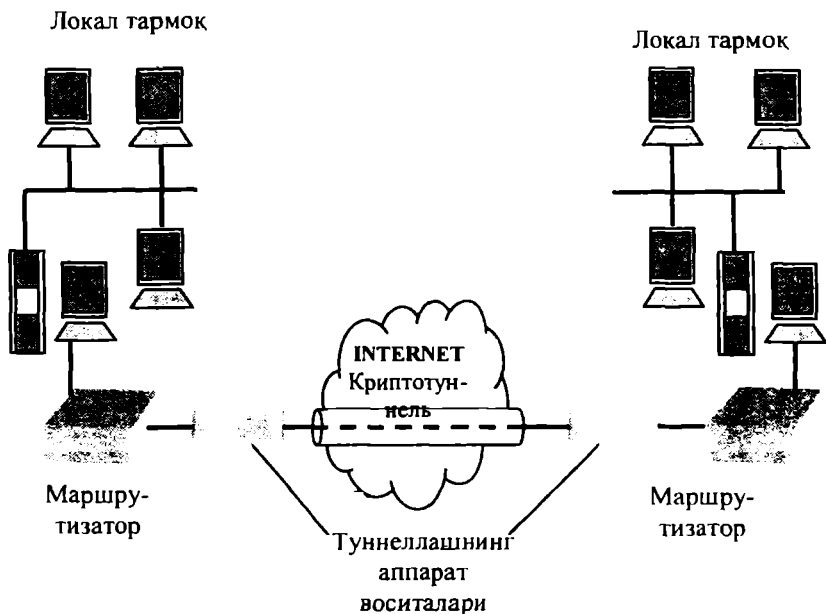
Ихтисослаштирилган аппарат воситалари асосидаги VPN. Ихтисослаштирилган аппарат курилмалари асосидаги VPN-воситаларнинг асосий афзаллиги-юқори унумдорлиги. VPN-пакетларни ишлашда керакли ҳисоблашлар ҳажми оддий пакетларни ишлашдагига нисбатан 50–100 марта ошади. Аппарат воситалари асосидаги VPNларда юқори тезликка уларда шифрлашнинг ихтисослаштирилган микросхемаларда амалга оширилиши эвазига эришилади. Бундай VPN-воситалар кўпинча IPSec протоколи билан

бирга ишлай олади ва локал тармоқлар орасида криптохимояланган туннелларни шакллантиришда ишлатилади. Баъзи ишлаб чиқарувчиларнинг VPNни шакллантирувчи асбоб-ускуналари бир вақтнинг ўзида «масофадаги компьютер-локал тармоқ» режимида химояланган боғланишни ҳам мададлайди.

Аппарат VPN-шлюзлар алоҳида аппарат қурилмаси кўринишида бўлади. Уларнинг асосий вазифаси -- трафикни юқори унумдорлик билан шифрлаш. Бу VPN-шлюзлар X.509 рақамли сертификатлари PKI очик калитларни бошқариш инфратузилмалари билан ишлайди, LDAP бўйича маълумот берадиган хизматлар билан ишлашни мададлайди.

Аппарат химояланган туннел ишлашининг энг оддий варианты - аппарат шифрлашдан фойдаланиб уланишларни яратиш. Туннеллашнинг аппарат воситалари одатда, локал ва глобал тармоқларнинг туташган жойида, маршрутизатордан кейин ўрнатилади (7.9-расм) ва автоматик тарзда берилган трафикни шифрлайди. Бундай ёндашишнинг асосий афзаллиги шундаки, ишчи станциялар ва маршрутизаторларнинг шакллантирилувчи криптотуннеллар билан ҳеч қандай боғлиқлиги йўқ, VPN ўрнатилганида уларни конфигурациясини ўзгартириш талаб этилмайди.

Аппарат шлюзларни инсталляциялаш дастурий шлюзлар ва маршрутизаторлар ва брендмауэрлар асосидаги шлюзларга нисбатан жуда осон амалга оширилади. Бундай қурилмаларни бошқариш иккита асосий масалани ечишни талаб этади: сертификация маркази орқали калитларни бошқариш ва химояланган туннеллашни бошқариш. Аксарият аппарат туннеллашнинг асосий сертификатация марказлари Windowsга мўътавоқ дастурий давоналардир. Аппарат туннелларини марказлашган ҳолда битта иш жойида туриб бошқариш мумкин. Бошқарувчи дастурлар туннелнинг асосий химоялаш функцияларининг бажарилишини ва хатоликларни ишлашни таъминлайди.



7.9-расм. Ихтисослаштирилган аппарат воситалар асосида туннеллаш схемаси.

Ихтисослаштирилган аппарат VPN-воситалар нархидан ташқари барча бўлиши мумкин бўлган кўрсаткичлари бўйича етакчи ҳисобланади.

TimeStep компанияси корхоналарда кенг масштабли ахборот алмашинуви учун IPSec билан бирга ишлай олувчи PERMIT Enterprise Snite деб аталувчи VPN-маҳсулотни ишлаб чиқди. Ушбу маҳсулот Internet орқали масофадан фойдаланишни ташкил этиш, корпоратив интратармоқ ва экстратармоқларни куриш учун тўлиқ ечим ҳисобланади. PERMIT Enterprise мавжуд тармоқларда тармоқ ва охириги фойдаланувчи унумдорлигига жиддий таъсир қилмаган ҳолда, осонгина сафланади, унинг масштабланувчи архитектураси бирнеча VPNларни яратиш ва уларни бошқариш имкониятини беради.

Компания томонидан шлюзнинг куйидаги тўртта модификацияси тақдим этилади:

– PERMIT/Gate 1520 нархи қиммат бўлмаган автоном қурилма бўлиб, қувватли телекомпьютерлар ёки SOHO сўнфидаги катта бўлмаган масофадаги офислар учун ишлатилади;

– PERMIT/Gate 2520 ва PERMIT/Gate 4520 ўтказиш қобилияти, мос ҳолда 4 ва 1- Мбит/с, бўлинмалар офислари ва кичик локал ҳисоблаш тармоқларига мўлжалланган, масофадаги юзлаб фойдаланувчиларни мададлайди;

– PERMIT/Gate 7520 (70 Мбит/с) ички локал ҳисоблаш тармоқларида ишлатилади ва масофадаги минглаб фойдаланувчиларни мададлайди.

PERMIT/Gate шлюзларининг муҳим афзаллиги – трафик ишланишининг юқори унумдорлигини таъминлаш мақсадида DES ва 3-DES шифрлаш алгоритмининг аппарат амалга оширилиши.

PERMIT/Gate7520 шлюзи IPSecнинг амалга оширилишининг аппарат воситаси билан ҳам жиҳозланганлиги, унумдорликка таъсир қилмаган ҳолда минглаб VPN уланишларни мададлашга имкон беради. Бу, зарурият туғилганда, корпоратив тармоқни осонгина кенгайтириш имконини яратади.

Мижоз дастурий таъминоти PERMIT/Client IPSec протоколини мададлайди ва масофадаги фойдаланувчиларга ўзининг тармоғи билан хавфсиз боғланиш имконини беради. Ушбу дастурий таъминот Windows95/98/XP/NT ёки MAC OS 7.1. бошқарувида ишловчи алоҳида ишчи станция томонидан манзилланган тармоқ трафигини химоялайди.

PERMIT/Gate шлюзларининг ҳар бири дастурли утилита PERMIT/Config билан бирга тақдим этилади. Бу дастурли утилита виртуал хусусий тармоқнинг ҳар қандай нуктасидан бир неча шлюзларнинг дастурий таъминотини масофадан конфигурациялаш, бошқариш ва модификациялашга имкон яратади.

VPNет компанияси VPN қуриш учун дастлабки интеграцияланган ечимлардан бири – VPNwareни тақлиф этди. Бу ечим ўз ичига қуйидаги маҳсулотларни олади:

– учта VPN-шлюз: штаб қароргоҳи ва йирик локал тармоқлар учун VSU.1100, бўлинмалар учун VSU-1010 ва катта бўлмаган офислар учун VSU-10;

- iPass компаниясидан дастурий сервер RoamServer;
- миждоз дастурий таъминоти VPNremote;
- бошқаришнинг дастурий тизими VPNmanager.

VPNет асбоб-ускуналари, «тармоқ-тармоқ» ва «тармоқ – масофадаги фойдаланувчи» хилидаги уланишларга мўлжалланган VPNни мададлайди. Ишлатиладиган махсулотларга боғлиқ холда VPNware тизими IPsecнинг стандарт амалга оширилиши ёрдамида оммавий IP тармоқ орқали узатиладиган маълумотларни химоялаш билан 25дан 5000гача фойдаланувчиларни мададлаши мумкин. Бу тизим турли масштабда тармоқларда йирик корхонанинг марказий локал тармоғида, бўлинма ва катта бўлмаган офис локал тармоғида ва масофадаги фойдаланувчиларни химоялашда ишлатилиши мумкин.

VSU-1010 ва VSU-10 шлюзлар IPsec билан бирга ишлай олади ва DES ва 3-DES алгоритмлари бўйича маълумотларни шифрлашни аппарат мададлашга эга. VPNнинг бошқарувчи иловаси статистикани йиғишга ва VPNдаги ходисаларни қайдлашга имкон беради. Ҳар хил VPNларни бошқаришни марказлаштириш эвазига химояни бошқаришнинг бошқа функцияларини соддалаштириш ва марказлаштириш, масалан, корпоратив брданмауэр яхлитлигини бузилишини назоратини таъминлаш мумкин. VPNет махсулотларининг афзаллиги-мавжуд тармоқ билан интеграцияланишининг соддаллиги, унумдорлигининг нисбатан юкорилиги ва IPsecнинг тўла амалга оширилиши.

Мижоз дастурий таъминоти VPNremote IPsec протоколини мададлайди ва Windows NT муҳитида ҳамда телефон тармоқлари орқали фойдаланилганда масофадаги ва мобил фойдаланувчилар, телекомпьютерлар ва бизнес-шерикларнинг маълумотларини химоялашда Windows95/98/XP муҳитида ишлайди.

Бошқарув тизими VPNmanager виртуал хусусий тармоқларни яратиш, конфигурациялаш ва бошқариш учун махсус ишлаб чиқилган. Тармоқ маъмури ушбу тизим ёрдамида, график интерфейсни ишлатиб масофадаги фойдаланувчиларни ва бизнес-шерикларни VPNга осонгина қўшиши мумкин. VPN мижозларини масофадан маъмурлашга Dyna-Policy функцияси атайган.

LanRover VPN Gateway шлюзи Shiva компанияси томонидан тақдим этилган бўлиб, ICISA томонидан сертификацияланган. Бу шлюз очик тармоқ орқали узатиладиган маълумотларни химоялаш технологияларининг кенг тўпламини мададлайди. Яхлитликни ва конфиденциалликни таъминлаш, фойдаланишнинг назорати, X.509нинг рақамли сертификатларига, Security Dynamics аппарат

калитларига, RADIUS протоколи ёки доменли схемага асосланган аутентификациялашнинг турли схемалари бу тўпламга киради.

Маълумотларни аппарат шифрлаш DES ёки 3-DES алгоритмлари асосида амалга оширилади. LanRover VPN Gateway шлюзлари Pentium-технологиянинг тезлиги, шифрловчи ихтисослаштирилган интеграл схемаларнинг тезкорлиги ва реал вақтнинг кўп вазидали операциялар тизим реактивлигининг ноёб бирикмасидан фойдаланади. Бу шлюзлар ишлатишда қулай ва уларнинг ишлаши охириги фойдаланувчилар учун шаффоф. Бу шлюзлар билан ишлаш қулайлигини таъминлаш мақсадида график фойдаланувчи интерфейсли утилита VPN manager тақдим этилади. Бу утилита маъмурга ҳар қандай Windows 95/NT тизимидан бирданига бир неча шлюзларни бошқаришни таъминлайди.

7.4. Канал ва сеанс сатҳларда химояланган виртуал каналларни қуриш

Канал сатҳида химояланган виртуал каналларни шакллантириш протоколлари.

PPTP, L2F ва L2TP протоколлар OSI модели канал сатҳининг туннеллаш протоколлари ҳисобланади. Ушбу протоколларнинг умумий хусусияти шундан иборатки, улар очик тармоқ, масалан, Internet орқали корпоратив тармоқ ресурсларидан химояланган кўп протоколли масофадан фойдаланишни ташкил этишда ишлатилади. Учала протоколни, одатда, химояланган канални шакллантириш протоколларига мансуб деб ҳисоблайдилар. Аммо бу таърифга уза тиладиган маълумотларни туннеллашни ва шифрлашни таъминловчи фақат PPTP протоколи аниқ мос келади, чунки L2F ва L2TP протоколлар фақат туннеллаш функцияларини мададлайди. Туннелланган маълумотларни химоялаш (шифрлаш, яхлитлик, аутентификация) учун бу протоколларда қўшимча, протокол, ҳусусан, IPSec протоколи ишлатилади.

PPTP протоколи маълумотларни IP, IPX ва NetBEUI протоколлари бўйича алмашиш учун химояланган каналларни яратишга имкон беради. Ушбу протоколлар маълумотлари PPP кадрларига жойланади ва сўнгра PPTP протоколи воситасида IP протоколининг пакетларига инкапсуляцияланади ва шу протокол ёрдамида шифрланган кўринишда ҳар қандай TCP/IP тармоғи орқали ташилади.

PPP сессияси доирасида узатилувчи пакетлар куйидаги тузилмага эга (7.10-расм):

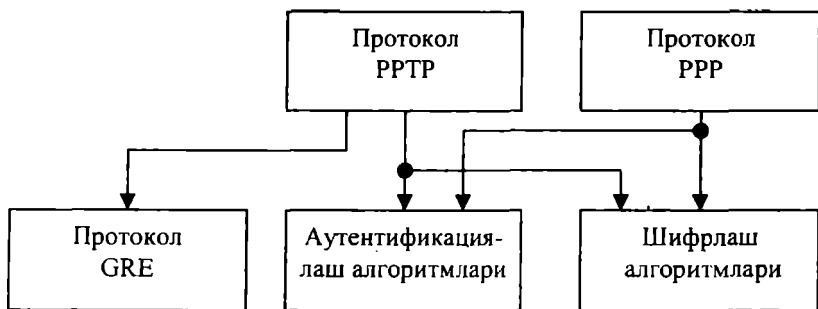
- Internet ичида ишлатилувчи канал сатхининг сарлавҳаси, масалан, Ethernet кадрининг сарлавҳаси;
- таркибида пакетни жўнатувчи ва қабул қилувчи манзиллари бўлган IP сарлавҳаси;
- маршрутлаш учун инкапсуляциялашнинг умумий усулининг сарлавҳаси GRE(Generic Routing Encapsulation);
- таркибида IP, IPX ёки NetBEUI пакетлари бўлган дастлабки пакет PPP.

Узатиладиган кадр сарлавҳаси	IP – сарлавҳа	GRE – сарлавҳа	PPP – сарлавҳа	Шифрланган маълумотлар PPP	Узатиладиган кадр охири
------------------------------	---------------	----------------	----------------	----------------------------	-------------------------

7.10-расм. PPTP туннели бўйича жўнатилади пакет тузилмаси.

Тармоқнинг қабул қилувчи узели IP пакетлардан PPP кадрларни чиқариб олади, сўнгра PPP кадрдан дастлабки пакет IP, IPX ёки NetBEUI пакетини чиқариб олиб уни локал тармоқ бўйича муайян манзилга жўнатади. Канал сатхининг инкапсуляцияловчи протоколларининг кўп протоколлилиги (унга PPTP протокол ҳам тааллуқли), уларнинг янада юқорирок сатҳнинг химояланган канал протоколларидан афзаллигидир. Масалан, агар корпоратив тармоқда IPX ёки NetBEUI ишлатилса, IPSec ёки SSL протоколларини ишлатиб бўлмайди, чунки улар IP тармоқ сатхининг фақат битта протоколига мўлжалланган.

Инкапсуляциялашнинг мазкур усули OSI моделининг тармоқ сатҳи протоколларига боғлиқ бўлмасликни таъминлайди ва очик IP-тармоқлар орқали ҳар қандай локал тармоқлардан (IP, IPX ёки NetBEUI) химояланган масофадан фойдаланишни амалга оширишга имкон беради. PPTP протоколига мувофиқ, химояланган виртуал канал яратишда масофадаги фойдаланувчини аутентификациялаш ва узатилувчи маълумотларни шифрлаш амалга оширилади (7.11-расм).



7.11-расм. PPTP протоколи архитектураси.

Масофадаги фойдаланувчини аутентификациялашда PPP учун қўлланиладиган турли протоколлардан фойдаланиш мумкин. Microsoft компанияси томонидан Windows 98/XP/NT/2000 га киритилган PPTPнинг амалга оширилишида аутентификациялашнинг куйидаги протоколлари мададланади: парол бўйича аниқлаш протоколи PAP (Password Authentication Protocol), қўл беришида аниқлаш протоколи MSCHAP (Microsoft Challenge – Handshaking Authentication Protocols) ва аниқлаш протоколи EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). PAP протоколдан фойдаланилганда идентификаторлар ва пароллар алоқа линиялари орқали шифрланмаган кўринишда узатилади, бунда аутентификациялашни фақат сервер ўтказди. MSCHAP ва EAP-TLS протоколларидан фойдаланилганда нияти бузук одамнинг ушлаб қолинган шифрланган паролли пакетдан қайта фойдаланишидан химоялаш ва мижоз ва VPN-серверни аутентификациялаш таъминланади.

PPTP ёрдамида шифрлаш Internet орқали жўнатишда маълумотлардан ҳеч ким фойдалана олмаслигини кафолатлайди. Шифрлаш протоколи MPPE (Microsoft Point-to-Point Encryption) фақат MSCHAP (1 ва 2 версиялари) ва EAP-TLS билан бирга ишлай олади ва мижоз ва сервер орасида параметрлар мувофиқлаштирилишида шифрлаш калитининг узунлигини автоматик тарзда танлай олади. MPPE протоколи узунлиги 40, 56 ёки 128 бит бўлган калитлар билан ишлашни мададлайди.

PPTP протоколи ҳар бир олинган пакетдан сўнг шифрлаш калити кийматини ўзгартиради. MPPE протоколи «нукта-нукта» ҳи-пидаги алоқа каналлари учун ишлаб чиқилган бўлиб, бу алоқа ка-

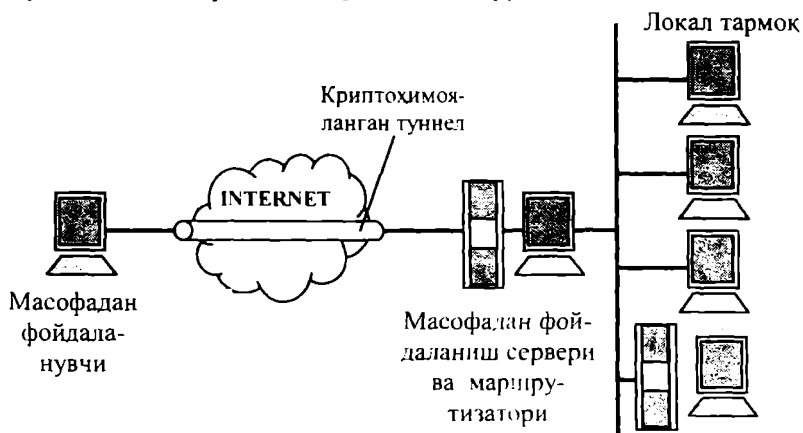
налларида пакетлар кетма-кет узатилади ва маълумотлар йўқотилиши жуда кам. Бу вазиятда навбатдаги пакет учун калит киймати олдинги пакетнинг расшифровкаси натижасига боғлиқ. Умумфойдаланувчи тармоқ орқали виртуал тармоқ куришда бу шартларга риоя қилиш мумкин эмас, чунки маълумотлар пакети кўпинча қабул қилувчига жўнатилган кетма-кетликда келмайди. Шунинг учун РРТР шифрлаш калитини ўзгартиришда пакетларнинг тартиб рақамидан фойдаланади. Бу расшифровка қилишни олдинги қабул қилинган пакетларга боғлиқ бўлмаган ҳолда амалга оширишга имкон беради.

РРТР протоколи учун қўллашнинг қуйидаги иккита асосий схемаси аниқланган:

- масофадан фойдаланувчининг Internet билан тўғридан-тўғри уланишидаги туннеллаш схемаси;

- масофадан фойдаланувчининг Internet билан провайдер орқали телефон линияси бўйича уланишидаги туннеллаш схемаси.

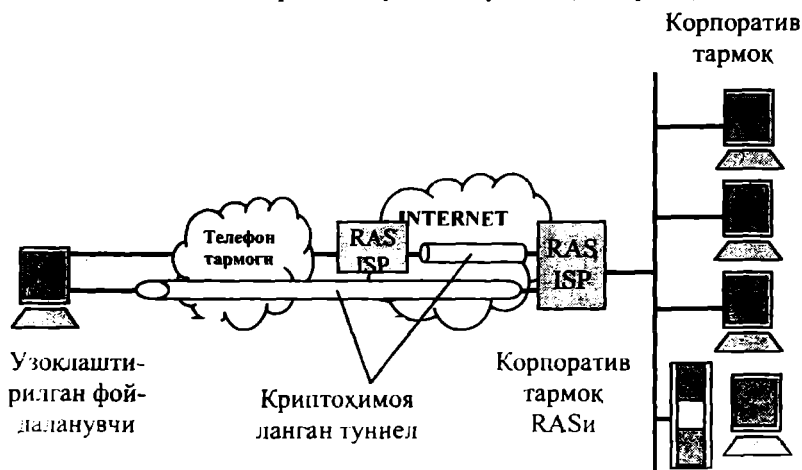
Туннеллашнинг биринчи схемаси амалга оширилганида (7.12-расм) масофадан фойдаланувчи Windows 98/XP/NT таркибидаги масофадан фойдаланиш сервери RAS (Remote Access Service)нинг мижоз қисми ёрдамида локал тармоқ билан масофавий боғланишни ўрнатади. Сўнгра фойдаланувчи локал тармоқдан масофадан фойдаланиш серверига, унинг IP манзилини кўрсатиб мурожаат этади ва у билан РРТР протоколи бўйича алоқа ўрнатади.



7.12 -расм. Масофадан фойдаланувчи компьютерини Internetга тўғридан-тўғри уланишидаги туннеллаш схемаси.

Масофадан фойдаланиш сервери вазифасини локал тармоқнинг чегара маршрутизатори бажариши мумкин. Масофадан фойдаланувчининг компютерида Windows 98/XP/NT таркибидаги RAS сервернинг мижоз қисми ва PPTPнинг драйвери, масофадан фойдаланувчи локал тармоқнинг серверида эса Windows NT Server таркибидаги RAS сервери ва PPTP драйвери ўрнатилиши шарт. PPTP протоколи ўзаро алоқадаги томонлар алмашадиган бир нечта хизматчи хабарни аниқлайди. Хизматчи хабарлар TCP протоколи бўйича узатилади. Муваффақиятли аутентификациялашдан сўнг химояланган алмашиш жараёни бошланади. Локал тармоқнинг ички серверлари PPTP протоколини мададламаслиги мумкин, чунки чегара маршрутизатор IP пакетлардан PPP кадрларини чиқариб олиб уларни локал тармоқ орқали керакли IP, IPX ёки NetBIOS форматида жўнатади.

Масофадаги компютерни Internetга телефон линияси бўйича провайдер ISP (Internet Service Provider) орқали улашда туннеллаш схемасининг иккита варианты бўлиши мумкин (7.13-расм).



7.13-расм. Масофадан фойдаланувчи компютерини ISP провайдери орқали телефон линиясидан фойдаланиб Internetга улашини туннеллаш схемасининг иккита варианты.

Схеманинг биринчи вариантнинг қурилиши протокол PPTPнинг провайдер ISPнинг масофадан фойдаланиш сервери ва чегара корпоратив маршрутизатор орқали мададланиши тахминига

асосланган. Сервер одатда, фойдаланувчиларнинг улашишни таъминловчи кўп сонли тезкорлиги паст портларга эга. Провайдер ISPнинг сервери RAS ва маршрутизатор орасида химояланган канал ҳосил бўлади. Мохияти бўйича бу - «шлюз-шлюз» хилидаги химояланган канал варианты.

Бу вариантда масофадан фойдаланувчининг компьюттери протокол PPTPни мададламаслиги мумкин. Масофадаги фойдаланувчи стандарт протокол PPP ёрдамида провайдер ISPда ўрнатилган масофадан фойдаланиш сервери RAS билан боғланади ва аутентификациялашни провайдерда ўтайди.

Провайдернинг сервери RAS фойдаланувчининг исми бўйича фойдаланувчиларнинг ҳисоб маълумотлари базасидан маршрутизаторнинг IP-манзилини топади. Бу маршрутизатор чегара маршрутизатори ва ушбу фойдаланувчининг локал тармоқдан масофадан фойдаланиш сервери ҳисобланади. Бу маршрутизатор билан провайдер сервери RAS Intrenet орқали PPTP протоколи бўйича сессия ўтказади. Провайдернинг сервери RAS локал тармоқдан масофадан фойдаланиш серверига фойдаланувчининг идентификаторини ва бошқа маълумотларни узатади. Улар асосида бу сервер CHAP протоколи бўйича фойдаланувчини яна аутентификациялайди. Агар фойдаланувчи иккинчи аутентификациялашдан (бу унинг учун шаффоф бўлади) муваффақиятли ўтса, провайдернинг RASи бу тўғрида фойдаланувчини PPP протокол бўйича огохлантиради ва сўнгра, провайдернинг масофадан фойдаланувчи сервери ва локал тармоқ орасида химояланган виртуал канал шаклланади.

Масофадан фойдаланувчининг компьюттери локал тармоқ IP, IPX, ёки NetBIOS билан ўзаро алоқа пакетларини PPP кадрларига жойлаб провайдернинг масофадан фойдаланувчи сервери RASга узатади. Провайдернинг RASи аталган манзил сифатида чегара маршрутизатори манзилини, манба манзили сифатида ўзининг шахсий IP-манзилини кўрсатган ҳолда PPP кадрларининг IP пакетларга инкапсуляциясини амалга оширади. Провайдернинг масофадан фойдаланувчи сервери ва локал тармоқ орасида узатишга аталган PPP пакетлари симметрик шифрда шифрланади. Бунда симметрик махфий калит сифатида CHAP протоколи бўйича аутентификациялаш учун провайдер RASининг ҳисоб маълумотлари базасида сақланувчи фойдаланувчи паролнинг дайджести ишлатилади. Симметрик шифрлаш алгоритмлари сифатида DES ёки RC-4 алгоритм ишлатилади.

Тавсиф этилган вариант кенг тарқалмади, чунки протокол PPTP, асосан, Microsoft компаниясининг махсулотларида – RAS Windows NT 4.0 нинг мижоз ва сервер қисмларида ҳамда RAS Windows 98/XPнинг мижоз қисмида амалга оширилган. Провайдерлар масофадан фойдаланиш сервери сифатида одатда RAS Windows NTга нисбатан қувватлироқ воситалардан фойдаланади. Бунда протокол PPTP Internet провайдерларининг масофадан фойдаланиш серверлари RAS орқали доимо мададланмайди. Ундан ташқари, бу схемада маълумотлар фойдаланувчи компьютери ва Internet провайдери орасида химояланмаган холда узатилади, натижада, унинг хавфсизлиги жиддий ёмонлашади.

Microsoft компанияси томонидан PPTP протоколини қўллашнинг яна бир бошқа схемаси тавсия этилган. Бу схемага биноан PPTP протоколининг провайдернинг масофадан фойдаланиш сервери томонидан мададланиши талаб этилмайди. Туннеллашнинг бу варианты (7.13-расм) кенг тарқалди.

Таъкидлаш лозимки, бу схемада корпоратив тармоқнинг чегара маршрутизатори, олдинги схемадагидек PPTP протоколни мададлаши шарт. Бундай маршрутизатор сифатида, хусусан, RAS хизмати ўрнатилган дастурий маршрутизатор Windows NT 4.0 ишлатилиши мумкин. Умуман, RAS хизмати ва PPTP протоколи ишлайдиган, масофадаги мижоз компьютер ива корпоратив тармоқ ичидаги компьютер орасида химояланган канални ярагиш мумкин.

Ушбу схемага биноан фойдаланувчи икки марта масофадан уланишни ўрнатиши лозим. Биринчи марта фойдаланувчи провайдернинг масофадан фойдаланиш серверига модем бўйича кўнғирок қилиб, PPP протоколи бўйича у билан алоқа ўрнатади ва провайдер ISP томонидан мададланувчи протоколларнинг бирига (PAP ёки CHAP) ёки терминал диалогига мувофиқ аутентификациядан ўтади. ISP провайдеридан аутентификациядан муваффақиятли ўтганидан сўнг фойдаланувчи локал тармоқдан масофадан фойдаланиш сервери билан, унинг IP-манзиллини кўрсатиб уланишни ўрнатади. Натижада, масофадаги компьютер ва локал тармоқ RAS орасида PPTP протоколи бўйича сессия ўрнатилади. Мижоз яна, энди ўзининг корпоратив тармоғи серверида аутентификацияланади. Масофадан фойдаланиш сервери фойдаланувчининг ҳақиқийлигини ўзининг ҳисоб маълумотлари базаси асосида текширади. Муваффақиятли аутентификациялашдан сўнг ахборотни химояланган алмашиш жараёни бошланади.

Криптохимояланган туннелнинг чегара курилмаларининг ўзаро алоқаси учун PPTP протоколида бошқарувчи хабарлар кўзда тутилган бўлиб, бу бошқарувчи хабарлар туннелни ўрнатиш, мададлаш ва узиш учун аталган. Бошқарувчи хабарларни алмашиш мижоз ва PPTPнинг сервери орасида ўрнатилувчи TCP-уланиш бўйича амалга оширилади. Бу уланиш бўйича узагиладиган пакетларда канал сатхи сарлавҳаси билан бир қаторда IP протоколининг сарлавҳаси, TCP протоколининг сарлавҳаси ва пакет маълумотлари соҳасидаги PPTPнинг бошқарувчи хабари бўлади.

L2F протоколи Cisco System компанияси томонидан OSI моделининг канал сатҳида химояланган виртуал гармок куриш учун, PPTP протоколига альтернатива сифатида ишлаб чиқилган. L2F протоколи турли тармок протоколлари томонидан мададланиши билан ажралиб туради ва Internet провайдерлари учун фойдаланишда анча қулай. L2F протоколи масофадаги фойдаланувчи компютери билан провайдер сервери алоқасини ташкил этишда масофадан фойдаланишнинг турли протоколларини (PPP, SLIP ва х.) ишлатишга йўл қуяди. Туннел орқали пакетларни ташишда ишлатилувчи очик тармок IP протоколи асосида ва бошқа, хусусан, X.25 протоколи асосида ишлаши мумкин.

L2F протоколи қуйидаги хусусиятларга эга:

– ҳақиқийликни текширувчи муайян протоколга катъий боғланмаганликни тахминловчи аутентификациялаш муолажаларининг мосланувчанлиги;

– охириги тизимлар учун шаффофлиги, яъни локаль тармокнинг ишчи станциялари ва масофадаги тизимга химоялаш серверидан фойдаланиш учун махсус дастурий таъминот талаб этилмайди;

– воситалар учун шаффофлиги, яъни масофадаги фойдаланувчиларни авторизациялаш локаль тармокнинг масофадан фойдаланиш серверига фойдаланувчиларни бевосита уланишига ўхшаб амалга оширилади;

– аудитнинг тўлиқлиги, яъни локаль тармок серверидан фойдаланиш ходисасини кайдлаш нафакат масофадан фойдаланиш сервери томонидан, балки провайдер сервери томонидан ҳам амалга оширилади.

L2F протоколининг спецификациясига мувофиқ химояланган туннелни ҳосил қилишда қуйидаги протоколлар ишлатилади:

– дастлабки инкапсуляцияланувчи протокол – бу протокол (IP, IPX, ёки NetBEUI) асосида локаль тармок ишлайди;

– протокол – «йўловчи» – бу протоколга дастлабки протокол инкапсуляцияланади ва бу протоколнинг ўзи ҳам очик тармок орқали масофадан фойдаланганда инкапсуляцияланиши мумкин; PPP протоколи тавсия этилади;

-- бошқарувчи (инкапсуляцияловчи) протокол, туннелни яратишда, мададлашда ва узишда ишлатилади (бундай протокол сифатида L2F ишлатилади);

– провайдер протоколи, инкапсуляцияланувчи протоколларни (дастлабки протокол ва протокол – «йўловчи») ташишда ишлатилади; энг кўп тарқалган провайдер протоколи IP протоколдир.

Таъкидлаш лозимки, L2F технологиясидан фойдаланилганда провайдернинг масофадан фойдаланиш сервери фойдаланувчини аутентификациялашни фақат виртуал канал яратилиши зарурлигини аниқлаш ва исталган локал тармокнинг масофадан фойдаланиш сервери манзилени топишда ишлатади. Ҳақиқийликни яқиний текшириш локал тармокнинг масофадан фойдаланиш сервери томонидан, у билан провайдер сервери уланганидан сўнг, бажарилади.

L2F протоколининг куйидаги камчиликларини кўрсатиш мумкин:

– унда IP протоколининг жорий версияси учун ахборот алмашинувининг охириги нукталари орасида криптохимояланган туннел яратиш кўзда тутилмаган;

– виртуал химояланган канал фақат провайдернинг масофадан фойдаланиш сервери ва локал тармокнинг чегара маршрутизатори орасида ярағилиши мумкин, бунда масофадаги фойдаланувчи компьютери билан провайдер сервери орасидаги жой очик қолади.

Ҳозирда L2F протоколи Internet стандарти лойихаси мақомига эга бўлган L2TP протоколига сингдирилган.

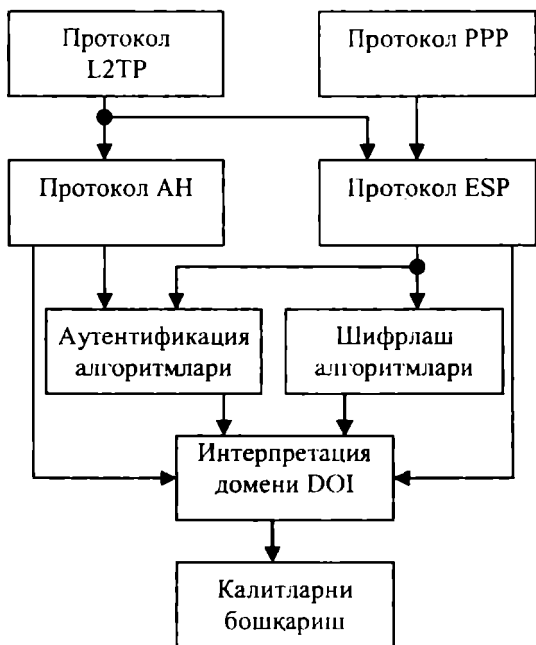
L2TP протоколи IETF ташкилотида Microsoft ва Cisco Systems компаниялари мададида ишлаб чиқилган. L2TP протоколи ихтиёрий муҳитли умуммақсад тармок орқали PPP-графикни химояланган туннеллаш протоколи сифатида ишлаб чиқилган.

PPTPдан фарқли холда L2TP протоколи IP протоколига боғланган эмас, шу сабабали ундан пакетларни коммутацияловчи тармокларда, масалан, ATM (Asynchronous Transfer Mode) ёки кадрларни ретрансляцияловчи (frame relay) тармокларда фойдаланиш мумкин.

L2TP протоколида PPTP ва L2F протоколларининг нафақат яхши хусусиятлари бирлаштирилган, балки янги функциялар, жум-

ладан, IPSec протоколлари стекининг АН ва ESP протоколлари билан ишлаш имконияти қўшилган.

L2TP протоколининг архитектураси 7.14-расмда келтирилган.



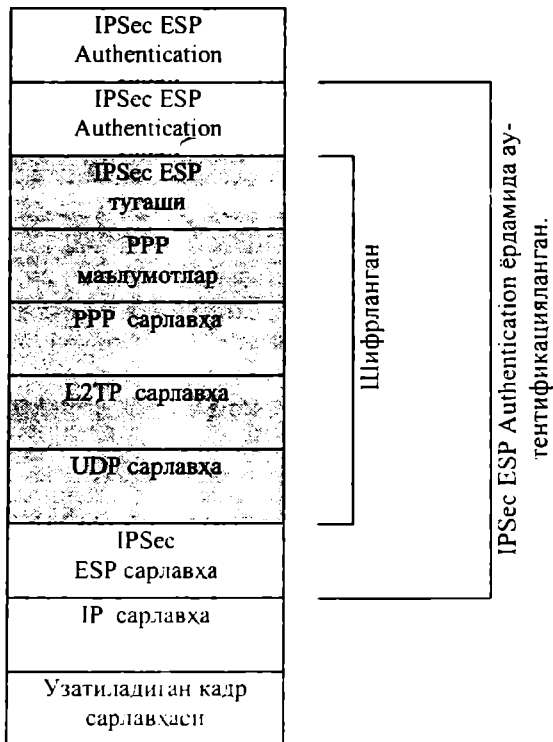
7.14 -расм. L2TP протоколининг архитектураси.

АН ва ESP протоколлари фойдаланувчиларнинг, келишилган ҳолда, шифрлаш ва аутентификациялашнинг турли криптографик алгоритмларини ишлатишларига йўл қўяди. Интерпретация домени DOT (Domain of Interpretation) ишлатилувчи протоколлар ва алгоритмларнинг бирга ишлашини таъминлайди.

Моҳияти бўйича, гибрид протокол L2TP масофадаги фойдаланувчиларни аутентификациялаш, химояланган виртуал уланишни яратиш ва маълумотлар оқимларини бошқариш функциялари билан кенгайтирилган PPP протоколидир.

L2TP протоколи транспорт сифатида UDP протоколини ишлатади ва туннельни бошқаришда ва маълумотларни ташишда хабарларнинг бир хил форматидан фойдаланади.

PPTP протоколидагидек, L2TP протоколи туннельга узатиш учун пакетни йиғишда аввал PPP ахборот маълумотлари майдонида PPP сарлавҳасини, сўнгра L2TP сарлавҳасини қўшади. Шу тариқа олинган пакет UDP протокол томонидан инкапсуляцияланади. L2TP протокол жўнатувчи ва қабул қилувчи порти сифатида UDP-портдан фойдаланади. 7.15-расмда L2TP туннели бўйича жўнатиловчи пакет тузилмаси келтирилган.



7.15-расм. L2TP туннели бўйлаб жўнатиладиган пакет тузилмаси

IPSec протоколлар стеки хавфсизлиги сиёсатининг танланган хилига боғлиқ ҳолда L2TP протоколи UDP-хабарни шифрлаши ва унга ESP (Encapsulation Security Payload)нинг сарлавҳасини ва охирини ҳамда IPSec ESP Authenticationнинг охирини қўшиши мумкин. Сўнгра IPга инкапсуляциялаш бажарилади. Таркибида жўнатувчи ва қабул қилувчи манзиллари бўлган IP-сарлавҳа қўшилади. Охирида L2TP маълумотларни узатишга тайёрлаш учун иккинчи PPP-инкапсуляциялашни бажаради.

Компьютер – қабул қилувчи маълумотларни қабул қилади. PPPнинг сарлавҳаси ва охирини ишлайди. IP сарлавҳани олиб ташлайди. IPSec ESP Authentication ёрдамида IP нинг ахборот майдони аутентификацияланади, IPSec ESP протоколи эса пакетнинг расшифровкасида ёрдам беради. Кейин компьютер UDP сарлавҳасини ишлайди ва туннелни идентификациялаш учун L2TP сарлавҳасидан фойдаланади. Энди PPP пакетнинг таркибида фақат фойдали маълумотлар бўлади, улар ишланади ва кўрсатилган қабул қилувчига юборилади.

L2TP протоколи «фойдаланувчи» ва «компьютер» сатҳларда аутентификациялашни таъминлайди ҳамда маълумотларни аутентификациялайди ва шифрлайди. Мижозларни ва VPN серверларини аутентификациялашнинг биринчи босқичида L2TP сертификация хизматидан олинган локал сертификатлардан фойдаланади. Мижоз ва сервер сертификатлар билан алмашишади ва химояланган улашиш ESP SA (Security Association)ни яратишади.

L2TP компьютерни аутентификациялашни тугатганидан сўнг, фойдаланувчи сатҳда аутентификациялашда фойдаланувчи исмини ва паролни очик кўринишда узатувчи ҳар қандай протокол, ҳатто PAP, ишлатилиши мумкин. Бу ҳамомила хавфсиз, чунки L2TP бутун сессияни шифрлайди. Аммо фойдаланувчини аутентификациялашни, компьютер ва фойдаланувчини аутентификациялашда турли калитлардан фойдаланувчи MSCHAP ёрдамида ўтказиш хавфсизликни ошириши мумкин.

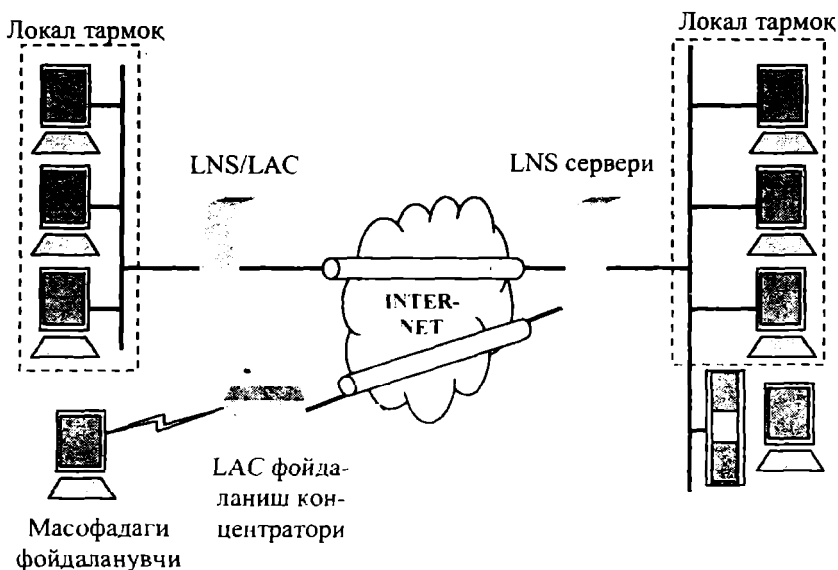
L2TP протоколининг тахмини бўйича провайдернинг масофадан фойдаланиш сервери ва корпоратив тармоқ маршрутизатори орасида туннел ҳосил қилувчи схемалардан фойдаланилади. Бу протокол олдингиларидан (PPTP ва L2F протоколларидан) фаркли ҳолда охириги абонентлар орасида, ҳар бири алоҳида иловага ажратилиши мумкин бўлган, бир неча туннелни бирданига очиш имко-

нятини тақдим этади. Бу хусусият туннеллашнинг мосланувчанлигини ва хавфсизлигини таъминлайди.

L2TP протоколининг спецификациясига биноан провайдернинг масофадан фойдаланиш сервери ролини. L2TP протоколининг мижоз қисмини амалга оширувчи ва масофадаги фойдаланувчига унинг локал тармоғидан Internet орқали тармоқли фойдаланишни таъминловчи, фойдаланишнинг концентратори LAC (L2TP Access Concentrator) бажариши лозим. Локал тармоқнинг масофадан фойдаланиш сервери сифатида PPP протоколи билан бирга ишлай олувчи платформаларда ишловчи гармоқ сервери LNS (L2TP Network Server)дан фойдаланилади (7.16-расм).

PPTP ва L2F протоколларидек L2TP протоколида химояланган виртуал канални шакллантириш уч босқичда амалга оширилади:

- локал тармоқнинг масофадан фойдаланиш сервери билан уланишни ўрнатиш;
- фойдаланувчини аутентификациялаш;
- химояланган туннелни конфигурациялаш.



7.16-расм. L2TP протоколи асосида туннеллаш схемаси.

Биринчи боскичда локал тармокнинг масофадан фойдаланиш сервери билан уланишни ўрнатиш учун масофадаги фойдаланувчи провайдер ISP билан PPP – улашни бошлаб беради. Провайдер сервери ISPда ишловчи фойдаланиш концентратори бу уланишни қабул қилади ва канал PPPни ўрнатади. Сўнгра фойдаланувчи концентратори LAC охириги узел ва унинг фойдаланувчисини қисман аутентификациялайди. Провайдер ISP фақат фойдаланувчининг исмидан фойдаланган ҳолда унга L2TP туннеллаш сервисининг кераклигини ҳал қилади. Агар бундай сервис керак бўлса, фойдаланиш концентратори LAC туннелли уланиш ўрнатилиши лозим бўлган тармок сервери LNS манзилени аниқлашга ўтади. Фойдаланувчи ва фойдаланувчи тармоғига хизмат кўрсатувчи сервер LNS орасидаги мувофиқликни аниқлашнинг қулайлигини таъминлаш мақсадида провайдер ISP томонидан ўзининг миждозлари учун мададланувчи маълумотлар базасидан фойдаланиш мумкин.

LNS серверининг IP-манзили аниқланганидан сўнг L2TPнинг бу сервер билан туннели бор ёки йўқлиги текширилади. Агар бундай туннел бўлмаса, у ўрнатилади. Провайдернинг фойдаланиш концентратори LAC ва локал тармокнинг тармок сервери LNS орасида L2TP протокол бўйича сессия ўрнатилади.

Транспортга ўзаро алоканинг «нуқта-нуқта» пакет режимини мададлаши талаби қўйилади. LAC ва LNS орасида туннел яратишда бу туннел доирасида янги уланишга чақириш идентификатори Call ID деб аталувчи идентификатор берилади. Концентратор LAC тармок серверига ушбу Call ID билан чақирик хусусидаги билдириш бўлган пакет жўнатади. LNS сервери чақирикни қабул қилиши ёки рад этиши мумкин.

Иккинчи боскичда локал тармокнинг тармок сервери LNS фойдаланувчини аутентификациялаш жараёнини бажаради. Бунинг учун аутентификациялашнинг стандарт алгоритмларидан бири, хусусан, CHAP алгоритми ишлатилиши мумкин. Таъкидлаш лозимки, L2TP протоколининг спецификациясида аутентификациялаш усулларининг тавсифи келтирилмаган. Чақирик хусусидаги билдириш таркибидан тармок сервери LNS томонидан фойдаланувчининг аутентификациялаш учун ахборот бўлиши мумкин. Бу ахборотни концентратор LAC фойдаланувчи билан мулоқот жараёнида йиғади. Аутентификациялашнинг CHAP протоколидан фойдаланилганда билдириш пакетида чақириш-сўзи, фойдаланувчи исми ва унинг жавоби бўлади. PAP протоколи учун бу ахборот фойдала-

нувчи исми ва шифрланмаган паролдан иборат бўлади. Тармоқ сервери LNS бу ахборотдан, масофадаги фойдаланувчини ўз маълумотларини қайтадан киритишга мажбур қилмаслик ва аутентификациялашнинг кўшимча циклини бажармаслик максатида, аутентификациялвш учун бирданига фойдаланиши мумкин.

Аутентификация натижаси жўнатилишида тармоқ сервери LNS ҳам фойдаланиш концентратори LACга фойдаланувчи узелининг IP-манзилини узатиши мумкин. Моҳияти бўйича фойдаланиш концентратори LAC масофадаги фойдаланувчи узели ва локал тармоқнинг тармоқ сервери орасида воситачи вазифасини бажаради. Масофадаги узелга корпоратив тармоқнинг манзиллар пулидан манзилнинг ажратилиши фойдаланувчига провайдер манзиллар пулидан оддий манзил олинишидаги ноқулайликлардан қутилишига имкон беради.

Учинчи босқичда провайдернинг фойдаланиш концентратори LAC ва локал тармоқнинг сервери LNS орасида химояланган туннел яратилади. Натижада, инкапсуляцияланган кадрлар PPP туннел орқали концентратор LAC ва тармоқ сервери LNS орасида иккала йўналишда узатилиши мумкин. Масофадаги фойдаланувчидан PPP кадри келганида концентратор LAC ундан кадрни копланган байтларни, назорат йиғинди байтларини чиқариб ташлайди, сўнгра уни L2TP протокол ёрдамида тармоқ протоколига инкапсуляциялайди ва туннел орқали тармоқ сервери LNSга жўнатади. LNS сервер L2TP протоколдан фойдаланиб, келган пакетдан PPP кадрни чиқариб олиб ишлайди.

Туннелнинг зарурий кийматларини созлаш бошқариш хабарлари ёрдамида амалга оширилади. L2TP протоколи ҳар қандай пакетни коммутацияловчи транспорт устидан ишлаши мумкин. Умумий ҳолда, бу транспорт, масалан, UDP протоколи, пакетларни кафолатли стқазиш ни таъминламайди. Шу сабабли L2TP протоколи бу масалаларни ҳар бир масофадаги фойдаланувчи учун туннел ичида уланишларни ўрнатиш муолажаларидан фойдаланиб, мустақил ҳал этади.

Таъкидлаш лозимки, L2TP протоколи криптохимоянинг муайян усулларини белгиламайди ва шифрлашни турли стандартларидан фойдаланиш мумкинлигини фараз қилади. Агар химояланган туннелнинг IP-тармоқда шакллантирилиши режалашгирилган бўлса, криптохимояни амалга оширишда IPSec протоколидан фойдаланилади. L2TP протоколи PPP алгоритмига нисбатан маълумот-

ларни химоялашнинг юкори савиясини таъминлайди, чунки унда 3DES (Triple Data Encryption Standard) шифрлаш алгоритми ишлатилади. Агар химоянинг бундан юкори савияси керак бўлмаса битта 56 хонали калитли DES алгоритмидан фойдаланиш мумкин. Ундан ташқари, L2TP протоколи HMAC (Hash Message Authentication Code) алгоритми ёрдамида маълумотларни аутентификациялашни таъминлайди. Аутентификациялаш учун бу алгоритм узунлиги 128 хонага тенг бўлган «хэш»ни яратади.

Шундай қилиб, PPTP ва L2TP протоколларининг функционал имкониятлари турлича, PPTP протоколи фақат IP-тармоқларда ишлатилиши мумкин ва унга туннелни яратиши ва ишлатилиши учун алоҳида TCP уланиш зарур. L2TP протоколи нафақат IP-тармоқларда ишлатилиши мумкин, туннелни яратиш ва у орқали маълумотларни ташишда хизматчи хабарлар бир хил формат ва протоколлардан фойдаланади. L2TP протоколи ташкилот учун муҳим бўлган маълумотларнинг қарийб 100 %ли хавфсизлигини кафолатлаши мумкин.

L2TP протоколининг камчилиги сифатида қуйидагиларни кўрсатиш мумкин:

– L2TP протоколини амалга оширишда ISP провайдерларнинг мадади зарур;

– L2TP трафикни танланган туннел доирасида чегаралайди ва фойдаланувчиларнинг Internetнинг бошқа қисмларидан фойдаланишига имкон бермайди;

– L2TP протоколида IP протоколининг жорий версияси учун ахборот алмашинувнинг охириги нукталари орасида криптохимояланган туннел яратиш кўзда тутилмаган;

– L2TPнинг таклиф этилган спецификацияси стандарт шифрлашни фақат IP-тармоқларда IPSec протоколи ёрдамида таъминлайди.

Сеанс сатҳида химояланган виртуал каналларни шакллантириш протоколлари.

Химояланган виртуал каналларини шакллантириш мумкин бўлган OSI моделининг энг юкори сатҳи – бешинчи–сеанс сатҳидир. Сеанс сатҳида химояланган виртуал тармоқни қуришда ахборот алмашинувини криптографик химоялаш, жумладан, аутентификациялаш ҳамда ўзаро алоқа томонлари орасида воситачиликнинг қатор функцияларини амалга ошириш имконияти пайдо бўлади. Ҳақиқатан, OSI моделининг сеанс сатҳи мантикий уланиш-

ларни ўрнатишга ва бу уланишларни бошқаришга жавобгар. Шу сабабли, бу сатҳда суралган уланишларнинг жоизлигини текширувчи ва тармоқлараро ҳаракатлар химоясининг бошқа функцияларининг бажарилишини таъминловчи дастур-воситачилардан фойдаланиш имконияти мавжуд.

Сеанс сатҳида химояланган виртуал канални шакллантириш протоколи химоянинг татбикий протоколлари ҳамда турли сервисларни тақдим этувчи юқори сатҳ протоколлари (HTTP, FTP, POP3, SMTP ва ҳ. протоколлар) учун шаффофдир. Аммо, сеанс сатҳида юқори сатҳли протоколларни амалга оширувчи иловаларга бевосита боғлиқлик бошланади. Шунинг учун мазкур сатҳга мос келувчи ахборот алмашиш протоколини амалга ошириш кўп ҳолларда юқори сатҳли иловаларга ўзгартиришлар киритилишини талаб этади.

Сеанс сатҳида ахборот алмашишда SSL протоколи кенг тарқалган. Сеанс сатҳида ўзаро алоқа томонлари орасида воситачилик функцияларини бажариш учун IETF ташкилоти томонидан стандарт сифатида SOCKS протоколи қабул қилинган.

SSL протоколи Netscape Communication компанияси томонидан мижоз-сервер иловаларида ахборотни химояланган алмашишни амалга ошириш учун ишлаб чиқилган. Ҳозирда SSL протоколи OSI моделининг сеанс сатҳида ишловчи химояланган канал протоколи сифатида ишлатилади. Бу протокол ахборот алмашиш хавфсизлигини таъминлашда ахборотни химоялашнинг криптографик усулларида фойдаланади. SSL протоколи тармоқнинг иккита абоненти орасида химояланган канал қуришнинг барча функцияларини жумладан, уларни аутентификациялаш, узатиловчи маълумотларнинг конфиденциаллигини ва яхлитлигини таъминлаш функцияларини бажаради. Асимметрик ва симметрик криптотизимлардан комплекс фойдаланиш технологияси SSL протоколининг ядроси ҳисобланади.

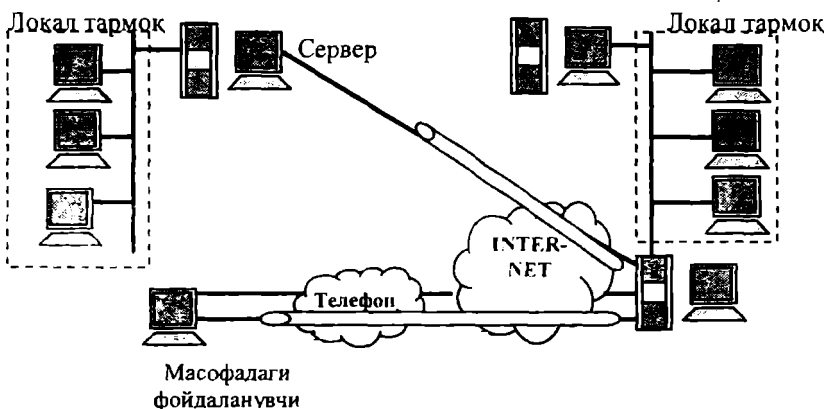
SSLда иккала томоннинг ўзаро аутентификациялаш фойдаланувчиларнинг (мижоз ва сервер) махсус сертификация марказларининг рақамли имзоси билан тасдиқланган очик калитларининг рақамли сертификатлари билан алмашиш орқали бажарилади. SSL протоколи ҳамма қабул қилган X.509 стандартларга мос келувчи сертификатларни ҳамда сертификатларни беришда ва ҳақиқийлигини текширишда ишлатилувчи PKI очик калитлари инфратузилмаларининг стандартини мададлайди.

Конфиденциаллик улашиш ўрнатилишида томонлар алмашинадиган симметрик сессия калитларида узатиувчи хабарларни шифрлаш орқали таъминланади. Сессия калитлари ҳам шифрланган кўринишда узатилади. Бунда улар абонентларнинг сертификатларидан чиқариб олинган очик калитларда шифрланади. Ахборотларни шифрлашда симметрик калитларнинг ишлатилишига асосий сабаб-симметрик калитларда шифрлаш ва расшифровка қилиш жараёнининг тезлиги асимметрик калитлар ишлатилишидагига караганда юқорилиги.

Айланувчи ахборотнинг хакикийлиги ва яхлитлиги электрон рақамли имзони шакллантириш ва текшириш эвазига таъминланади.

Асимметрик шифрлаш алгоритмлари сифатида RSA ҳамда Диффи-Хеллман алгоритмлари ишлатилади. Симметрик шифрлаш алгоритмлари сифатида эса RC2, RC4, DES ҳамда Triple DES алгоритмлари ишлатилади. Хэш функцияларини ҳисоблашда MD5 ва SHA-1 стандартлари ишлатилиши мумкин. SSL протоколининг 3,0 версиясида криптографик алгоритмлари тўплами кенгайтирилувчи ҳисобланади.

SSL протокоliga мувофиқ криптохимояланган туннеллар виртуал тармоқнинг охириги нукталари орасида яратилади. Ҳар бир химояланган туннелни бошлаб берувчилари-туннел охириги нукталаридаги компьютерларда ишловчи мижоз ва сервер (7.17-расм).



7.17-расм. SSL протоколи асосида шаклланган криптохимояланган туннеллар.

Ҳимояланган уланишни шакллантиришда ва мададлашда SSL протоколи мижоз ва сервер ўзаро алоқасининг куйидаги босқичларини кўзда тутади:

- SSL сессиясини ўрнатиш;
- ҳимояланган ўзаро алоқа.

SSL сессияни ўрнатиш жараёнида куйидаги масалалар ечилади:

- томонларни аутентификациялаш;
- ҳимояланган ахборот алмашинувида ишлатилувчи криптографик алгоритмлар ва зичлаштириш алгоритмларини мувофиқлаштириш;

- умумий махфий мастер-калитни шакллантириш;
- ахборот алмашишни криптографик ҳимоялаш учун шакллантирилган мастер-калит асосида умумий махфий сеанс калитларини генерациялаш.

Кўл беришиш муолажаси деб ҳам аталувчи SSL-сессияни ўрнатиш муолажаси ахборот алмашишни бевосита ҳимоялашдан олдин пухта ишланади ва SSL протоколи таркибига кирувчи бошланғич саломлаш (HandShake Protocol) протоколи бўйича ба-жарилади.

Мижоз ва сервер орасида қайта уланиш ўрнатилишида томонлар, ўзаро келишув бўйича, олдинги умумий сир асосида янги сеанс калитларини шакллантиришлари мумкин (ушбу муолажа SSL-сессиянинг давоми деб аталади).

SSL 3.0 протоколи аутентификациялашнинг куйидаги учта режимини мададлайди:

- томонларни ўзаро аутентификациялаш;
- мижозни аутентификацияламасдан серверни бир томонлама аутентификациялаш;
- тўлиқ анонимлик.

Охирги вариантдан фойдаланилганда томонларнинг ҳақиқийлигини кафолатламасдан ахборот алмашиш хавфсизлиги таъминланади. Бу ҳолда ўзаро алоқадаги томонлар, алоқа катнашчиларини алмаштириб қўйиш билан боғлиқ ҳужумлардан ҳимояланмайдилар.

SSL протоколига мувофиқ ўзаро алоқадаги томонларни аутентификациялашда ва умумий махфий калитни шакллантиришда кўпинча RSA алгоритмидан фойдаланилади.

Очик калитлар ва уларнинг эгалари орасидаги мувофиқлик махсус сертификация марказлари томонидан берилувчи ракамли

сертификатлар ёрдамида ўрнатилади. Сертификат таркибида куйидаги ахборот бўлган маълумотлар блокидир:

- сертификация марказининг номи;
- сертификат эгасининг исми;
- сертификат эгасининг очик калити;
- сертификатнинг таъсир муддати;
- сертификатни ишлашда фойдаланиладиган идентификатор ва криптоалгоритмнинг параметрлари;
- сертификат таркибидаги барча маълумотларни тасдиқловчи сертификация марказининг рақамли имзоси.

Сертификат таркибидаги сертификация марказининг рақамли имзоси очик калит ва унинг эгасининг ҳақиқийлигини ва бир маънода мослигини таъминлайди. Сертификация маркази очик калитларнинг ҳақиқийлигини тасдиқловчи нотариус ролини ўтайди. Натижада, бу калит эгаларига химояланган ўзаро алоқа хизматидан, олдиндан шахсий учрашувсиз фойдаланишларига имкон беради.

1999 йили SSL 3,0 версияси ўрнига, SSL протоколига асосланган ва ҳозирда Internet стандарти ҳисобланган TLS протоколи келди. SSL 3.0 ва TLS протоколлари орасидаги фарк жуда ҳам жиддий эмас.

SSL ва TLS протоколларининг камчилиги – ўзларининг хабарларини ташишда тармок сатҳидаги фақат битта – IP-протолидан фойдаланишлари ва, демак, фақат IP-тармоқларда ишлай олишлари. Ундан ташқари, SSL/TLSнинг амалда қўлланиши татбикий протоколлар учун тўла шаффоф эмас.

SSLнинг яна бир салбий томони шундай иборатки, агар мижоз ва сервер уланишни узсалар, улар уни маълумотларнинг минимал ҳажмини алмашиш йўли билан тиклашлари ва Session ID нинг эски параметрларидан фойдаланишлари мумкин. Нияти бузук одам олдинги сессиялардан бирини обрўсизлантириб уни тиклаш муолажасини сервер билан ўтказиши мумкин. Натижада, бу сессияда узатиладиган кейинги барча маълумотлар обрўсизлантирилади.

Ундан ташқари, SSLда аутентификациялашда ва ширфлашда бир хил калитдан фойдаланилади. Бу эса маълум бир ҳолатларда заифликка олиб келиши мумкин. Бундай ечим турли калитлар ишлагилганига нисбатан кўп статистик маълумотларни йиғишга имкон беради.

SOCKS протокли OSI моделининг сеанс сатҳида мижоз-сервер иловаларининг ўзаро алоқа муолажасини сервер-воситачи ёки проху-сервер орқали ташкил этади.

Умумий ҳолда, тармоқлараро экранларда анъанавий ишлатилувчи дастур-воситачилар қуйидаги функцияларни бажариши мумкин:

- фойдаланувчини идентификациялаш ва аутентификациялаш;
- узатилувчи маълумотларни криптохимоялаш;
- ички тармоқ ресурсларидан фойдаланишни чегаралаш;
- ахборотлар оқимини филтрлаш ва ўзгартириш, масалан, вирусларни кидириш ва ахборотни шаффоф шифрлаш;
- чиқадиган ахборот оқимлари учун ички тармоқ манзилларини трансляциялаш.

Аввал *SOCKS* протоколи фақат мижоз иловаларининг серверга сўровларини қайта йўналтириш ҳамда бу иловаларга олинган жавобни қайтариш учун ишлаб чиқилган эди. Ушбу муолажаларнинг ўзи тармоқ IP-манзиллари NATни (Network Address Translation) трансляциялаш функцияларини амалга ошириш имкониятини беради. Чиқувчи пакетлардаги жўнатувчиларнинг IP-манзилларини шлюзининг битта IP-манзили билан алмаштириш ички тармоқ топологиясини ташқи фойдаланувчилардан беркитишга имкон беради ва натижада, рухсатсиз фойдаланиш масаласи мураккаблашади. Тармоқ манзилларини трансляциялаш хавфсизликни ошириш билан бир қаторда хусусий манзиллаш тизимини мададлаш имконияти ҳисобига тармоқ ички манзили маконини кенгайтиришга имкон беради.

SOCKS протоколи асосида тармоқли ўзаро алоқани химоялаш бўйича воситачиликнинг бошқа функциялари ҳам амалга оширилиши мумкин. Масалан, *SOCKS* ахборот оқимлари йўналишни назоратлашда ва фойдаланувчилар ва ахборотлар атрибутларига боғлиқ ҳолда фойдаланишни чегаралашда ишлатилиши мумкин. *SOCKS* протоқолининг воситачилик функцияларини бажаришдаги самарали ишлатилиши унинг OSI моделининг сеанс сатҳига мўлжалланганлиги билан таъминланади. Татбиқий сатҳдаги воситачиларга қараганда, сеанс сатҳида энг юқори тезкорликка, юқори сатҳ протоқолларига (HTTP, FTP, POPS, SMTP ва х.) боғлиқ бўлмасликка эришилади. Ундан ташқари, *SOCKS* протоқоли IP протоқолга боғланмаган ва операцион тизимга боғлиқ эмас. Маса-

лан, мижоз иловалари ва воситачи орасида ахборот алмашишда IPX протоколи ишлатилиши мумкин.

SOCKS протоколи туфайли тармоқлараро экранлар ва виртуал хусусий тармоқлар турли тармоқлар орасида хавфсиз ўзаро алокани ва ахборот алмашинувини ташкил этишлари мумкин. SOCKS протоколи ушбу тизимларни хавфсиз бошқаришни унификацияланган стратегия асосида амалга оширишга имкон беради. Таъкидлаш лозимки, SOCKS протоколи асосида ҳар бир илова ва ҳар бир сеанс учун алоҳида ҳимояланган туннел яратилиши мумкин.

SOCKS протоколи спецификациясига мувофиқ тармоқ шлюзига (тармоқлараро экранга) ўрнатилувчи SOCKS – *сервер* ва ҳар бир фойдаланувчи компьютерга ўрнатилувчи SOCKS – *мижоз* фаркланади. SOCKS-сервер ҳар қандай татбикий сервер билан бу серверга мос келувчи татбикий мижоз номидан ўзаро алокани таъминлайди. SOCKS-мижоз мижоз томонидан татбикий серверга бўлган барча сўровларни ушлаб қолиб уларни SOCKS-серверга узатишга аталган. Таъкидлаш лозимки, мижоз иловаларининг сўровларини ва SOCKS-сервер билан ўзаро алокани ушлаб қолишни бажарувчи SOCKS-мижозлар универсал мижоз дастурларига ўрнатилиши мумкин. SOCKS-серверга сеанс (сокет) сатҳидаги трафик маълум, шунинг учун у синчиклаб назоратлаши, хусусан, фойдаланувчиларнинг муайян иловалари ишини, агар уларнинг ахборот алмашишга зарур ваколатлари бўлмаса, блокировка қилиши мумкин. SOCKS протоколининг 4- ва 5- версиялари кенг тарқалган. Ҳозирда SOCKS протоколининг 5-версияси IETF ташкилоти томонидан Internetнинг стандарти сифатида маъқулланган.

SOCKS протоколининг 4-версиясига биноан уланишни ўрнатишнинг умумий схемаси куйидагича:

– тармоқдаги қандайдир сервер билан боғланишни истаган мижоз SOCKS-сервер (ихтисослаштирилган проху-сервер) билан уланиб унга махсус сўров юборади. Бу сўровда IP-манзил ва у уланиши керак бўлган масофадаги сервер порти бўлади;

– SOCKS-сервер масофадаги сервер-манзилат билан уланади;

– мижоз ва масофадаги сервер уланиш занжири бўйича ўзаро алоқа қилади, SOCKS-сервер маълумотларни ретрансляциялайди;

SOCKS протоколининг 5-версияси тўртинчи версиянинг жиддий ривожини ҳисобланади. У куйидаги кўшимча имкониятларни амалга оширади:

– номларидан SOCKS-мижозлар мурожаат этувчи фойдаланувчиларни аутентификациялаш кўзда тутилган. SOCKS-сервер SOCKS-мижоз билан аутентификациялаш усулини келишиб олишлари мумкин. Аутентификациялаш компьютер ресурсларидан фойдаланишни чегаралашга имкон беради. Икки томонлама аутентификациялаш ҳам жоиз ҳисобланади, яъни фойдаланувчи, ўз навбатида, керакли SOCKS-сервер билан уланганига ишонч ҳосил қилиши мумкин;

– доменли исмларни ишлатиш жоиз ҳисобланади: SOCKS-мижоз SOCKS-серверга нафақат уланишни ўрнатишда керак бўлган компьютернинг IP-манзилини, балки унинг DNS исмини ҳам узатиши мумкин;

– нафақат TCP-протокол, балки UDP протокол ҳам мададланади;

SOCKS протоколининг 5-версиясига биноан уланишни ўрнатишнинг умумий схемаси куйидагича тавсифланиши мумкин:

– тармоқдаги кандайдир татбикий сервер билан уланиш ўрнатишни истаган татбикий мижознинг сўровини мана шу компьютерда ўрнатилган SOCKS-мижоз ушлаб қолади;

– SOCKS-сервер билан уланган SOCKS-мижоз унга ўзи мададловчи аутентификациялашнинг барча усулларининг идентификаторларини билдиради;

– SOCKS-сервер аутентификациялашнинг қайси усулидан фойдаланишни ҳал қилади (агар SOCKS-сервер SOCKS-мижоз томонидан таклиф этилган аутентификациялаш усулларидан бирортасини ҳам мададламаса, уланиш узилади);

– таклиф этилган аутентификациялаш усулидан бирортаси мададланса SOCKS сервер танланган усул бўйича фойдаланувчини (унинг номидан SOCKS-мижоз катнашади) аутентификациялайди муваффақиятсиз аутентификациялашда SOCKS-сервер уланишни узади;

– муваффақиятли идентификациялашдан кейин SOCKS-мижоз SOCKS-серверга тармоқдаги сўралаётган татбикий сервер DNS исмини ёки IP-манзилини узатади, сўнгра SOCKS-сервер фойдала-

нишни чегаралашнинг мавжуд қондалари асосида ушбу татбиқий сервер билан уланишни ўрнатиш бўйича қарор қабул қилади;

– уланиш ўрнатилган ҳолда татбиқий миждоз ва татбиқий сервер бир-бирлари билан уланиш занжири орқали алоқа қиладилар SOCKS-сервер маълумотларни ретрансляциялайди ҳамда тармоқли ўзаро алоқа хавфсизлиги бўйича воситачилик функцияларини бажариши мумкин масалан аутентификациялаш жараёнида SOCKS-миждоз ва SOCKS-сервер сеанс калитларини алмаштиришган бўлсалар, улар орасидаги барча трафик шифрланиши мумкин.

Фойдаланувчиларни SOCKS-сервер томонидан аутентификациялаш X.509 форматидаги рақамли сертификатларга ёки паролларга асосланиши мумкин. SOCKS-миждоз ва SOCKS-сервер орасидаги трафикни шифрлаш учун OSI моделининг сеансли ёки пастрок сатҳларига мўлжалланган протоколлар ишлатилиши мумкин. SOCKS-сервер фойдаланувчиларни аутентификациялаш. IP-манзилларини трансляциялаш ва трафикни криптохимоялашдан бошқа яна қуйидаги функцияларни бажариши мумкин:

– ички тармоқ ресурсларидан фойдаланишни чегаралаш;

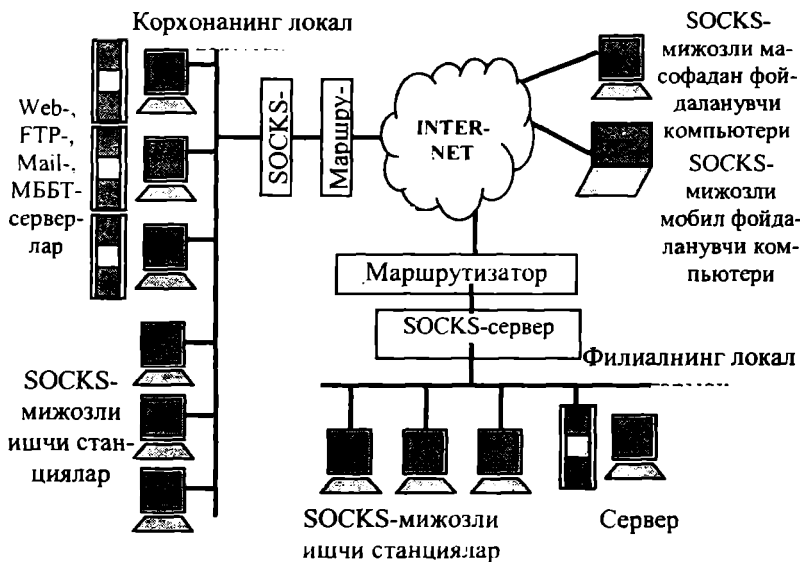
– ташки тармоқ ресурсларидан фойдаланишни чегаралаш;

– хабарлар окимини филътрлаш, масалан, вирусларни динамик кидириш;

– ходисаларни кайдлаш ва уларга реакция кўрсатиш;

– ташки тармоқдан сўралган маълумотларни кэшлаш.

Шундай қилиб, SOCKS протоколи бўйича химояланган виртуал тармоқларни шакллантириш учун ҳар бир локал тармоқ билан Internet уланган нуктадаги компьютер-шлюзда SOCKS-сервер, локал тармоқдаги ишчи станцияларда ва масофадан фойдаланувчиларнинг компьютерларида эса SOCKS-миждоз ўрнатилади. Моҳияти бўйича, SOCKS-серверга SOCKS протоколини мададловчи тармоқлараро экран сифатида қараш мумкин (7.18-расм).



7.18-расм. SOCKS протоколи бўйича ўзаро алоқа схемаси.

Масофадаги фойдаланувчилар Internet га коммутацияланувчи ёки ажратилган линиялар орқали уланишлари мумкин. Ҳимояланган виртуал тармоқ фойдаланувчиси қандайдир татбикий сервер билан уланишга уринганида SOCKS-мижоз SOCKS-сервер билан ўзаро алоқани бошлайди. Ўзаро алоқанинг биринчи босқичи тугаганидан сўнг фойдаланувчи аутентификацияланади, фойдаланиш қоидаси эса унинг кўрсатилган манзилдаги компьютерда ишлайдиган муайян тармоқ иловаларига уланиш ҳуқуқига эга эканлигини кўрсатади. Кейинги ўзаро алоқалар криптографик ҳимояланган канал бўйича юз бериши мумкин.

SOCKS-серверга, локал тармоқларни рухсатсиз фойдаланишдан ҳимоялашдан ташқари, бу локал тармоқ фойдаланувчиларининг Internetнинг очик ресурсларидан (Telnet, WWW, SMTP, POP ва х.) фойдаланишларининг назорати ҳам юкланиши мумкин. Фойдаланиш бутунлай авторизацияланган, чунки фойдаланувчининг компьюттери эмас, балки ўзи идентификацияланади ва аутентификацияланади. Фойдаланиш қоидалар муайян ходимнинг ваколатига кўра Internet нинг маълум ресурслари билан боғланишга рухсат бериши ёки бермаслиги мумкин. Фойдаланиш қоидаларининг

таъсири бошқа параметрлар, масалан, аутентификациялаш усули ёки сутка вақтига боғлиқ бўлиши мумкин. Тармоқли ўзаро алоқа хавф-сизлигининг янада юқори даражасига эришиш учун Internet томонидан фойдаланишга рухсат берилган локал тармоқ серверлари, SOCKS-серверга уланувчи, химояланган очик қисм тармоқни хосил қилувчи алоҳида сегментга ажратилиши лозим.

7.5. IPSec протоколлар стекини химояланган виртуал хусусий тармоқлар қуришда ишлатилиши

IPSec протоколи (Internet Protocol Security) асосан IP тармоқларда маълумотларни хавфсиз узатишни таъминлашга аталган. IPSecнинг ишлатилиши қуйидагиларни кафолатлайди:

- узатилаётган маълумотларнинг яхлитлигини, яъни маълумотлар узатилишида бузилмайди, йўқолмайди ва такрорланмайди;
- жўнатувчининг аутентлигини, яъни маълумотлар ҳақиқий жўнатувчи томонидан узатилган;
- узатиладиган маълумотларнинг конфиденциаллигини, яъни маълумотлар шундай шаклда узатиладик, уларни рухсатсиз кўздан кечиришнинг олди олинади.

Таъкидлаш лозимки, маълумотлар хавфсизлиги тушунчасига одатда, яна бир талаб-маълумотларнинг фойдаланувчанлиги киритилади. Маълумотларнинг фойдаланувчанлиги деганда маълумотлар етказилишининг кафолати тушунилади. IPSec протоколлари бу масалани ҳал этмайди ва уни транспорт сатҳи ISPга қолдиради. IPSec протоколлар стеки тармоқ сатҳида ахборот химоясини таъминлайди. Бу химоянинг ишловчи иловаларга кўринмаслигига олиб келади.

IP-пакет IP тармоқларда коммуникациянинг фундаментал бирлиги ҳисобланади. Унинг тузилмаси 7.19-расмда келтирилган. IP-пакет таркибида манба манзили S ва ахборот қабул қилувчининг манзили D, транспорт сарлавҳаси, бу пакетда ташилувчи маълумотлар хили хусусидаги ахборот ва маълумотларнинг ўзи бўлади.

IP-сарлавҳа		Транспорт TCPси ёки UDP сарлавҳа	Маълумотлар
Адрес-S	Адрес-D		

7.19-расм. IP-пакет тузилмаси.

Аутентификациялашни, узатилувчи маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлаш мақсадида, IPSec протоколларининг стеки қатор стандартлаштирилган криптографик технологиялар асосида қурилган:

- калитларни алмаштириш очик тармоқдан фойдаланувчилар орасида махфий калитларни тақсимлашнинг Диффи-Хеллман алгоритми бўйича амалга оширилади;

- иккала томоннинг ҳақиқийлигини қафолатлаш ва main-in-the-middle ўртадаги одам хилидаги ҳужумларни олдини олиш мақсадида Диффи-Хеллман алгоритми бўйича алмашишларни имзолашда очик калитлар криптографиясидан фойдаланилади;

- очик калитларнинг ҳақиқийлигини тасдиқлашда рақамли сертификатлар ишлатилади;

- маълумотларни шифрлашда блокли симметрик алгоритмлардан фойдаланилади;

- хэшлаш функциялари асосида ахборотларни аутентификациялаш алгоритмлари ишлатилади.

Химояланган канални ўрнатиш ва мададлашдаги асосий масалалар қуйидагилар:

- фойдаланувчилар ёки компьютерларни аутентификациялаш;

- химояланган каналнинг охириги нуқталари орасида узатилувчи маълумотларни шифрлаш ва аутентификациялаш;

- каналнинг охириги нуқталарини маълумотларни аутентификациялашда ва шифрлашда керак бўладиган махфий калитлар билан таъминлаш.

Юқорида санаб ўтилган масалаларни ҳал этишда IPSec тизими ахборот алмашиш хавфсизлиги воситаларининг комплексидан фойдаланади.

IPSec протоколининг аксарият амалга оширилишида қуйидаги компонентлардан фойдаланилади:

- IPSecнинг асосий протоколи. Ушбу компонент химояни инкапсуляцияловчи протокол ESP (Encapsulation Security Payload)ни ва сарлавҳани аутентификацияловчи протоколи AH (Authentication Header)ни амалга оширади. У сарлавҳаларни ишлайди; пакетга қўлланиладиган хавфсизлик сиёсатини аниқлаш учун SPD ва SAD маълумотлар базаси билан ўзаро алоқа қилади;

- калит ахборотларини алмашишни бошқариш протоколи IKE. IKE одатда фойдаланиш сатҳида қўлланилади (операцион тизимга ўрнатилгани бундан истисно);

– хавфсизлик сиёсатларининг маълумотлар базаси SPD (Security Policy Database). Бу энг муҳим компонентлардан бири бўлиб, пакетга қўлланиладиган хавфсизлик сиёсатини белгилайди. SPD дан асосий протокол IPSec томонидан кирувчи ва чиқувчи пакетларни ишлашда фойдаланилади;

– хавфсиз ассоциацияларнинг маълумотлар базаси SPD (Security Association Database). Бу маълумотлар базаси кирувчи ва чиқувчи ахборотни ишлаш учун хавфсиз ассоциациялар SA(Security Association) рўйхатини сақлайди. Чиқувчи SAлардан чиқувчи пакетларни химоялашда, кирувчи SAлардан эса IPSec сарлавҳали пакетларни ишлашда фойдаланилади. SAD маълумотлар базаси SA билан қўлда ёки калитларин бошқариш протоколлари IKE ёрдамида тўлдирилади;

– хавфсизлик сиёсатини ва хавфсиз ассоциацияларни бошқариш. Бу – хавфсизлик сиёсатини ва SAни бошқарувчи иловалар.

Асосий протокол IPSec (ESP ва AHни амалга оширувчи) TCP/IP протоколларининг транспорт ва тармоқ стеклари билан ўзаро узвий алоқада бўлади. IPSecни тармоқ сатхининг қисми дейиш мумкин. IPSecнинг асосий модули иккита интерфейсни – кириш йўли ва чиқиш йўли интерфейсларни таъминлайди. Кириш йўли интерфейси кирувчи пакетлар томонидан, чиқиш йўли интерфейси эса чиқувчи пакетлар томонидан фойдаланилади. IPSecнинг амалга оширилиши TCP/IP протоколлар стекининг транспорт ва тармоқ сатҳлари орасидаги интерфейсга боғлиқ бўлмаслиги лозим.

SPD ва SAD маълумотлар базаси IPSec ишлашига жиддий таъсир кўрсатади. Улардаги маълумотлар тузилмасини танлаш IPSec ишлашининг унумдорлигига таъсир этади.

IPSecдаги барча протоколларни иккита гуруҳга ажратиш мумкин:

– узатиловчи маълумотларни бевосита ишловчи (уларнинг хавфсизлигини таъминлаш учун) протоколлар;

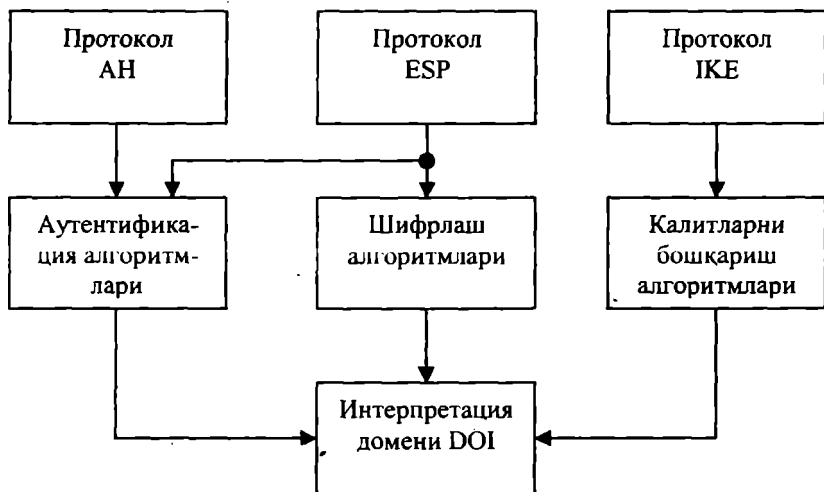
– биринчи гуруҳ протоколларига керакли химояланган ула-нишлар параметрларини автоматик тарзда мувофиқлаштиришга имкон берувчи протоколлар.

IPSec ядросини учта AH, ESP ва виртуал канал ва калитларни бошқариш IKE параметрларини мувофиқлаштирувчи протоколлар ташкил этади.

IPSecнинг хавфсизлик воситаларининг архитектураси 7.20-расмда келтирилган.

Архитектуранинг юқори сатҳида куйидаги протоколлар жойлашган:

– виртуал канал параметрларини мувофиқлаштирувчи ва калитларни бошқариш протоколи IKE. Бу протокол химояланган канални инициализациялаш усулини, жумладан, ишлатилувчи криптохимоялаш алгоритмларини мувофиқлаштиришни ҳамда химояланган уланиш доирасида махфий калитларни алмашиш ва бошқариш муолажаларини белгилайди;



7.20-расм. IPSec протоколлари стекининг архитектураси.

– сарлавхани аутентификацияловчи протокол АН. Бу протокол маълумотлар манбаини аутентификациялашни, уларнинг, қабул қилинганидан сўнг, яхлитлигини ва ҳақиқийлигини текшириш ва такрорий ахборотларнинг тикиштирилишидан химояни таъминлайди;

– химояни инкапсуляцияловчи протокол ESP. Бу протокол узатишувчи маълумотларни криптографик беркитишни, аутентификациялашни ва яхлитлигини таъминлайди ҳамда такрорий ахборотларнинг тикиштирилишидан химоялайди.

АН ва ESP протоколлари ҳар бири алоҳида ва биргаликда ишлатилиши мумкин. Бу протоколлар вазифаларининг қисқача баёнидан кўриниб турибдики, уларнинг имкониятлари қисман бир хил.

АН протоколи фақат маълумотларни яхлитлигини ва аутентификациялашни таъминлашга жавоб беради. ESP протоколи кувватлироқ ҳисобланади, чунки у маълумотларни шифрлаши мумкин, ундан ташқари, АН протоколи вазифасини ҳам бажариши мумкин.

IKE, АН ва ESP протоколларининг ўзаро алоқалари қуйидагича кечади. Аввал IKE протоколи бўйича иккита нуқта орасида мантикий уланиш ўрнатилади. Бу уланиш IPSec стандартларида «хавфсиз ассоциация» -Security Association, SA номини олган. Ушбу мантикий канал ўрнатилишида каналнинг охириги нукталарини аутентификациялаш бажарилади ҳамда маълумотларни ҳимоялаш параметрлари, масалан, шифрлаш алгоритми, сессия махфий калити ва ҳ. танланади. Сўнгра хавфсиз ассоциация SA томонидан ўрнатилган доирада АН ва ESP протоколи ишлай бошлайди. Бу протоколлар ёрдамида узатилувчи маълумотларнинг исалган ҳимояси, танланган параметрлардан фойдаланилган ҳолда бажарилади.

IPSec архитектурасининг *ўрта сатҳини* IKE протоколида қўлланилувчи параметрларни мувофиқлаштириш ва калитларни бошқариш алгоритмлари ҳамда АН ва ESP протоколларида ишлатилувчи аутентификациялаш ва шифрлаш алгоритмлари ташкил этади.

Таъкидлаш лозимки, IPSec архитектурасининг юқори сатҳидаги виртуал канални ҳимоялаш протоколлари (АН ва ESP) муайян криптографик алгоритмларга боғлиқ эмас. Аутентификациялаш ва шифрлашнинг кўп сонли турли-туман алгоритмларидан фойдаланиш имконияти туфайли IPSec тармокни ҳимоялашни ташкил этишнинг юқори даражадаги мосланувчанлигини таъминлайди. IPSecнинг мосланувчанлиги деганда ҳар бир масала учун унинг счилишининг турли усуллари тавсия этилиши тушунилади. Бир масала учун танланган усул, одатда, бошқа масалаларни амалга ошириш усулларига боғлиқ эмас. Масалан, шифрлаш учун DES алгоритмининг танланиши маълумотларни аутентификациялашда ишлатилувчи дайджестни ҳисоблаш функциясини танлашга таъсир қилмайди.

IPSec архитектурасининг *пастки сатҳи* интерпретациялаш домени DOI (Domain of Interpretation)дан иборат. Интерпретациялаш доменининг қўлланиш заруриятига куйидагилар сабаб бўлди. АН ва ESP протоколлари модулли тузилмага эга, яъни фойдаланувчилар ўзаро келишилган ҳолда шифрлаш ва аутентификациялашнинг турли криптографик алгоритмларидан фойдаланишлари мумкин. Шу сабабли, барча ишлатилувчи ва янги киритилувчи протокол ва алгоритмларнинг биргаликда ишлашини таъминловчи модул зарур. Айнан шу вазифалар интерпретациялаш доменига юклатилган.

Интерпретациялаш домени маълумотлар базаси сифатида IPSecда ишлатиладиган протоколлар ва алгоритмлар, уларнинг параметрлари, протокол идентификаторлари ва ҳ. хусусидаги ахборотларни саклайди. Мохияти бўйича интерпретациялаш домени IPSec архитектурасида фундамент ролини бажаради. АН ва ESP протоколларида аутентификациялаш ва шифрлаш алгоритмлари сифатида миллий стандартларга мос келувчи алгоритмлардан фойдаланиш учун бу алгоритмларни интерпретациялаш доменида рўйхатдан ўтказиш лозим.

АН ёки ESP протоколлари узатиловчи маълумотларни куйидаги иккита режимда химоялаши мумкин:

– туннел режимда; IP пакетлар бутунлай, уларнинг сарлавҳаси билан бирга химояланади.

– транспорт режимда; IP пакетларнинг фақат ичидагилари химояланади.

Туннел режими асосий режим ҳисобланади. Бу режимда дастлабки пакет янги IP пакетга жойланади ва маълумотлар тармоқ бўйича узатиш янги IP-пакет сарлавҳаси асосида амалга оширилади. Туннел режимда ишлашда ҳар бир оддий IP-пакет криптохимояланган кўринишда бутунлайча IPSec конвертига жойланади. IPSec конверти, ўз навбатида бошқа химояланган IP-пакетга инкапсуляцияланади. Туннел режими одатда махсус ажратилган хавфсизлик шлюзларида – маршрутизаторлар ёки тармоқлараро экранларда амалга оширилади. Бундай шлюзлар орасида химояланган туннеллар шакллантирилади.

Туннелнинг бошқа томонида қабул қилинган химояланган IP-пакетлар «очилади» ва олинган дастлабки IP-пакетлар қабул

килувчи локал тармок компьютерларига стандарт қоидалар бўйича узатилади. IP-пакетларни туннеллаш туннелларни эгаси бўлмиш локал тармоқдаги оддий компьютерлар учун шаффоф ҳисобланади. Охирги тизимларда туннел режими масофадаги ва мобил фойдаланувчиларни мададлаш учун ишлатилиши мумкин. Бу ҳолда фойдаланувчилар компютерида IPSecнинг туннел режимини амалга оширувчи дастурий таъминот ўрнатилиши лозим.

Транспорт режимида тармок орқали IP-пакетни узатиш бу пакетнинг дастлабки сарлавҳаси ёрдамида амалга оширилади. IPSec конвертига криптоҳимояланган кўринишда фақат IP-пакет ичидаги жойланади ва олинган конвертга дастлабки IP-сарлавҳа кўшилади. Транспорт режими туннел режимига нисбатан тезкор ва охирги тизимларда қўлланиш учун ишлаб чиқилган. Ушбу режим масофадаги ва мобил фойдаланувчиларни ҳамда локал тармок ичидаги ахборот окимини ҳимоялашни мададлашда ишлатилиши мумкин. Таъкидлаш лозимки, транспорт режимида ишлаш ҳимояланган ўзаро алоқа гуруҳига кирувчи барча тизимларда ўз аксини топади ва аксарият ҳолларда тармок иловаларини қайта дастурлаш талаб этилади.

Туннел ёки транспорт режимидан фойдаланиш маълумотларни ҳимоялашга қўйиладиган талабларга ҳамда IPSec ишловчи узел ролига боғлиқ. Ҳимояланувчи канални тугалловчи узел-хост (охирги узел) ёки шлюз (оралиқдаги узел) бўлиши мумкин. Мос ҳолда, IPSecни қўллашнинг куйидаги учта асосий схемаси фаркланади:

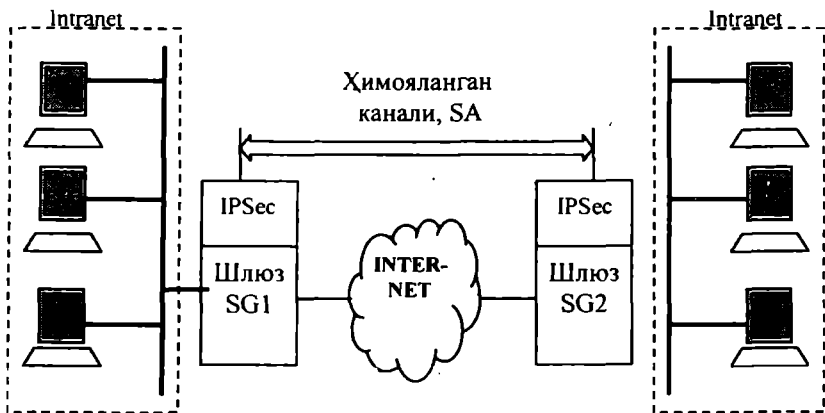
- «хост – хост»;
- «шлюз – шлюз»;
- «хост – шлюз»;

Биринчи схемада ҳимояланган канал тармокнинг охирги иккита узели, яъни Н1 ва Н2 хостлар орасида ўрнатилади (7.21-расм), IPSecни мададловчи хостлар учун транспорт, ҳам туннел режимларидан фойдаланишга руҳсат берилади.



7.21-расм. «Хост-хост» схемаси.

Иккинчи схемага биноан, химояланган канал ҳар бирида IPsec протоколи ишловчи, *хавфсизлик шлюзлари SG1 ва SG2* (Security Gateway) деб аталувчи ораликдаги иккита узеллар орасида ўрнатилади (7.22-расм).

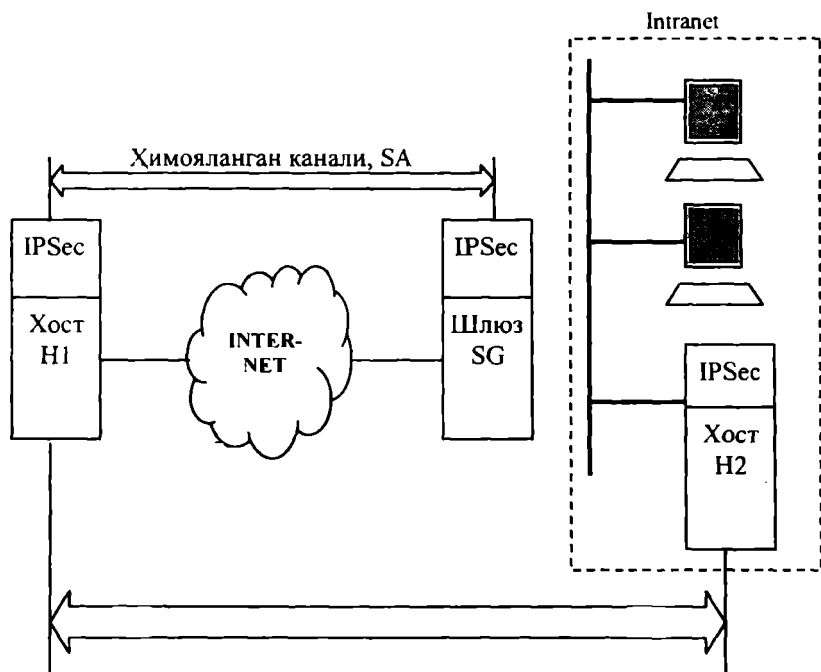


7.22-расм. «Шлюз-шлюз» схемаси.

Хавфсизлик шлюзи иккита тармоққа уланувчи тармоқ қурилмаси бўлиб, ўздан кейин жойлашган хостлар учун шифрлаш ва аутентификациялаш функцияларини бажаради. VPNнинг хавфсизлик шлюзи алоҳида дастурий маҳсулот, алоҳида аппарат қурилма ҳамда VPN функциялари билан тўлдирилган маршрутизатор ёки тармоқлараро экран кўринишида амалга оширилиши мумкин.

Маълумотларни химояланган алмашиш тармоқларга уланган, хавфсизлик шлюзларидан кейин жойлашган ҳар қандай иккита охириги узеллар орасида рўй бериши мумкин. Охириги узеллардан IPSec протоколни мададлаш талаб қилинмайди, улар ўзларининг трафигини химояланмаган ҳолда корхонанинг ишончли тармоғи Intranet оркали узатади. Умумфойдаланувчи тармоққа юборилувчи трафик хавфсизлик шлюзи оркали ўтади ва бу шлюз ўзининг номи-дан IPSec ёрдамида трафикни химоялашни таъминлайди. Шлюз-ларга фақат туннел режимида ишлашга рухсат берилади, ваҳоланки улар транспорт режимини ҳам мададлашлари мумкин (бу ҳолда самара кам бўлади).

«Хост – шлюз» схемаси кўпинча химояланган масофадан фой-даланишда ишлатилади (7.23-расм).



7.23-расм. «Хост-хост» канали билан тўлдирилган «хост-шлюз» схемаси.

Бу ерда химояланган канал IPSec ишловчи масофадаги H1 хост ва корхона Intranet тармоғига кирувчи барча хостлар учун трафикни химояловчи SG шлюз орасида ташкил этилади. Масофадаги хост шлюзга пакетларни жўнатишда ҳам транспорт ва ҳам туннел режимларидан фойдаланиши мумкин, шлюз эса хостга пакетларни факат туннел режимида жўнатади.

Бу схемани масофадаги H1 хост ва шлюз томонидан химояланувчи ички тармоққа тегишли бирор H2 хост орасида параллел яна бир химояланган канални яратиб модификациялаш мумкин. Иккита SAдан бундай комбинациялаб фойдаланиш ички тармоқдаги трафикни ҳам ишончли химоялашга имкон беради.

Кўрилган IPSec асосида химояланган канални қуриш схемалари турли-туман виртуал химояланган тармоқларни (VPN) яратишда кенг қўлланилади. IPSec асосида турли архитектурага эга бўлган виртуал химояланган тармоқлар, жумладан, масофадан фойдаланувчи VPN(Remote Access VPN), корпорация ичидаги VPN(Intranet VPN) ва корпорациялараро VPN(Extranet VPN) қурилади.

IPSec асосидаги VPN-технологияларининг жозибалилигини куйидаги сабаблар оркали изохлаш мумкин:

- тармоқ сатхининг химояси тармоқда ишловчи барча татбиқий тизимлар учун шаффоф, яъни барча иловалар химояланган тармоқда ҳеч қандай тузатишсиз ва ўзгаришсиз худди очик тармоқда ишлаганидек ишлайверади;

- химоялаш тизимининг масштабланувчанлиги таъминланади, яъни мураккаблиги ва унумдорлиги турли бўлган объектларни химоялаш учун мураккаблиги, унумдорлиги, нархи даражаси бўйича адекват бўлган химоялашнинг дастурий ёки дастурий-аппарат воситаларидан фойдаланиш мумкин;

- масштабланувчи қатордаги ахборотни химоялаш маҳсулотлари бирга ишлай оладилар, шу сабабли уларни турли сатҳдаги объектларда (масофадаги ягона терминаллардан то ихтиёрий масштабли локал тармоқларгача) ресурсларидан ва трафигидан барча бегоналар фойдалана ололмайдиган ягона корпоратив тармоққа бирлаштириш мумкин.

8.1. РКІнинг ишлаш принципи

Тарихан ахборот хавфсизлигини бошқарувчи ҳар қандай марказнинг вазифалари доирасига ахборот хавфсизлигининг турли воқиталари томонидан ишлатилувчи калитларни бошқариш кирган. Бу-калитларни бериш, янгилаш, бекор қилиш ва тарқатиш.

Симметрик криптографиядан фойдаланилганда калитларни тарқатиш масаласи энг мураккаб муаммога айланган, чунки:

- N фойдаланувчи учун ҳимояланган $N(N-1)/2$ калитни тарқатиш лозим эди. N бир неча юзга тенг бўлганида бу сермашаккат вазифага айланиши мумкин;

- бундай тизимнинг мураккаблиги (калитларнинг кўплиги ва тарқатиш каналининг махфийлиги) хавфсизлик тизимини қуриш қоидаларининг бири – тизим оддийлигига тўғри келмайди, натижада, заиф жойларнинг пайдо бўлишига олиб келади.

Асимметрик криптография фақат N махфий калитни тавсия этиб, бу муаммони четлаб ўтишга имкон яратади. Бунда ҳар бир фойдаланувчида фақат битта махфий калит ва махсус алгоритм бўйича махфий калитдан олинган очик калит бўлади.

Очик калитдан махфий калитни олиб бўлмаслиги сабабли очик калитни ҳимояланмаган ҳолда барча ўзаро алоқа қатнашчиларига тарқатиш мумкин. Ўзининг махфий калити ва ўзаро алоқадаги шеригининг очик калити ёрдамида ҳар қандай фойдаланувчи ҳар қандай криптоамалларни бажариши мумкин: бўлинувчи сирни ҳисоблаш, ахборотнинг конфиденциаллиги ва яхлитлигини ҳимоялаш, электрон рақамли имзони яратиш.

Шундай қилиб, симметрик криптографиянинг иккита асосий муаммоси ҳал этилади:

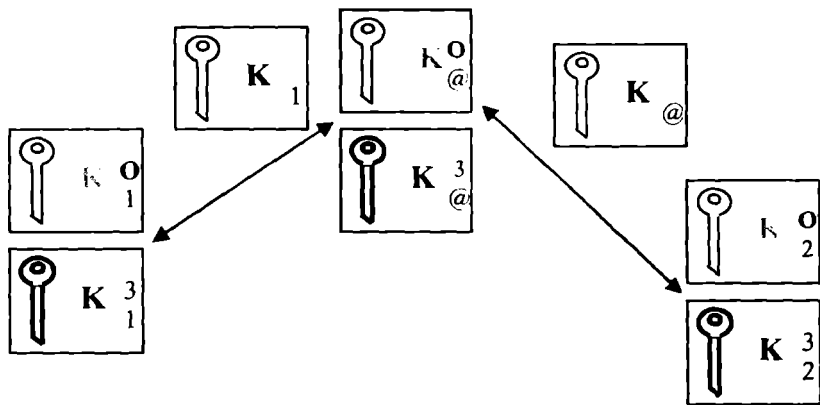
- калитлар сонининг кўплиги – улар энди атиги N та;
- таркатишнинг мураккаблиги – уларни очик таркатиш мумкин.

Аммо бу технологиянинг битта камчилиги – хужум килувчи нияти бузук одам ўзаро алоқа катнашчилари ўртасида жойлашганида *man-in-the-middle* (ўртадаги одам) хужумига мойиллиги.

Очик калитларни бошқариш инфратузилмаси РКІ ушбу камчиликни бартараф қилишга имкон беради ва *man-in-the-middle* хужумидан самарали химояланишни таъминлайди. Очик калитлар инфратузилмаси корпоратив ахборот тизимларининг ишончли ишлаши учун аталган ва ички ва ташқи фойдаланувчиларга ишончли муносабатлар занжири ёрдамида хавфсиз ахборот алмашишга имкон беради. Очик калитлар инфратузилмаси фойдаланувчининг шахсий махфий калитини унинг очик калити билан боғловчи электрон паспортга ўхшаб ишловчи ракамли сертификатларга асосланади.

Man-in-the-middle хужумидан химоялаш. *Man-in-the-middle* хужуми амалга оширилганида нияти бузук одам очик канал орқали узатиловчи ўзаро алоқанинг қонуний иштирокчилари калитларини секингина ўзининг очик калитига алмаштириб, қонуний иштирокчиларнинг ҳар бири билан бўлинувчи сир яратиши ва сўнгра уларнинг барча ахборотларини ушлаб қолиши ва расшифровка қилиши мумкин.

Хужум килувчининг ҳаракатини ва бу хужумдан химояланиш усулини мисол орқали (8.1-расм) кўриб чиқайлик. Фараз қилайлик, фойдаланувчилар 1 ва 2 ўзларига умумий бўлган бўлинувчи сирни Диффи-Хеллман схемаси бўйича ҳисоблаб, химояланган уланишни ўрнатишга қарор қилдилар. Аммо 1- ва 2- фойдаланувчиларнинг K_1 ва K_2 калитлари очик канал орқали узатилаётган онда нияти бузук, одам @ бу каналларни манзилатга етказмай ушлаб қолди. Нияти бузук одам ўзининг махфий ва очик калитини яратиб, очик К калитини 1 ва 2-фойдаланувчиларга секингина уларнинг хақиқий очик K_1 ва K_2 калитларининг ўрнига жўнатади. Натижада, 1 ва 2 – фойдаланувчилар бўлинувчи сирни ўзаро эмас, балки 1-@ ва 2-@ схемалари бўйича яратадилар, чунки улар ўзларининг махфий калитларидан ва нияти бузук одам @нинг очик калити K_w дан фойдаланадилар.



8.1-расм. «Man-in-the-middle» хужумини амалга ошириш.

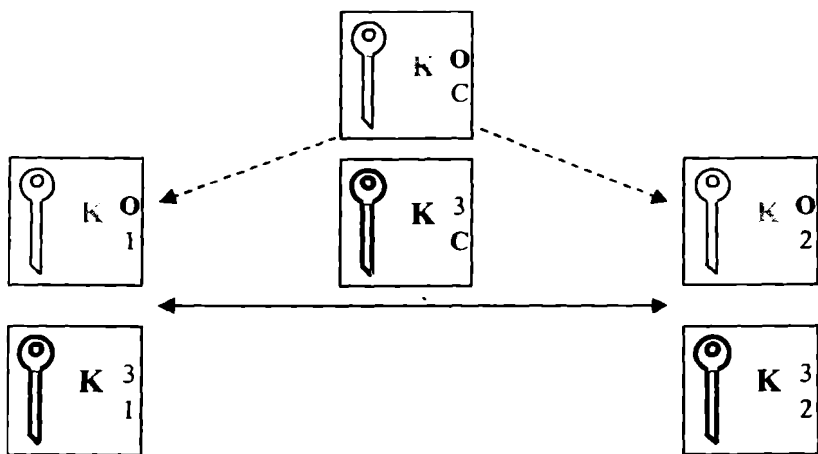
1-фойдаланувчи 2-фойдаланувчига шифрланган ахборотни жўнатган вақтида нияти бузук одам @ уни ушлаб қолиши ва расшифровка қилиши мумкин (унда 1-фойдаланувчи билан бўлинувчи сир $K_{1@}$ бор). Сўнгра нияти бузук одам @ ахборотни (ўзгартирилгани бўлиши мумкин) ўзи ва 2-чи фойдаланувчи хисоблаган бўлинувчи сир $K_{@2}$ дан фойдаланиб янгидан шифрлайди. Натигада, 2-фойдаланувчи 1-фойдаланувчи билан химояланган каналга эгаман деб ўйлаб, нияти бузук одам жўнатган ахборотни олади, расшифровка қилади ва ишлатади.

Бу хужумга қарши самарали восита – нотариус ёки сертификациялаш идораси СА (Certificate Authority). Очик калитларнинг нотариал тасдиқланган сертификатларини қўллаш man-in-the-middle хужумини олдини олишга имкон беради.

1-фойдаланувчи нотариусга боради, нотариус 1-фойдаланувчининг очик калитини ўзининг махфий калитидан фойдаланиб, электрон рақамли имзоси билан имзолайди. Бунда нотариус рақамли имзоси билан нафакат 1-фойдаланувчининг очик калитини, балки фойдаланувчи хусусидаги қатор аниқ ахборотни (Ф.И.Ш., иш жойи ва х.) ҳамда имзонинг таъсир муддатини имзолайди. Ҳосил бўлган хужжат (файл) 1-фойдаланувчи *очик калитининг сертификати* деб аталади. Нотариусдан ўзининг очик калити учун сертификат олишнинг худди шу муолажасини 2-фойдаланувчи ҳам бажаради.

1 ва 2-фойдаланувчи имзо чекилган очик калитларини алмашишганидан сўнг, улар нотариуснинг электрон ракамли имзосини ва сертификат ҳақиқатан 1 ёки 2- фойдаланувчига берилганлигини текширади. Нотариуснинг электрон ракамли имзосини текшириш фойдаланувчилар нотариусга ташриф буюрганларида эҳтиётдан олиб қуйилган нотариусни очик калити ёрдамида шеригидан олган сертификатни расшифровка қилиш орқали бажарилади. Натижада, нотариус СА орқали фойдаланувчилар орасида оддий ишонч занжири пайдо бўлади (8.2-рasm).

Нияти бузук одам @ нотариусга бориб 1-фойдаланувчининг сертификатини ололмайди, чунки унга бу сертификатни олиш вақтида паспортини кўрсатишига ва у 1- фойдаланувчи эканлигини исботлашига тўғри келади.



8.2-рasm. Нотариус СА орқали фойдаланувчилар орасидаги оддий ишонч занжири.

Очик калит сертификатлари. Очик калит сертификатларини шакллантириш Х.509 стандарт тарафидан тавсия этилган қатъий аутентификациялаш принципига ва очик калитли крiптотизим хусусиятларига асосланади.

Очик калит сертификати деганда маълумотлар бўлими ва имзо бўлимидан ташкил топган маълумотлар тузилмаси тушуни-лади. Маълумотлар бўлимида очик калит хусусидаги ва калит эгасини идентификацияловчи маълумотлар бўлади. Имзо бўлимида очик

калитли маълумотлар бўлими учун генерацияланган очик калит эгасини аутентификацияловчи электрон рақамли имзо бўлади. Сертификация маркази СА сертификатлардаги очик калитларни аутентификациялашни таъминловчи ишончли учинчи томон хисобланади.

Сертификациялаш маркази ўзининг жуфт (очик-махфий) калитига эга бўлиб, махфий калит сертификатларни имзолаш учун ишлатилса, очик калит чоп этилади ва ундан фойдаланувчилар сертификатдаги очик калитнинг ҳақиқийлигини текширишда фойдаланадилар. Таъкидлаш лозимки, сертификация марказининг очик калитини хавфсиз узатиш нафақат сертификация марказига шахсан мурожаат асосида, балки бу очик калитни керакли ваколатга эга бўлган бошқа сертификация маркази томонидан сертификациялаш асосида ҳам амалга ошириш мумкин. Сертификация маркази фойдаланувчининг очик калити сертификатини маълумотларнинг маълум тўпламини рақамли имзо билан тасдиқлаш орқали шакллантиради.

Одатда, маълумотларнинг бу тўпламига куйидагилар кирди:

- очик калитнинг таъсир даври: даврнинг бошланиши ва нихояси саналарини ўз ичига олади;

- калитнинг рақами ва серияси;

- фойдаланувчининг ноёб исми;

- фойдаланувчининг очик калити хусусидаги ахборот: ушбу калит аталган алгоритмнинг идентификатори ва очик калитнинг ўзи;

- электрон рақамли имзони текшириш муолажасида ишлатилувчи алгоритм (масалан, электрон рақамли имзони генерацияловчи алгоритм идентификатори);

- сертификация марказининг ноёб исми;

Очик калит сертификати куйидаги хусусиятларга эга:

- сертификация марказининг очик калитидан фойдаланувчининг ҳар бири сертификатга киритилган очик калитни чиқариб олиши мумкин;

- сертификация марказидан ташқари ҳеч бир томон сертификатни билинтирмасдан ўзгартира олмайди (сертификатларни сохталаштириш мумкин эмас).

Сертификатларни сохталаштириш мумкин эмаслиги, уларни умумфойдаланувчи маълумотномаларда, химояламасдан чоп этишга имкон туғдиради.

Очик калит сертификатини яратиш жуфт калитни (очик-махфий) яратишдан бошланади. Калитни генерациялаш муолажаси куйидаги иккита усул орқали амалга оширилиши мумкин:

– сертификация маркази калитлар жуфтини яратади. Очик калит сертификатга киритилади, унинг жуфти-махфий калит эса фойдаланувчига узатилади (фойдаланувчини аутентификациялашни ва калит узатилишининг конфиденциаллигини таъминлаган ҳолда).

– фойдаланувчи калитлар жуфтини ўзи яратади. Махфий калит фойдаланувчида сақланади, очик калит эса химояланган канал орқали сертификация марказига юборилади.

Ҳар бир фойдаланувчи сертификация маркази томонидан шакллантирилган битта ёки бир нечта калитларнинг эгаси бўлиши мумкин. Фойдаланувчи бир неча турли сертификация марказларидан олинган сертификатларга ҳам эга бўлиши мумкин.

Амалда бошқа сертификация марказидан сертификат оладиган фойдаланувчиларни аутентификациялаш эҳтиёжи туғилади.

Сертификатларни бошқариш тизимларининг базавий тузилмалари. Сертификатларни бошқариш тизими-ўзаро ахборот алмашишда хавфсизликни таъминлаш мақсадида очик калитли криптографик технологиялардан фойдаланишга зарур бўлган дастурий-аппарат воситалари ҳамда ташкилий-техник тадбирлар комплекси.

Очик калитларни бошқариш инфратузилмаси PKI man-in-the-middle хужумларидан ишончли химоялашни амалга оширишга имкон берувчи нотариуслар тармоғидан иборат. Нотариус орқали фойдаланувчилар орасидаги оддий ишонч занжири (8.2-расм) битта нотариусга, унга ташриф буюрган фойдаланувчиларнинг очик калитларини, имзоланган сертификатларни яратиш йўли билан химоялашга имкон беради.

Бу тизимнинг самарали ишлаши куйидагиларга боғлиқ:

– ўзаро алоқа иштирокчилари сертификация маркази очик сертификатининг ҳақиқий нусхасига эга бўлишлари шарт;

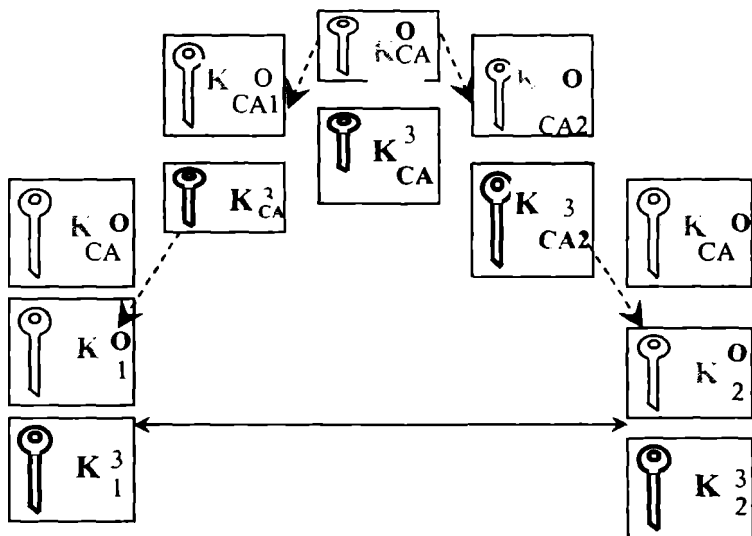
– ўзаро алоқа иштрокчилари ишлатадиган ахборотни химоялаш воситалари ўзаро алоқадаги шеригининг ҳар қандай сертификатини сертификация марказининг очик сертификатидан фойдаланиб автоматик тарзда текшира олиши лозим.

Баъзида ўзаро алоқадаги шериклар сертификация марказидан жуда узокда бўлишлиги мумкин. Бу ҳолда СА, нотариусларининг тақсимланган катламлари яратилади.

Сертификациялашнинг учта базавий модели фарқланади:

- сертификатларнинг иерархик (шажара) занжирига асосланган сертификациялашнинг иерархик модели;
- кросс-сертификациялаш модели (ўзаро сертификациялашни кўзда тутати);
- сертификациялашнинг тармок (гибрид) модели (иерархик ва ўзаро сертификациялаш элементларини ўз ичига олади);

Иерархик моделда СА лар бошка СА ларга сертификатлар берувчи илдиз сертификация марказига иерархик тобеликда жойлашган (8.3-расм).

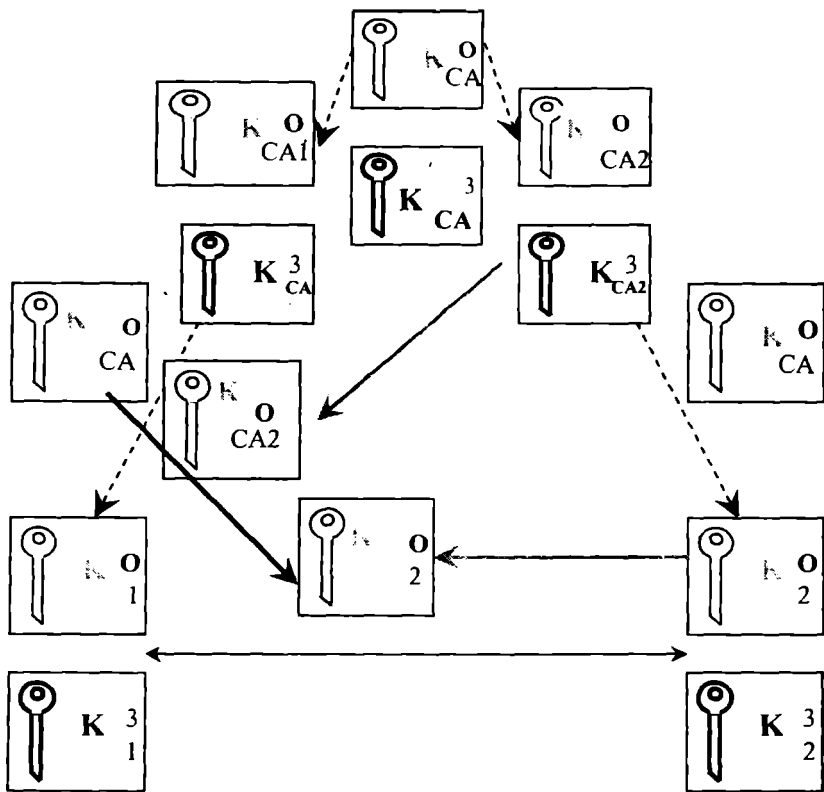


8.3-расм. САнинг икки сатхли иерархияси.

Илдиз сертификация марказининг вазифаси тобе СА1 ва СА2ларни кайдлашдан иборат. Ҳар бир СА хавфсизликнинг ягона даражасини таъминлаш мақсадида сертификациялашнинг берилган сиёсатига мувофик ишлайди. 8.3-расмда келтирилган мисолда СА нотариусларнинг яна бир иерархик сатхи яратилади. Нотариуслар:

- фойдаланувчиларга ўхшаб сертификатларини марказий САда имзолашади;
- марказий САга ўхшаб оддий фойдаланувчиларнинг сертификатларини махфий калитлари билан, имзолайдилар.

Масофадаги шерикнинг ҳақиқийлигини текшириш мантики куйидагича курилади (8.4-расм):



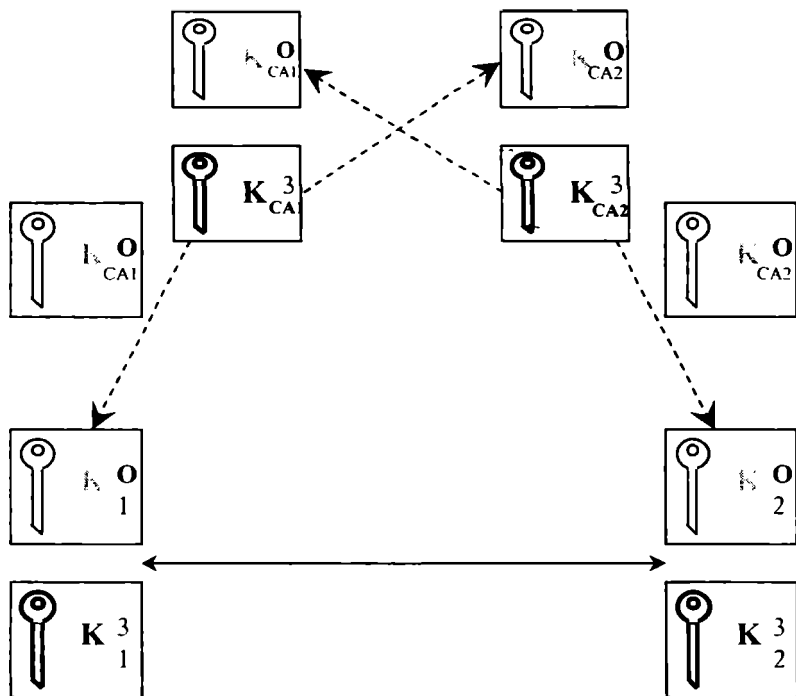
8.4-расм. Масофадаги абонент сертификатини текшириш схемаси.

- фойдаланувчи шеригининг сертификатини олиб, уни нота-ниш СА имзолаганини аниклайди;
- у шеригидан ушбу САнинг сертификатини сўрайди;
- САнинг сертификатини олиб, уни марказий СА сертификати билан текширади;
- муваффақиятли текширишдан сўнг фойдаланувчи бу САга ишона бошлайди ва унинг сертификати билан масофадаги фойдаланувчи сертификатини текширади.

Худди шундай текширишни иккинчи шерик ҳам бажаради. Мухими, ишлатиладиган ахборотни химоялаш тизимлари бундай мураккаб иерархик текширишларни автоматик тарзда бажараол-

синлар. Тавсифланган иерархик схемани, зарурият туғилганда, иерархиянинг янги сатхларини киригиб, давом эттириш мумкин.

Кросс-сертификациялаш моделида иерархиянинг бир шоҳида бўлмаган муस्ताқил САлар сертификация марказлари тармоғида ўзаро сертификацияланадилар. Текшириш схемаси ўзгармайди, чунки фойдаланувчига бегона нотариус унинг нотариусига тобедек туюлади (8.5-расм).



8.5-расм. Кросс-сертификациялаш схемаси.

Таъкидлаш лозимки, кросс-сертификациялаш модели сертификатларни бошқариш тизимининг тармоқли архитектурасининг хусусий холи ҳисобланади.

Сертификатларни бошқариш тизимининг иерархик ва тармоқ архитектураларининг умумлаштирилган схемалари 8.6-расмда келтирилган.

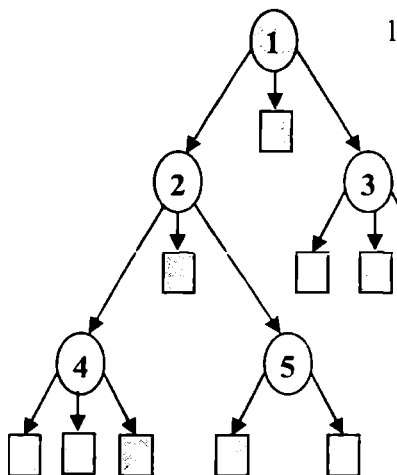
Сертификатларни бошқариш тизимининг *иерархик тузилмаси* куйидаги афзалликларга эга:

– у мавжуд федерал ва идора ташкилий-бошқарув тузилмаларга ўхшаш ва уларнинг принциплари бўйича қурилиши мумкин;

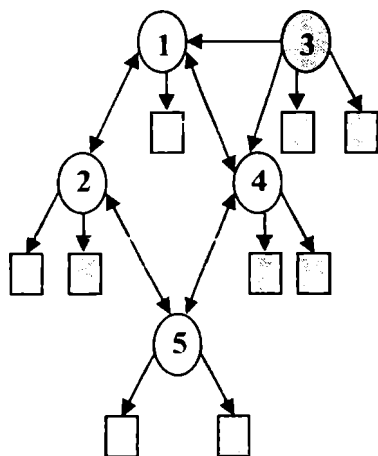
– у исмларнинг иерархик дарахтига осонгина боғланиши мумкин;

– у ўзаро алоқадаги барча томонлар учун сертификатлар занжирини кидириш, қуриш ва верификациялашнинг оддий алгоритмини аниқлайди;

Иерархик тузилма



Тармоқли тузилма



Сертификациялашнинг ишончли маркази



Сертификат чикиши



Сертификациялашнинг тасдиқловчи маркази



Кросс-сертификациялаш



Фойдаланувчи

8.6-расм. Сертификатларни бошқариш тизимининг иерархик ва тармоқли архитектуралари.

– иккита фойдаланувчининг ўзаро алоқани таъминлаши учун улардан бирининг иккинчисига ўзининг сертификатлар занжирини тақдим этиши кифоя, бу ўзаро алоқа билан боғлиқ муаммоларни камайтиради.

Иерархик архитектурага қуйидаги камчиликлар характерли:

- барча охирги фойдаланувчиларнинг ўзаро алоқасини таъминлаш учун факат битта илдизли ишончли СА бўлиши шарт;
- тижорат тузилмаларининг ўзаро алоқаси иерархикдан кўра кўпроқ тўғри характерга эга.

Сертификатларни бошқариш тизимининг *тармоқ архитектураси* қуйидаги афзалликларга эга:

- у анчагина мослашувчан ва замонавий бизнесда мавжуд бўлган бевосита ишончли ўзаро муносабатларнинг ўрнатилишига имкон беради;
- охирги фойдаланувчи ҳеч бўлмаганда унинг сертификатини босиб чиқарган марказга ишониши шарт ва тизимдаги ишонч муносабатлари мана шунга асосланган;
- фойдаланувчилари ўзаро тез-тез алоқа қилувчи турли тасдиқловчи САларни бевосита кросс-сертификациялаш мумкин, бу занжирларни верификациялаш жараёнини қисқартиради;
- тасдиқловчи СА калити обрўсизлантирилганидан сўнг тиклаш жараёни иерархик тузилмага қараганда тармоқ тузилмасида оддийроқ.

Аммо сертификатларни бошқаришнинг тармоқ архитектураси қуйидаги камчиликларга эга:

- барча ўзаро алоқа томонлар учун сертификатлар занжирини кидириш ва қуриш алгоритми жуда мураккаб бўлиши мумкин;
- фойдаланувчи унинг сертификатини бошқа барча фойдаланувчилар томонидан текширилишини таъминловчи занжирни тақдим этаолмайди.

Эхтимол, яқин орада сертификациялаш иерархиясининг энг юқори сатҳида турли ташкилотларнинг ишонч занжирлари алоқасини таъминловчи давлат нотариуси бўлади.

8.2. Очик калитларни бошқариш инфратузилмасининг мантиқий тузилмаси ва компонентлари

Очик калитларни бошқариш инфратузилмаси РКЎнинг асосий вазифалари қуйидагилар:

– рақамли калитлар ва сертификатларнинг ҳаёт циклини мададлаш (яъни калитларни генерациялаш, сертификатларни яратиш ва имзолаш, уларни тақсимлаш ва х.);

– обрўсизлантириш факглари кайдлаш ва чакириб олинган сертификатларнинг «кора» рўйхатини чоп этиш;

– фойдаланувчининг тизимдан фойдаланиш вақтини имкони борича камайтирувчи идентификациялаш ва аутентификациялаш жараёнларини мададлаш:

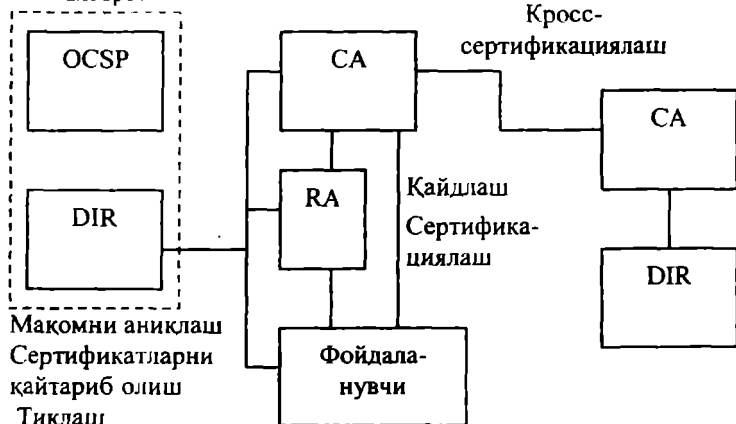
– мавжуд иловалар ва хавфсизлик қисм тизимининг барча компонентларини интеграциялаш механизмини (PKIга асосланган) амалга ошириш;

– барча фойдаланувчилар ва иловалар учун бир хил ва таркибда барча зарурий калит компонентлари ва сертификатлар бўлган хавфсизликнинг ягона токенидан фойдаланиш имкониятини тақдим этиш.

Хавфсизлик токени – фойдаланувчининг тизимдаги барча ҳуқуқлари ва қуршовини аниқловчи хавфсизликнинг шахсий воситаси, масалан смарт-карта.

8.7-расмда очик калитларни бошқариш инфратузилмасининг мантиқий тузилмаси ва асосий компонентлари келтирилган.

Сертификатлар бўйича ахборот



8.7-расм. PKIнинг мантиқий тузилмаси ва асосий компонентлари.

Расмда куйидаги белгилашлар қабул қилинган:

- CA – сертификациялаш маркази;
- RA – қайдлаш маркази;
- OCSP – жорий сертификат мақомининг протоколи (Online Certificate Status Protocol);
- DIR – X.511, X.519, DAP, LDAP фойдаланиш протоколлари бўйича директория хизмати.

Қайдлаш маркази RA – PKI элементи, қайдлашни амалга оширувчи вакил, яъни фойдаланувчига сертификатни химояланган ҳолда бериш имкониятини таъминлаш мақсадида фойдаланувчиларни аутентификациялашни ва уларни қайдлашни амалга оширади. Қайдлаш марказининг хусусияти шундан иборатки, у функционал нуқтаи назаридан сертификация марказига қараганда фойдаланувчига яқинроқ. Ундан ташқари, айнан қайдлаш маркази PKIнинг ўзаро алоқага лаёқатлигини таъминловчи самарали интерфейс хисобланади.

Сертификация маркази CA – PKIнинг элементи (сертификатларнинг ишончли манбаи, нотариус), унга сертификатларни яратиш ва ёки тасдиқлаш ишониб топширилган. Сертификация марказининг ишлаш схемаси куйидагича:

- CA шахсий калитларини генерациялайди ва фойдаланувчилар сертификатларини текширишга аталган CA сертификатларини шакллантиради;
- фойдаланувчилар сертификациялашга сўровларни шакллантирадilar ва уларни у ёки бу усул бўйича CAга етказдилар;
- CA фойдаланувчилар сўровлари асосида уларнинг сертификатларини шакллантиради;
- CA бекор қилинган сертификат рўйхатларини (CRL) шакллантиради ва вақти-вақти билан янгилайди;
- фойдаланувчи сертификатлари, CA сертификатлари ва бекор қилинганлар рўйхати CRL сертификатлар маркази томонидан чоп этилади (фойдаланувчиларга тарқатилади ёки умумфойдаланувчи маълумотномага жойлаштирилади).

PKI бажарадиган функцияларни шартли равишда бир неча гуруҳларга ажратиш мумкин:

- сертификатларни бошқариш функциялари;
- калитларни бошқариш функциялари;
- кўшимча функциялар (хизматлар).

Сертификатларни бошқариш функцияларига қуйидагилар киради:

– *қайдлаш*. Нафакат функцияларнинг бир қисми, балки РКІнинг хавфсизлиги ҳам тўғри қайдлашга ва идентификациялашга асосланган. Фойдаланувчилар сифатида физик фойдаланувчилар, татбикий дастур, тармок қурилмаси ва х. иштирок этиши мумкин. Идентификациялашда ишлатиладиган усулларни сертификациялаш сиёсати белгилайди. Шундай қилиб, фойдаланувчиларни идентификациялаш ва қайдлаш РКІ тизимининг минимал тўлик компонентлари ҳисобланади;

– *очиқ калитларни сертификациялаш*. Сертификациялаш жараёнига сертификациялаш маркази СА жавоб беради. Моҳиятан, сертификациялаш жараёни фойдаланувчи исмини очиқ калит билан боғлашдан иборат.

СА қуйидаги ҳаракатларни бажарган ҳолда фойдаланувчи ва пастрок сатҳдаги СА сертификатларини имзолайди:

- фойдаланувчиларнинг ҳақиқийлигини текшириш;
- сертификатга идентификатор бериш;
- маълумотларни сертификатга киритиш;
- ҳаракат вақтини (бошланиш-ниҳояси) ўрнатиш;
- сертификатни имзолаш;
- сертификатни сертификатларнинг очиқ серверида чоп этиш.

Санинг махфий калитини сақлаш. Бу тизимнинг энг нозик нуқтаси. СА махфий калитининг *обрўсизлантирилиши* унинг ихтиёридаги бутун тизимни бузади. Санинг махфий калити жойлашган компьютер ишончли кўрикланиши лозим;

– *сертификатлар базасини сақлаш ва сертификатларни тақсимлаш*. Тизим ишлашининг қулайлигини таъминлаш мақсадида фойдаланувчиларнинг ва оралик САларнинг (энг юкори сатҳ САсидан бўлак) барча сертификатлари сертификатлар сервери деб аталувчи умумфойдаланувчи серверга олиб қўйилади. Бу ҳолда фойдаланувчилар абонентнинг сертификатини, ҳатто у тармокда вақтинча бўлмаган ҳолда ҳам, олишлари мумкин;

– *сертификатни янгилаш*. Ушбу жараён сертификат таъсири муддати ўтган ҳолда фаоллашади ва фойдаланувчи очиқ калити учун янги сертификатни беришдан иборат бўлади. Агар калитлар жуфти обрўсизлантирилган бўлса ёки янги сертификат сиёсат, кенгайиш ёки хусусият атамаларида олдингисидан фаркланса бу усул ишлатилмайди. Яроклилиқ муддати даврида сертификатнинг исми

ва мансублиги (фойдаланувчининг бошқа бўлимга ўтиши) каби жиддий бўлмаган хусусиятларининг ўзгариши ҳам сертификатни олдинги очик калит билан янгилашни (регенерациялашни) талаб этишга олиб келиши мумкин.

– *калитларни янгилаш.* Фойдаланувчилар ёки учинчи томон калитларнинг янги жуфтини генерациялаганларида янги очик калитга мос келувчи сертификатни яратиш зарур. Бу усулдан сертификатни янгилаш мумкин бўлмаган ҳолларида ҳам фойдаланилади;

– *сертификатни қайтариб олиш мақомини аниқлаш.* Ушбу жараён фойдаланувчига сертификатининг қайтариб олинган эмаслигини текширишга имкон беради. Бу жараён сертификатнинг очик калитлар каталоги PKDда (Public Key Directory) ва сертификатларни қайтариб олиш рўйхати CRLда (Certificate Revocation List) борлигини текшириш орқали ёки бу масалани ечишга ваколати бўлган учинчи томонга сўров ёрдамида ташкил этилиши мумкин.

– *сертификатни қайтариб олиш.* Бу жараён турли ҳолатлар натижасида хавфсизликнинг муайян сиёсатига боғлиқ ҳолда (масалан, калитларнинг обрўсизлантирилиши, исмларнинг ўзгариши, фойдаланишнинг тўхташи ва х.) бўлиши мумкин.

– *калитларни бошқариш функцияси* – калитларни генерациялаш ва тақсимлаш асосий қисм гуруҳларига бўлинади.

Калитларни тақсимлаш функциялари ўз навбатида очик калитларни тақсимлаш ва токенларни персоналлаштиришга бўлинади. Токенларни персоналлаштиришда физик курилмалар – токенлардан фойдаланиб махфий калитларни ва қўшимча маълумотларни сақлаш ташкил этилади; токенларнинг персонализацияси СА, РА ва фойдаланувчи томонидан мададланиши лозим. Масалан, смарт-картанинг персонализацияси ўрнатиш (файл тизимини яратиш) муолажасини, тасодиқий PIN-кодни ёки паролни танлаш, бу смарт-картага тегишли барча маълумотларни етказиш ва сақлашни ўз ичига олиши мумкин.

Қўшимча функциялар (хизматлар) гуруҳи таркибига қуйидагилар киради:

– ўзаро сертификациялаш (турли САларда кросс-сертификациялаш);

– очик калитни унинг унга қуйиладиган арифметик талабларга мос келишини, яъни очик калит ҳақиқий эканлигини текшириш;

– сертификатни текшириш; агар фойдаланувчи бошқа фойдаланувчининг рақамли имзосига ишонини хоҳласа ва мос серти-

фидатни текшираолмаса, текширишни ишончли учинчи томондан илтимос қилиши мумкин;

– архивлаш хизматлари ва ҳ.

Очиқ калитлар инфратузилмаси РКІ қуйидаги қатор иловалар ва стандартларни мададлайди:

– очик калит сертификатларини мададловчи воситалар ўрнатилган Linux, FreeBSD, HP-UX, Microsoft Windows, Novell Netware, Sun Solaris операцион тизимлари;

– очик калит сертификатлари асосида фойдаланувчиларни аутентификациялаш механизмини мададловчи маълумотлар базасини бошқариш тизимлари, хусусан Oracle, DB2, Informix, Sybase;

– IP протоколи асосида амалга оширилувчи виртуал химояланган тармоқларни (VPN) ташкил этиш воситалари, хусусан Cisco Systems, Nortel Network компанияларининг телекоммуникация асбоб-ускуналари ҳамда ихтисослаштирилган дастурий гаъминот.

– электрон ҳужжат айланиши тизимлари, масалан, Lotus Notes, Microsoft Exchange, ҳамда химояланган почта алмашиш стандарти S/MIMEни мададловчи почта тизимлари;

– Microsoft Active Directory, Novell NDS, Netscape iPlanet каталогларининг хизмати;

SSL стандарти асосида амалга оширилувчи Web-ресурслардан фойдаланиш тизимлари.

– фойдаланувчиларни аутентификациялаш тизимлари, хусусан, RSA компаниясининг SecurID ва ҳ.

Ўз навбатида, очик калитлар инфратузилмаси санаб ўтилган функционал соҳаларни интеграциялаши мумкин. Натижада, очик калитлар инфратузилмаларини компания ахборот тизимига интеграциялаш ва умумий стандартлар ва очик калит сертификатларидан фойдаланиш йўли билан ахборот хавфсизлигининг комплекс тизимини яратиш мумкин.

Юқорида келтирилганлар очик калитлар инфратузилмасини яратиш ва мададлаш хизматлари аҳамиятини ошишига олиб келади.

IX боб. АХБОРОТ-КОММУНИКАЦИОН ТИЗИМЛАРДА СУЌИЛИБ КИРИШЛАРНИ АНИҚЛАШ

9.1. Хавфсизликни адаптив бошқариш концепцияси

Ташкилотларда химоялаш билан боғлиқ бўлган муаммоларни ечиш учун аксарият ҳолларда қисман ёндашишлардан фойдаланишади. Бу ёндашишлар, одатда, аввало, фойдалана олувчи ресурсларнинг жорий даражаси орқали аниқланади. Ундан ташқари, хавфсизлик маъмурлари кўпинча ўзларига тушунарли бўлган хавфсизлик хавф-хатарларига реакция кўрсатишади. Аслида хавф-хатарлар жуда кўп бўлиши мумкин. Корпоратив ахборот тизимини фақат қатъий жорий назорати ва хавфсизликнинг умумий сиёсатини таъминловчи комплекс ёндашиш хавфсизлик хавф-хатарларини анчагина камайтириши мумкин.

Охириги вақтда турли компаниялар томонидан қатор ёндашишлар ишлаб чиқилдики, бу ёндашишлар нафақат мавжуд заифликларни аниқлашга, балки ўзгарган эски ёки пайдо бўлган янги заифликларни аниқлашга ва уларга мос химоялаш воситаларини қарши қўйишга имкон беради. Хусусан, ISS(Internet Security Systems) компанияси томонидан *хавфсизликни адаптив бошқариш модели* ANS (Adaptive Network Security) ишлаб чиқилди.

Хавфсизликка адаптив ёндашиш, тўғри лойиҳаланган ва яхши бошқарилувчи жараён ва воситалар ёрдамида хавфсизлик хавф-хатарларини реал вақт режимида назоратлаш, аниқлаш ва уларга реакция кўрсатишга имкон беради.

Тармоқнинг адаптив хавфсизлиги қуйидаги асосий учта элемент орқали таъминланади:

- хавф-хатарларни баҳолаш;
- химояланишни таҳлиллаш;
- ҳужумларни аниқлаш.

Хавф-хатарларни баҳолаш. Заифликларни (қелтирадиган зарарнинг жиддийлик даражаси бўйича), тармоқ қисм тизимларини

(жиддийлик даражаси бўйича), таҳдидларни (уларнинг амалга оширилиши эҳтимоллиги бўйича) аниқлаш ва рутбалашдан иборат. Тармоқ конфигурацияси муттасил ўзгариши сабабли, хавф-хатарларни баҳолаш жараёни ҳам узлуксиз ўтказилиши лозим. Корпоратив ахборот тизимининг ҳимоялаш тизимини куриш хавф-хатарларни баҳолашдан бошланиши лозим.

Ҳимояланишни таҳлиллаш – тармоқнинг заиф жойларини кидириш. Тармоқ уланишлардан, узеллардан, хостлардан, ишчи станциялардан, иловалардан ва маълумот базаларидан таркиб топган. Буларнинг барчаси ҳимояланиш самарадорлигининг сақланишига ҳамда ноъмалум заифликларининг аниқланишига мухтож. Ҳимояланишни таҳлиллаш технологияси тармоқни тадқиқлаш, нозик жойларини топиш, бу маълумотларни умумлаштириш ва улар бўйича ҳисобот бериш имкониятига эга. Агар бу технологияни амалга оширувчи тизим адаптив компонентга ҳам эга бўлса, аниқланган заифликларни автоматик тарзда бартараф этиш мумкин. Ҳимояланишни таҳлиллаш технологияси тармоқ хавфсизлиги сиёсатини, уни ташкилот ташқарисидан ёки ичкарисидан бузишга урнишлардан олдин, амалга оширишга имкон берувчи таъсирчан усул ҳисобланади.

Ҳимояланишни таҳлиллаш технологияси томонидан идентификацияланувчи муаммоларнинг баъзилари куйидагилар:

- тизимлардаги «тешиklar» (back door) ва троян оти хилидаги дастур;

- кучсиз пароллар;

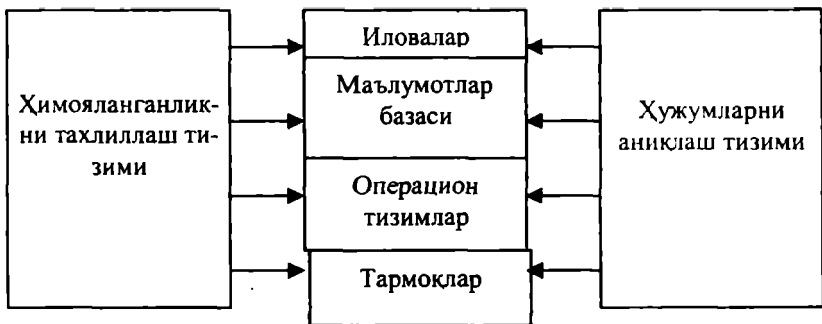
- ҳимояланмаган тизимдан суқилиб киришга ва «хизмат килишдан воз кечиш» хилидаги ҳужумларга таъсирчанлик;

- операцион тизимлардаги зарурий янгиланишларнинг йўқлиги;

- тармоқлараро экранларнинг, Web-серверларнинг ва маълумотлар базасининг нотўғри созланиши ва х.

Ҳужумларни аниқлаш – корпоратив тармоқдаги шубҳали ҳаракатларни баҳолаш жараёни. Ҳужумларни аниқлаш операцион тизим ва иловаларни қайдлаш журналларини ёки реал вақтдаги трафикни таҳлиллаш орқали амалга оширилади. Тармоқ узеллари ёки сегментларида жойлаштирилган ҳужумларни аниқлаш компонент-

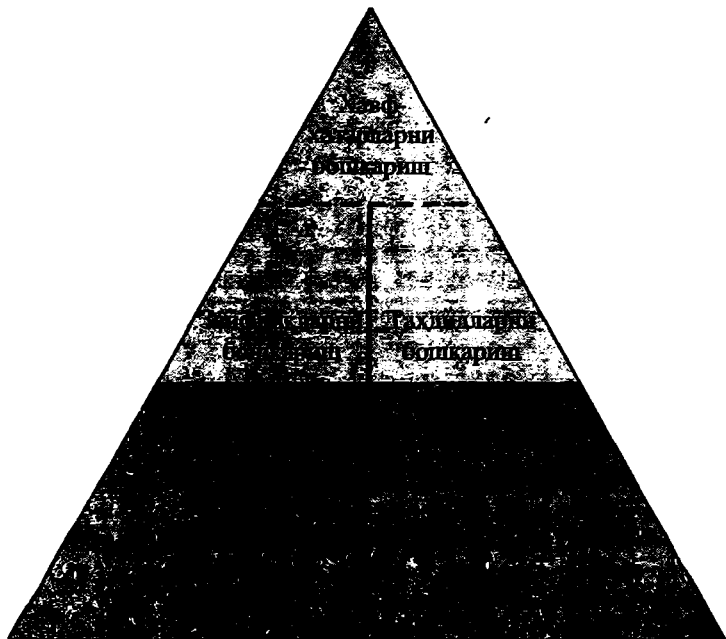
лари турли ходисаларни, хусусан, маълум заифликлардан фойдаланувчи ҳаракатларни ҳам баҳолайди (9.1-расм).



9.1-расм. Ҳимояланганликни таҳлиллаш ва ҳужумларни аниқлаш тизимларининг ўзаро алоқаси.

Хавфсизликни адаптив бошқариш модели ANSnинг адаптив компоненти, янги заифликлар хусусидаги энг охириги ахборотни тақдим қилган ҳолда, ҳимояланишни таҳлиллаш жараёнини модификациялашга жавоб беради. У ҳужумларни аниқлаш компоненти ҳам, уни ҳужумлар хусусидаги охириги ахборот билан тўлдириш орқали, модификациялайди. Адаптив компонентнинг мисоли сифатида янги вирусларни аниқлаш учун вирусга қарши дастурнинг маълумотлар базасини янгилаш механизмини кўрсатиш мумкин.

Хавфсизликни адаптив бошқариш моделидан (9.2-расм) фойдаланиш барча таҳдидларни назоратлаш ва уларга ўз вақтида самарали реакция кўрсатиш имконини беради. Бу эса ўз навбатида, нафакат таҳдидларнинг амалга оширилишига сабаб бўлувчи заифликларни баргараф қилишга, балки заифликлар пайдо бўлиш шартларини таҳлиллашга имкон беради.



9.2-расм. Хавфсизликни адаптив бошқариш модели.

Тармоқ хавфсизлигини адаптив бошқариш модели тармоқда суиистеъмол қилишни камайтиришга, тармоқдаги ходисалардан фойдаланувчилар, маъмурлар ва компания раҳбариятининг хабардорлик даражасини ошишига ҳам имкон беради. Таъкидлаш лозимки, ушбу модель олдин ишлатилувчи ҳимоялаш механизмларидан (фойдаланишни чегаралаш, аутентификациялаш ва х.) воз кечмайди. Уларнинг функционалигини янги технология эвазига кенгайтиради. Ўзларининг ахборот хавфсизлигини таъминлаш тизимларини замонавий талабларга мос қилишни хоҳловчи ташкилотлар мавжуд ечимларни урта янги компонент-ҳимояланишни таҳлиллаш, ҳужумларни аниқлаш ва хавф-хатарни баҳолаш билан гўлдириши лозим.

9.2. Ҳимояланишни таҳлиллаш

Ҳимояланишни таҳлиллаш воситалари заифликларни топиб ва ўз вақтида йўқ килиб хужумни амалга ошириш имкониятини бар-тараф қилади. Натижада, ҳимоялаш воситаларини ишлатилишига бўладиган барча сарф-харажатлар камаяди.

Ҳимояланишни таҳлиллаш воситалари тармоқ сатҳида, опера-цион тизим сатҳида ва иловалар сатҳида ишлаши мумкин. Улар текширишлар сонини бора-бора кўпайтириш, ахборот тизимида «ичкарилаб бориш» ва унинг барча сатҳларини тадқиқлаш орқали заифликларни кидириши мумкин.

Тармоқ протоколлари ва сервислари ҳимояланишини таҳлил-лаш воситалари. Ҳар қандай тармоқда абонентларнинг ўзаро алоқаси иккита ва ундан кўп узеллар орасида ахборот алмашилиши муолажаларини белгиловчи тармоқ протоколлари ва сервисларидан фойдаланишга асосланган. Тармоқ протоколлари ва сервисларини ишлаб чиқишда уларга ишланувчи ахборот хавфсизлигини таъмин-лаш бўйича талаблар (одатда, шубҳасиз етарли бўлмаган) қўйилган. Шу сабабли, тармоқ протоколларида аниқланган заифликлар хусу-сида ахборотлар пайдо бўлмоқда. Натижада, корпоратив тармоқда фойдаланадиган барча протокол ва сервисларни доимо текшириш зарурияти туғилади.

Ҳимояланишни таҳлиллаш тизими заифликларни аниқлаш бўйича тестлар сериясини бажаради. Бу тестлар нияти бузук одам-арнинг корпоратив тармоқларга хужумларида қўлланилганига ўхшаш.

Заифликларни аниқлаш мақсадида сканерлаш текширувчи ти-зим хусусидаги дастлабки ахборотни, хусусан, рухсат этилган про-токоллар ва очик портлар, операцион тизимнинг ишлатилувчи вер-сиялари ва ҳ. хусусидаги ахборотни олиш билан бошланади. Ска-нерлаш кенг тарқалган хужумлар, масалан, тўлик саралаш усули бўйича паролларни танлашдан фойдаланиб, суқилиб киришни ими-тациялашга уриниш билан тугайди.

Ҳимояланишни таҳлиллаш воситалари ёрдамида тармоқ сатҳида нафақат Internet нинг корпоратив тармоқдан рухсатсиз фойдаланиши имкониятини тестлаш, балки ташкилот ички тармоғида текширишни амалга ошириш мумкин. Тармоқ сатҳида ҳимояланишни таҳлиллаш тизими ташкилот хавфсизлик даражаси-

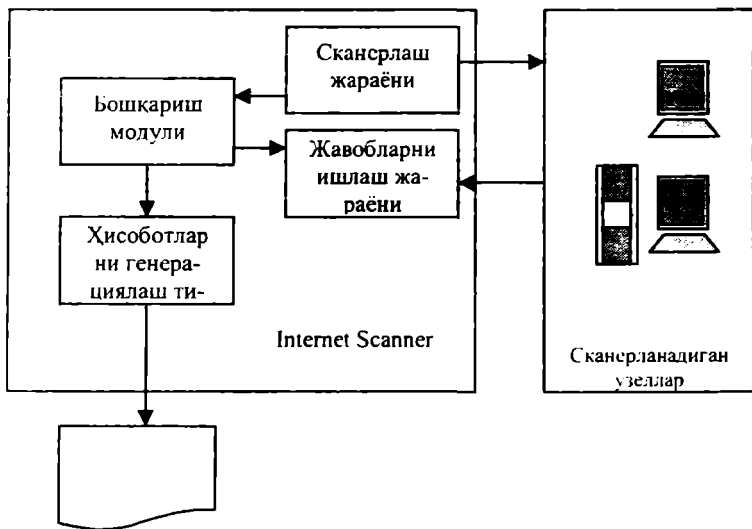
ни баҳолашга ҳамда тармок дастурий ва аппарат таъминотини соzлаш самарадорлигини назоратлашга хизмат килади.

Ҳимояланишни таҳлиллашни амалга оширувчи (Internet Scanner тизими мисолида) намунавий схема 9.3-расмда келтирилган.

Ҳимояланишни таҳлиллаш воситаларининг бу синфи нафақат тармок протоколлари ва сервислари, балки тармок билан ишлашга жавобгар тизимли ва татбикий дастурий таъминоти заифликларини ҳам таҳлиллайди. Бундай таъминот қаторига Web-, FTP-, ва почта серверларини, тармоқлараро экранларни, браузерларни ва х. кири-тиш мумкин.

Баъзи воситалар дастурий таъминотни таҳлиллаш билан бир қаторда аппарат воситаларини сканерлайди. Бундай воситаларга коммутацияловчи ва маршрутловчи асбоб-ускуналар киради.

Операцион тизим ҳимояланишини таҳлиллаш воситалари. Воситаларнинг бу синфи операцион тизим ҳимояланишига таъсир этувчи унинг соzланишларини текширишга аталган. Бундай соzлашлар қуйидагиларни аниқлайди:



9.3-расм. Internet Scanner тизими мисолида ҳимояланганликни таҳлиллаш схемаси.

- фойдаланувчиларнинг ҳисоб ёзуви, масалан, парол узунлиги ва унинг таъсир муддати;
- фойдаланувчиларнинг жиддий тизимли файллардан фойдаланиш ҳуқуқлари;
- заиф тизимли файллар;
- ўрнатилган патчлар ва ҳ.

Операцион тизим сатҳидаги ҳимояланишни таҳлиллаш тизимлари операцион тизимлар конфигурациясини назоратлашда ҳам ишлатилиши мумкин.

Тармок сатҳи ҳимояланишни таҳлиллаш воситаларидан фарқли равишда, ушбу тизимлар таҳлилланувчи тизимни ташқаридан эмас, балки ичкаридан сканерлайди, яъни улар ташқаридаги нияти бузук одамлар ҳужумларини имитацияламайди. Операцион тизим сатҳида ҳимояланишни таҳлиллаш тизимларининг баъзилари (масалан, Internet Security Systems компаниясининг System Scanner тизими) заифликларни аниқлаш имкониятидан ташқари, аниқланган муаммоларнинг бир қисмини автоматик тарзда бартараф қилишга ёки ташкилотда қабул қилинган хавфсизлик сиёсатини қониктирмайдиган тизим параметрларига тузатиш кириштишга имкон беради.

Танланувчи ҳимоялашни таҳлиллаш воситаларига қўйиладиган умумий талаблар. Танланувчи тизимга қўйиладиган мажбурий талаб-корхона тармок инфратузилмасини ўзгартириш заруриятининг йўқлиги. Акс ҳолда бундай қайтадан ташкил этишга қилинадиган харажат ҳимояланишни таҳлиллаш тизими нархидан ошиб кетиши мумкин. Ҳозирда бу талабга фақат Internet Security Systems компаниясининг Security Systems тизими жавоб беради.

Ҳимояланишни таҳлиллаш воситаларини нотўғри ишлатиш улардан нияти бузук одамларнинг корпоратив тармокқа сукилиб кириш учун фойдаланишларига имкон яратади. Шу сабабли, ҳимояланишни таҳлиллаш воситалари ўзларининг компонентларидан ва йиғилган маълумотлардан фойдаланишни чегараловчи механизмлар билан таъминланиши лозим. Бундай механизмларга қуйидагилар киради:

- фақат маъмур ҳуқуқига эга бўлган фойдаланувчи томонидан ушбу воситаларни ишга тушириш;
- сканерлаш маълумотлари архивини шифрлаш;
- масофадан бошқаришда уланишни аутентификациялаш;
- каталоглар билан ишлаш учун махсус ҳуқуқларни аниқлаш ҳ.

Заифликларни аниқлаш жараёнининг қуйидаги имкониятларига эътиборни қаратиш лозим:

- бир неча қурилма ёки сервисларни параллел ишлаш эвазига сканерлаш тезлигини ошириш;
- тизимдан рухсатсиз фойдаланишни олдини олиш учун ҳар бир сканерланувчи узелга билдириш қоғозини юбориш;
- ёлғон ишлашларни минималлаштириш учун тармокни эксплуатация талабларига тўғрилаш.

Корпоратив тармок ҳолатининг доимо ўзгариб туриши, унинг химояланишига таъсир кўрсатади. Шу сабабли, химояланишни тахлиллашнинг яхши тизими жадвал бўйича ишлаш режимига эга бўлиб, маъмур уни эслагунича ўзи тармок узеллари заифликларини текшириши ва пайдо бўлган муаммолар хусусида нафақат маъмурни огоҳлантириши, балки аниқланган заифликларни йўқотиш усулларини тавсия этиши лозим.

Эътибор бериш зарур бўлган характеристикалардан бири-хисоботларни генерациялаш тизимининг мавжудлиги. Бу тизим фойдаланувчиларнинг турли категорияларлари – техник мутахассислардан тортиб то ташкилотлар раҳбарлари учун тафсилоти турли даражада бўлган ҳужжатларни яратишга имкон бериши лозим.

Ҳужжатларда маълумотларни ифодалаш шакли ҳам муҳим ҳисобланади. Фақат матнли ахборот билан тўлдирилган ҳужжатларнинг фойдаси бўлмайди. Графиклардан фойдаланиш эса маъмурга ташкилот тармоғидаги барча муаммоларни яққол намоён этишга имкон беради. Ҳисоботларда аниқланган муаммоларни йўқотиш бўйича тавсияларнинг мавжудлиги химояланишни тахлиллаш воситаларини танлашдаги мажбурий шарт ҳисобланади.

Доимо янги заифликларнинг аниқланиши химояланишни тахлиллаш тизимининг заифликлар маълумотлари базасини тўлдира олиши имкониятига эга бўлишини тақозо этади. Бу заифликларни тавсифловчи махсус тил ёрдамида ёки тизим ишлаб чиқарувчилари томонидан заифликларни вақти-вақти билан тўлдириш йўли билан амалга оширилади. Корпоратив тармок узелларининг химояланиш даражасининг ўзгаришини тахлиллаш учун танланувчи восита ўтказилган сканерлаш сеанслари хусусидаги ахборотни тўпланишига имкон бериши лозим.

9.3. Ҳужумларни аниқлаш

Тармоқ ахборотини таҳлиллаш усуллари. Моҳияти бўйича, ҳужумларни аниқлаш жараёни корпоратив тармоқда бўлаётган шубҳали ҳаракатларни баҳолаш жараёнидир. Бошқача айтганда ҳужумларни аниқлаш ҳисоблаш ёки тармоқ ресурсларига йўналтирилган шубҳали ҳаракатларни идентификациялаш ва уларга реакция кўрсатиш жараёни. Ҳозирда ҳужумларни аниқлаш тизимида қуйидаги усуллар ишлатилади:

- статистик усул;
- эксперт тизимлари;
- нейрон тармоқлари.

Статистик усул. Статистик ёндашишнинг асосий афзаллиги – аллақачон ишлаб чиқилган ва ўзини танитган математик статистика аппаратини ишлатиш ва субъект характериға мослаш.

Аввал таҳлилланувчи тизимнинг барча субъектлари учун профиллар аниқланади. Ишлатиладиган профилларнинг эталондан ҳар қандай четланиши рухсат этилмаган фойдаланиш ҳисобланади. Статистик усуллар универсал ҳисобланади, чунки мумкин бўлган ҳужумларни ва улар фойдаланадиган заифликларни билиш талаб этилмайди. Аммо бу усуллардан фойдаланишда бир қанча муаммолар пайдо бўлади:

1. Статистик тизимлар ходисалар келиши тартибига сезувчанмаслар; баъзи ҳолларда бир ходисанинг ўзи, келиши тартибига кўра аномал ёки нормал фаолиятни характерлаши мумкин.

2. Аномал фаолиятни адекват идентификациялаш мақсадида ҳужумларни аниқлаш тизими томонидан кузатиловчи характеристикалар учун чегаравий (бўсағавий) қийматларни бериш жуда қийин.

3. Статистик усуллар вақт ўтиши билан бузгунчилар томонидан шундай «ўрганилиши» мумкинки, ҳужум ҳаракатлари нормал каби қабул қилинади.

Эксперт тизимлари. Эксперт тизими одам-эксперт билимларини қамраб олувчи қоидалар тўпламидан ташкил топган. Эксперт тизимдан фойдаланиш ҳужумларни аниқлашнинг кенг тарқалган усули бўлиб, ҳужумлар хусусидаги ахборот қоидалар кўринишида ифодаланади. Бу қоидалар ҳаракатлар кетма-кетлиги ёки сигнатуралар кўринишида ёзилиши мумкин. Бу қоидаларнинг ҳар бирининг бажарилишида рухсатсиз фаолият мавжудлиги хусусида

қарор қабул қилинади. Бундай ёндашишнинг муҳим афзаллиги – ёлғон тревоганинг умуман бўлмаслиги.

Эксперт тизимининг маълумотлари базасида ҳозирда маълум бўлган аксарият ҳужумлар сценарияси бўлиши лозим. Эксперт тизимлари, долзарбликни сақлаш мақсадида, маълумотлар базасини муттасил янгилашни талаб этади. Гарчи эксперт тизимлари қайдлаш журналларидаги маълумотларни кўздан кечиришга яхши имкониятни тавсия қилсада, сўралган янгиланиш эътиборсиз қолдирилиши ёки маъмур томонидан қўлда амалга оширилиши мумкин. Бу энг қаида, эксперт тизими имкониятларининг бўшашига олиб келади.

Эксперт тизимларининг камчиликлари ичида энг асосийси – номаълум ҳужумларни акслантира олмаслиги. Бунда олдиндан маълум ҳужумнинг ҳатто озгина ўзгариши ҳужумларни аниқлаш тизимининг ишлашига жиддий тўсик бўлиши мумкин.

Нейрон тармоқлари. Ҳужумларни аниқлаш усулларининг аксарияти қоидалар ёки статистик ёндашиш асосида назоратланувчи муҳитни таҳлиллаш шаклларида фойдаланади. Назоратланувчи муҳит сифатида қайдлаш журналлари ёки тармоқ трафиғи кўрилиши мумкин. Бундай таҳлиллаш маъмур ёки ҳужумларни яниқлаш тизими томонидан яратилган, олдиндан аниқланган қоидалар тўпламига таянади.

Ҳужумни вақт бўйича ёки бир неча нияти бузук одамлар ўртасида ҳар қандай бўлиниши эксперт тизимлар ёрдамида аниқлашга қийинчилик туғдиради. Ҳужумлар ва улар усулларининг турли-туманлиги туфайли, эксперт тизимлари қоидаларининг маълумотлар базасининг ҳатто, доимий янгиланиши ҳам ҳужумлар диапозонини аниқ идентификациялашни қафолатламайди.

Нейрон тармоқларидан фойдаланиш эксперт тизимларининг юкорида келтирилган муаммоларни бартараф этишнинг бир усули ҳисобланади. Эксперт тизимлари фойдаланувчига кўрилайётган харақтеристикалар маълумотлар базасидаги қоидаларга мос келиши ёки мос келмаслиги хусусида аниқ жавоб бераолса, нейротармоқ ахборотни таҳлиллайди ва маълумотларни аниқлашга ўрганган харақтеристикаларига мос келишини баҳолаш имкониятини тақдим этади. Нейротармоқли ифодаланишнинг мослик даражаси 100 %га етиши мумкин, аммо танлаш ҳақиқийлиги тамоман қўйилган масала мисолларини таҳлиллаш сифатига боғлиқ.

Аввал предмет соҳасининг олдиндан танлаб олинган мисолида нейротармокни тўғри идентификациялашга «ўргатишади». Нейротармок реакцияси таҳлилланади, кониқарли натижаларга эришиш мақсадида тизим созланади. Нейротармок ҳам вақт ўтиши билан, предмет соҳаси билан боғлиқ маълумотларни таҳлиллашни ўтказишига қараб «тажриба орттиради».

Нейротармоқларнинг суниестемол килинишни аниқлашдаги муҳим афзаллиги, уларнинг атайин килинадиган ҳужумлар харақтеристикаларини «ўрганиш» ва тармоқда олдин кузатилганига ўхшамаган элементларни идентификациялаш қобилиятидир.

Юқорида тавсифланган ҳужумларни аниқлаш усулларининг ҳар бири афзалликларга ва камчиликларга эга. Шу сабабли, ҳозирда тавсифланган усулларнинг фақат биттасидан фойдаланувчи тизимни учратиш қийин. Одатда, бу усуллар биргаликда ишлатилади.

Ҳужумларни аниқлаш тизимларининг туркумланиши. Ҳужумларни аниқлаш тизимлари IDS (Intrusion Detection System) да ишлатилувчи ҳужумларни аниқловчи механизмлар бир неча умумий усулларга асосланган. Таъкидлаш лозимки, бу усуллар бир-бирини инкор этмайди. Аксарият тизимларда бир неча усулларнинг комбинациясидан фойдаланилади.

Ҳужумларни аниқлаш тизимлари қуйидаги аломатлари бўйича туркумланиши мумкин:

- реакция кўрсатиш усули бўйича;
- ҳужумларни фош этиш усули бўйича;
- ҳужум хусусидаги ахборотни йиғиш усули бўйича.

Реакция кўрсатиш усули бўйича пассив ва актив IDSлар фарқланади. Пассив IDS лар ҳужум фактларини қайдлайди, маълумотларни журнал файлига ёзади ва огоҳлантиришлар беради. Актив IDSлар, масалан, тармоқлараро экранни қайта конфигурациялаш ёки маршрутизатордан фойдаланиш рўйхатини генерациялаш билан ҳужумга қарши ҳаракат қилишга уринади.

Ҳужумларни фош этиш усули бўйича IDSларни қуйидаги икита категорияга ажратиш қабул қилинган:

- аномал хатти-ҳаракатни аниқлаш (anomaly-based);
- суниестемолликларни аниқлаш (misuse detection ёки signature-based).

Аномал хатти-ҳаракатни аниқлаш йўли билан ҳужумларни аниқлаш технологияси қуйидаги гипотезага асосланган. Фойдаланувчининг аномал хатти-ҳаракати (яъни ҳужуми ёки қандайдир

ғаразли ҳаракати) – нормал хатти-ҳаракатдан четлашиш. Аномал хатти-ҳаракатга мисол тарикасида қисқа вақт оралиғида уланишларнинг катта сонини, марказий процессорнинг юқори юкланишини ва х. кўрсатиш мумкин.

Агар фойдаланувчининг нормал хатти-ҳаракати профилини бир маънода тавсифлаш мумкин бўлганида, ундан ҳар қандай четланишларни аномал хатти-ҳаракат сифатида идентификациялаш мумкин бўлар эди. Аммо, аномал хатти-ҳаракат ҳар доим ҳам хужум бўлавермайди. Масалан, тармок маъмури томонидан юборилган кўп сонли сўровларни хужумларни аниқлаш тизими «хизмат кўрсатишдан воз кечиш» хилидаги хужум сифатида идентификациялаши мумкин.

Ушбу технология асосидаги тизимдан фойдаланилганда иккита кескин ҳолат юз бериши мумкин:

– хужум бўлмаган аномал хатти-ҳаракатни аниқлаш ва уни хужумлар синфига киритиш;

– аномал хатти-ҳаракат таърифига мос келмайдиган хужумларни ўтказиб юбориш. Бу ҳолат хужум бўлмаган аномал хатти-ҳаракатни хужумлар синфига киритишга нисбатан хавфлироқ ҳисобланади.

Бу категория тизимларини соzлашда ва эксплуатациясида маъмур қуйидаги қийинчиликларга дуч келади:

– фойдаланувчи профилини қуриш сермехнат масала бўлиб, маъмурдан катта дастлабки ишларни талаб этади.

– юқорида келтирилган иккита кескин ҳаракатлардан бирининг пайдо бўлиши эҳтимоллигини пасайтириш учун фойдаланувчи хатти-ҳаракатининг чегаравий қийматларини аниқлаш зарур.

Аномал хатти-ҳаракатларни аниқлаш технологияси хужумларнинг янги хилини аниқлашга мўлжалланган. Унинг кимчилиги – доимо «ўрганиш» зарурияти.

Суиистеъмолликларни аниқлаш йўли билан хужумларни аниқлаш технологиясининг моҳияти хужумларни сигнатура кўринишида тавсифлаш ва ушбу сигнатурани назоратланувчи маконда (тармок трафигида ёки кайдлаш журналида) кидиришдан

иборат. Хужум сигнатураси сифатида аномал фаолиятни характерловчи ҳаракатлар шаблони ёки символлар сатри ишлатилиши мумкин. Бу сигнатуралар вирусга қарши тизимларда ишлатилувчи маълумотлар базасига ўхшаш маълумотлар базасида сақланади. Таъкидлаш лозимки, вирусга қарши резидент мониторлар ҳужумларни аниқлаш тизимларининг хусусий ҳоли ҳисобланади. Аммо бу йўналишлар бошидан параллел ривожланганлари сабабли, уларни ажратиш қабул қилинган. Ушбу хил тизимлар барча маълум ҳужумларни аниқласада, янги, ҳали маълум бўлмаган ҳужумларни аниқлай олмайди.

Бу тизимларни эксплуатациясида ҳам маъмурлар муаммоларга дуч келади. Биринчи муаммо – сигнатураларни тавсифлаш механизмларини, яъни ҳужумларни тавсифловчи тилларни яратиш. Иккинчи муаммо, биринчи муаммо билан боғлиқ бўлиб, ҳужумларни шундай тавсифлаш лозимки, унинг барча модификацияларини қайдлаш имкони туғилсин.

Ҳужум хусусидаги ахборотни йиғиш усули бўйича туркумлаш энг оммавий ҳисобланади:

- тармок сатҳида ҳужумларни аниқлаш (network-based);
- хост сатҳида ҳужумларни аниқлаш (host-based);
- илова сатҳида ҳужумларни аниқлаш (application-based).

Тармок сатҳида ҳужумларни аниқлаш тизимида тармокдаги трафикни эшитиш орқали нияти бузук одамларнинг мумкин бўлган ҳаракатлари аниқланади. Ҳужумни кидириш «хостдан-хостгача» принципи бўйича амалга оширилади. Ушбу хилга тааллуқли тизимлар, одатда ҳужумлар сигнатурасидан ва «бир зумда» таҳлиллашдан фойдаланиб, тармок трафигини таҳлиллайди. «Бир зумда» таҳлиллаш усулига биноан тармок трафиги реал ёки унга яқинрок вақтда мониторингланади ва мос аниқлаш алгоритмларидан фойдаланилади. Кўпинча руҳсатсиз фойдаланиш фаолиятини характерловчи трафикдаги маълум сатрларни кидириш механизмларидан фойдаланилади.

Хост сатҳида ҳужумларни аниқлаш тизими маълум хостда нияти бузук одамларни мониторинглаш, детектирлаш ва

ҳаракатларига реакция кўрсатишга аталган. Тизим химояланган хостда жойлашиб, унга қарши йўналтирилган ҳаракатларни текширади ва ошқор қилади. Бу тизимлар операцион тизим ёки илова-ларнинг қайдлаш журналларини таҳлиллайди. Қайдлаш журналларини таҳлиллаш усулини амалга ошириш осон бўлсада, у қуйидаги камчиликларга эга:

- журналда қайд этилувчи маълумотлар ҳажмининг катталиги назоратланувчи тизим ишлаши тезлигига салбий таъсир кўрсатади;
- қайдлаш журналинини таҳлиллашни мутахассислар ёрдамисиз амалга ошириб бўлмайди;
- ҳозиргача журналларни сақлашнинг унификацияланган формати мавжуд эмас;
- қайдлаш журналларидаги ёзувни таҳлиллаш реал вақтда амалга оширилмайди.

IDSнинг учинчи хили маълум иловадаги муаммоларни қидиришга асосланган.

Ҳужумларни аниқлаш тизимининг компонентлари ва архитектураси. Мавжуд ечимларнинг таҳлили ҳужумларни аниқлашнинг намунавий тизими компонентларининг рўйхатини келтиришга имкон беради.

Кузатиш модули назоратланувчи макондан (қайдлаш журнали ёки тармок трафиги) маълумотларни йиғишни таъминлайди. Унинг қуйидаги номлари ҳам учрайди: сенсор (sensor), монитор (monitor), зонд (probe) ва ҳ. Ҳужумларни аниқлаш тизими архитектурасининг қурилишига боғлиқ ҳолда кузатиш модули бошқа компонентлардан алоҳида, бошқа компьютерда жойлашиши мумкин.

Ҳужумларни аниқлаш қисм тизими асосий модул бўлиб, кузатиш модулидан олинadиган ахборотни таҳлиллайди. Ушбу таҳлиллаш натижаси бўйича қисм тизим ҳужумларни идентификациялаш, реакция кўрсатиш вариантлари бўйича тўхтамга келиши, маълумотлар омборида ҳужумлар хусусидаги ахборотни сақлаши мумкин ва ҳ.

Билимлар базасида, ҳужумларни аниқлаш тизимларида ишлатиладиган усулларга боғлиқ ҳолда, фойдаланувчилар ва ҳисоблаш

тизим профиллари, рухсатсиз фойдаланишларни характерловчи хужум сигнатуралари ёки шубҳали сатрлар сақланиши мумкин. Билимлар базаси хужумларни аниқлаш тизимларини ишлаб чиқарувчилари, тизимдан фойдаланувчилар ёки учинчи томон, масалан, бу тизимни мададловчи аутсорсинг компанияси томонидан тўлдирилиши мумкин.

Маълумотлар омбори хужумларни аниқлаш тизими ишлаши жараёнида йиғилган маълумотларнинг сақланишини таъминлайди.

График интерфейс тизимнинг ниҳоятда зарурий компоненти бўлиб, хужумларни аниқлаш тизими ишлашини бошқарувчи операция тизимга боғлиқ ҳолда де-факто Windows ва Unix стандартларига мос келиши лозим.

Реакция кўрсатиш қисм тизими аниқланган хужумлар ва бошқа назоратланувчи ходисаларга реакция кўрсатишни амалга оширади. Мавжуд тизимларда ишлатиладиган реакция кўрсатиш усулларини куйидаги учта категорияга ажратиш мумкин:

- билдириш;
- сақлаш;
- фаол реакция кўрсатиш.

Билдириш усули бўйича хужум хусусидаги ахборот хавфсизлик маъмурига, тизимнинг консолига ёки электрон почта бўйича, пейджерга факс ёки телефон орқали жўнатилиши мумкин.

Сақлаш усулига реакция кўрсатишнинг куйидаги вариантлари тааллуқли:

- ходисаларни маълумотлар базасида қайдлаш;
- хужумларни реал вақт масштабида тиклаш.

Биринчи вариант химоялашнинг бошқа тизимларида ҳам кенг қўлланилади. Иккинчи вариантни амалга ошириш учун хужум килувчини компания тармоғига ўтказиб юбориш ва унинг барча ҳаракатларини қайдлаш лозим. Бу хавфсизлик маъмурига кейин вақтнинг реал масштабида (ёки берилган тезликда) хужум килувчи томонидан қилинган барча ҳаракатларни тиклашга, муваффақиятли таҳлиллашга ва уларни кейинчалик бартараф этишга ҳамда

муҳокама килиш жараёнида йигилган ахборотдан фойдаланишга имкон беради.

Фаол реакция кўрсатиш категориясига қуйидаги вариантлар тааллуқли:

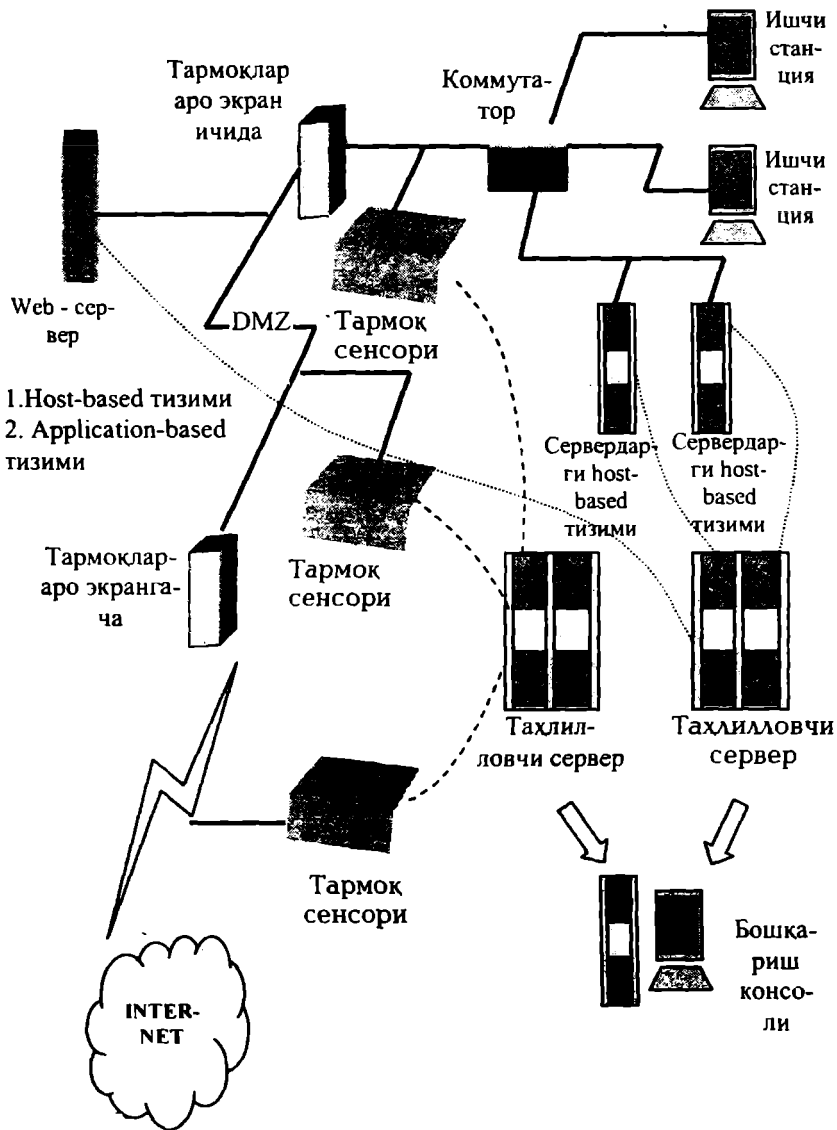
- хужум килувчи ишини блокировка килиш;
- хужум килинувчи узел билан сеансни тугаллаш;
- тармок асбоб-ускуналари ва химоя воситаларини бошқариш.

Реакция кўрсатиш механизмларининг ушбу категорияси бир томондан етарлича самарали бўлса, иккинчи томондан улардан жуда эҳтиётлик билан фойдаланиш зарур, чунки уларни нотўғри ишлатиш бугун корпоратив ахборот тизими ишга лаёқатлигининг бузилишига олиб келиши мумкин.

Компонентларни бошқариш қисм тизими хужумларни аниқлаш тизимининг турли компонентларини бошқаришга аталган. «Бошқариш» атамаси орқали хужумларни аниқлаш тизимининг турли компонентлари (масалан, кузатиш модуллари) учун хавфсизлик сиёсатини ўзгартириш ҳамда ушбу компонентлардан ахборотни (масалан, кайдланган хужум хусусидаги) олиш тушунилади. Бошқариш ички протоколлар ва интерфейслар ва ишлаб чиқилган стандартлар (масалан, SNMP) ёрдамида амалга оширилиши мумкин.

Хужумларни аниқлаш тизимлари иккита архитектура «автом агент» ва «агент-менеджер» архитектуралари асосида қурилади. Биринчи ҳолда тармокнинг ҳар бир химояланувчи узел ва сегментларига тизим агентлари ўрнатилиб, бу агентлар ўзаро ахборот алмаша олмайдилар ҳамда уларни ягона консол орқали марказлаштирилган ҳолда бошқариб бўлмайди. «Агент-менеджер» архитектураси бу камчиликлардан холи. Бу ҳолда катта тармокнинг турли қисмларида жойлашган кўпгина IDSдан иборат хужумларни аниқлашнинг тақсимланган тизими dIDS (distributed IDS)да маълумотларни йиғиш серверлари ва марказий таҳлилловчи сервер кайдланувчи маълумотларни марказлаштирилган йиғишни ва таҳлиллашни амалга оширади. dIDS модулларини бошқариш бошқаришнинг марказий консоли орқали амалга оширилади. Филиаллари турли ҳудудлар, ҳатто, шаҳарлар бўйича тарқалган йирик ташкилотлар учун бундай архитектуранинг ишлатилиши жиддий аҳамиятга эга.

dIDS ишлашининг умумий схемаси 9.4-расмда келтирилган.



9.4-расм. Таксимланган IDS ишлашининг умумий схемаси.

Бундай тизим турли IDSлардан хужумлар хусусидаги ахборотларни марказлаштирилиши эвазига корпоратив қисм тармок химояланишини кучайтиришга имкон беради. Хужумларни аникловчи тақсимланган тизим dIDS куйидаги қисм тизимлардан ташкил топган: бошқариш консоли, таҳлилловчи серверлар, тармок агентлари, хужум хусусидаги ахборотни йиғувчи сервер. Марказий таҳлилловчи сервер, одатда, маълумотлар базаси ва Web-сервердан ташкил топган бўлиб, хужумлар хусусидаги ахборотни сақлашга ва қулай Web-интерфейс ёрдамида маълумотларни манипуляциялашга имкон беради. Тармок агенти dIDSнинг энг муҳим компонентларидан бири ҳисобланиб, мақсади марказий таҳлилловчи серверга хужум хусусида хабар бериш бўлган кичкина дастурдир. Хужум хусусидаги ахборотни йиғувчи сервер марказий таҳлилловчи серверга мантикий таянган ва тармок агентларидан олинган маълумотларни гуруҳлашда фойдаланиладиган параметрларни белгилайди.

Маълумотларни гуруҳлашни куйидаги параметрлар бўйича амалга ошириш мумкин:

- хужум қилувчининг IP-манзили;
- қабул қилувчининг порти;
- агент номери;
- сана, вақт;
- протокол;
- хужум хиллари ва ҳ.

IDSдан фойдаланиш самарадорлигига қандайдир шубҳалар бўлишига қарамай, фойдаланувчилар IDSнинг бемалол тарқатилувчи ва тижорат воситаларидан кенг фойдаланадилар.

9.4. Компьютер вируслари ва вирусдан химояланиш муаммолари

Компьютер вирусининг кўп таърифлари мавжуд. Биринчи таърифни 1984 йили Фред Коэн берган: «Компьютер вируси – бошқа дастурларни, уларга ўзини ёки ўзгартирилган нусхасини ки-

ритиш оркали, уларни модификациялаш билан захарловчи дастур. Бунда киритилган дастур кейинги кўпайиш қобилиятини саклайди». Вируснинг ўз-ўзидан кўпайиши ва ҳисоблаш жараёнини модификациялаш қобилияти бу таърифдаги таянч тушунчалар ҳисобланади. Компьютер вирусининг ушбу хусусиятлари тирик табиат организмларида биологик вирусларнинг паразитланишига ўхшаш.

Ҳозирда компьютер вируси деганда қуйидаги хусусиятларга эга бўлган дастурий код тушунилади:

– аслига мос келиши шарт бўлмаган, аммо аслининг хусусиятларига (ўз-ўзини тиклаш) эга бўлган нусхаларни яратиш қобилияти;

– ҳисоблаш тизимининг бажарилувчи объектларига яратилувчи нусхаларнинг киритилишини таъминловчи механизмларнинг мавжудлиги.

Таъкидлаш лозимки, бу хусусиятлар зарурий, аммо етарли эмас. Кўрсатилган хусусиятларни ҳисоблаш муҳитидаги зарар келтирувчи дастур таъсирининг деструктивлик ва сир бой бермаслик хусусиятлари билан тўлдириш лозим.

Вирусларни қуйидаги асосий аломатлари бўйича туркумлаш мумкин:

- яшаш макони;
- операцион тизим;
- ишлаш алгоритми хусусияти;
- деструктив имкониятлари.

Компьютер вирусларини яшаш макони, бошқача айтганда вируслар киритилувчи компьютер тизими объектларининг хили бўйича туркумлаш асосий ва кенг тарқалган туркумлаш ҳисобланади (9.5-расм).



9.5-расм. Яшаш макони бўйича компьютер вирусларининг туркумланиши.

Файл вируслари бажарилувчи файлларга турли усуллар билан киритилади (энг кўп тарқалган вируслар хили) ёки файл-эгизакларни (компаньон вируслар) яратади ёки файлли тизимларни (link-вируслар) ташкил этиш хусусиятидан фойдаланади.

Юклама вируслар ўзини дискнинг юклама секторига (boot – секторига) ёки винчестернинг тизимли юкловчиси (Master Boot Record) бўлган секторга ёзади. Юклама вируслар тизим юкланишида бошқаришни оловчи дастур коди вазифасини бажаради.

Макровируслар ахборотни ишловчи замонавий тизимларнинг макродастурларини ва файлларини, хусусан Microsoft Word, Microsoft Excel ва х. каби оммавий муҳаррирларнинг файл-хужжатларини ва электрон жадвалларини захарлайди.

Тармоқ вируслари ўзини тарқатишда компьютер тармоқлари ва электрон почта протоколлари ва командаларидан фойдаланади.

Баъзида тармок вирусларини «курт» хилидаги дастурлар деб юри-тишади. Тармок вируслари Internet-куртларга (Internet бўйича таркалади), IRC-куртларга (чатлар, Internet Relay Chat) бўлинади.

Компьютер вирусларининг кўпгина комбинацияланган хилла-ри ҳам мавжуд, масалан – тармокли макровирус тахрирланувчи хужжатларни захарлайди ҳамда ўзининг нусхаларини электрон почта оркали тарқатади. Бошқа бир мисол сифатида файл-юклама вирусларини кўрсатиш мумкинки, улар файлларни ҳамда дисклар-нинг юкланадиган секторини захарлайди.

Вирусларнинг ҳаёт даври. Ҳар қандай дастурдагидек компью-тер вируслари ҳаёти даврининг иккита асосий босқичини – сақланиш ва бажарилиш босқичларини ажратиш мумкин.

Сақланиш босқичи вируснинг дискда у киритилган объект би-лан биргаликда шундайгина сақланиш даврига тўғри келади. Бу босқичда вирус вирусга қарши дастур таъминотига заиф бўлади, чунки у фаол эмас ва химояланиш учун операцион тизимни назорат қила олмайди.

Компьютер вирусларининг *бажарилиш даври*, одатда, бешта босқични ўз ичига олади:

1. Вирусни хотирага юклаш.
2. Қурбонни кидириш.
3. Топилган қурбонни захарлаш.
4. Деструктив функцияларни бажариш.
5. Бошқаришни вирус дастур-элтувчисига ўтказиш.

Вирусни хотирага юклаш. Вирусни хотирага юклаш операци-он тизим ёрдамида вирус киритилган бажарилувчи объект билан бир вақтда амалга оширилади. Масалан, агар фойдаланувчи вирус бўлган дастурий файлни ишга туширса, равшанки, вирус коди уш-бу файл қисми сифатида хотирага юкланади. Оддий ҳолда, вирусни юклаш жараёни-дискдан оператив хотирага нусхалаш бўлиб, сўнгра бошқариш вирус бадани кодига узатилади. Бу ҳаракатлар операцион тизим томонидан бажарилади, вируснинг ўзи пассив ҳолатда бўлади. Мураккаброк вазибаларда вирус бошқаришни ол-ганидан сўнг ўзининг ишлаши учун қўшимча ҳаракатлар бажариши мумкин. Бу билан боғлиқ иккита жиҳат кўрилади.

Биринчиси вирусларни аниқлаш муолажасининг максимал му-раккаблашиши билан боғлиқ. Сақланиш босқичида баъзи вируслар химояланишни таъминлаш максидида етарлича мураккаб алгоритм-дан фойдаланади. Бундай мураккаблашишга вирус асосий бадани-

ни шифрлашни киритиш мумкин. Аммо факат шифрлашни ишла-тиш чала чора хисобланади, чунки юкланиш боскичида расшиф-ровкани таъминловчи вирус кисми очик кўринишда сакланиши ло-зим. Бундай холатдан кутилиш учун вирусларни ишлаб чиқувчилар расшифровка қилувчи кодини «мутациялаш» механизмидан фойда-ланади. Бу усулнинг мохияти шундан иборатки, объектга вирус нухаси киритилишида унинг расшифровка қилувчига тааллужли кисми шундай модификацияланадики, оригинал билан матнли фаркланиш пайдо бўлади, аммо иш натижаси ўзгармайди.

Кодни мутациялаш механизмидан фойдаланувчи вируслар *полиморф вируслар* номини олган. Политморф вируслар (polymorphic)-кийин аникланадиган вируслар бўлиб, сигнатуралар-га эга эмас, яъни таркибида бирорта хам кодининг доимий кисми йўк. Полиморфизм файлли, юкламали ва макровирусларда учрай-ди.

Стелс-алгоритмлардан фойдаланилганда вируслар ўзларини тизимда тўла ёки кисман беркитишлари мумкин. Стелс-алгоритмларидан фойдаланадиган вируслар – *стелс-вируслар* (Stealth) деб юритилади. Стелс-вируслар операцион тизимнинг ши-кастланган файлларга мурожаатини ушлаб қолиш йўли билан ўзини яшаш маконидалигини яширади ва операцион тизимни ахбо-ротни шикастланмаган кисмига йўналтиради.

Иккинчи жиҳат *резидент вируслар* деб аталувчи вируслар би-лан боғлиқ. Вирус ва у киритилган объект операцион тизим учун бир бутун бўлганлиги сабабли, юкланишдан сўнг улар, табиий, ягона манзил маконида жойлашади. Объект иши тугаганидан сўнг у оператив хотирадан бўшалади. Бунда бир вақтнинг ўзида вирус хам бўшалиб сакланишнинг пассив боскичига ўтади. Аммо баъзи вируслар хили хотирада сакланиш ва вирус элтувчи иши тугашидан сўнг фаол қолиш қобилиятига эга. Бундай вируслар резидент но-мини олган. Резидент вируслар, одатда, факат операцион тизимга рухсат этилган имтиёзли режимлардан фойдаланиб яшаш макони-ни захарлайди ва маълум шароитларда зараркунандалик вазифаси-ни бажаради. Резидент вируслар хотирада жойлашади ва компью-тер ўчирилишигача ёки операцион тизим қайта юкланишигача фаол холда бўлади.

Резидент бўлмаган вируслар фақат фаоллашган вақтларида хо-тирага тушиб захарлаш ва зараркунандалик вазифаларини бажара-ди. Кейин бу вируслар хотирани бутунлай тарк этиб яшаш макони-да қолади.

Таъкидлаш лозимки, вирусларни резидент ва резидент бўлмаганларга ажратиш факат файл вирусларига тааллуқли. Юкла- нувчи ва макровируслар резидент вирусларга тегишли.

Қурбонни қидириш. Қурбонни кидириш усули бўйича вирус- лар иккита синфга бўлинади. Биринчи синфга операцион тизим функцияларидан фойдаланиб фаол кидиришни амалга оширувчи вируслар киради. Иккинчи синфга кидиришнинг пассив механизм- ларини амалга оширувчи, яъни дастурий файлларга тузук қўювчи вируслар тааллуқли.

Топилган қурбонни захарлаш. Оддий ҳолда захарлаш деганда қурбон сифатида танланган объектда вирус кодининг ўз-ўзини нус- халаши тушунилади.

Аввал файл вирусларининг захарлаш хусусиятларини кўрайлик. Бунда иккита синф вируслари фаркланади. Биринчи синф вируслари ўзининг кодини дастурий файлга бевосита кирит- майди, балки файл номини ўзгартириб, вирус бадани бўлган янги файлни яратади. Иккинчи синфга қурбон файлларига бевосита ки- рувчи вируслар тааллуқли. Бу вируслар киритилиш жойлари билан характерланади. Қуйидаги вариантлар бўлиши мумкин:

1. **Файл бошига киритиш.** Ушбу усул MS-DOSнинг *com*- файллари учун энг қулай ҳисобланади, чунки ушбу форматда хиз- матчяи сарлавҳалар кўзда тутилган.

2. **Файл охирига киритиш.** Бу усул энг кўп тарқалган бўлиб, вируслар кодига бошқаришни узатиш дастурнинг биринчи коман- даси (*com*) ёки файл сарлавҳасини (*exe*) модификациялаш орқали таъминланади.

3. **Файл ўртасига киритиш.** Одатда, бу усулдан вируслар тузилмаси олдиндан маълум файлларга (масалан, *Command.com* файли) ёки таркибида бир хил кийматли байтлар кетма-кетлиги бўлган, узунлиги вирус жойлашишига етарли файлларга татбикан фойдаланади.

Юклама вируслар учун захарлаш босқичининг хусусиятлари улар киритилувчи объектлар – кайишқок ва қаттиқ дисklarнинг юкланиш секторларининг сифати ва қаттиқ дискнинг бош юклама ёзуви (MBR) орқали аниқланади. Асосий муаммо-ушбу объект ўлчамларининг чегараланганлиги. Шу сабабли, вируслар ўзларининг қурбон жойида сиғмаган қисмини дискда саклаши, ҳамда захарланган юқловчи оригинал кодини ташиши лозим.

Макровируслар учун захарлаш жараёни танланган хужжат-курбонда вирус кодини саклашдан иборат. Баъзи ахборотни ишлаш дастурлари учун буни амалга ошириш осон эмас, чунки хужжат файллари форматининг макропрограммаларни саклаши кўзда тутилмаган бўлиши мумкин.

Деструктив функцияларни бажариш. Деструктив имкониятлари бўйича беziён, хавфсиз, хавfli ва жуда хавfli вируслар фаркланади.

Беziён вируслар – ўз-ўзидан таркалиш механизми амалга оширилувчи вируслар. Улар тизимга зарар келтирмайди, фақат дискдаги бўш хотирани сарфлайди холос.

Хавфсиз вируслар – тизимда мавжудлиги турли таассурот (овоз, видео) билан боғлиқ вируслар, бўш хотирани камайтирсада, дастур ва маълумотларга зиён етказмайди.

Хавfli вируслар – компьютер ишлашида жиддий нуқсонларга сабаб бўлувчи вируслар. Натижада, дастур ва маълумотлар бузилиши мумкин.

Жуда хавfli вируслар – дастур ва маълумотларни бузилишига ҳамда компьютер ишлашига зарур ахборотни ўчирилишига бевосита олиб келувчи, муолажалари олдиндан ишлаш алгоритмларига жойланган вируслар.

Бошқаришни вирус дастур – элтувчисига ўтказиш. Таъкидлаш тозимки, вируслар бузувчилар ва бузмайдиганларга бўлинади.

Бузувчи вируслар дастурлар захарланганида уларнинг ишга лаёқатлигини саклаш хусусида кайғурмайдилар, шу сабабли уларга ушбу боскичнинг маъноси йўқ.

Бузмайдиган вируслар учун ушбу боскич хотирада дастурни коррект ишланиши шарт бўлган кўринишда тиклаш ва бошқаришни вирус дастур-элтувчисига ўтказиш билан боғлиқ.

Зарар келтирувчи дастурларнинг бошқа хиллари. Вируслардан ташқари зарар келтирувчи дастурларнинг қуйидаги хиллари мавжуд:

- троян дастурлари;
- мантикий бомбалар;
- масофадаги компьютерларни яширинча маъмурловчи хакер утилиталари;
- Internetдан ва бошқа конфиденциал ахборотдан фойдаланиш паролларини ўғирловчи дастурлар.

Улар орасида аниқ чегара йўқ: троян дастурлари таркибида вируслар бўлиши, вирусларга мантикий бомбалар жойлаштирилиши мумкин ва ҳ.

Троян дастурлар ўзлари кўпаймайди ва таркатилмайди. Ташқаридан троян дастурлар мутлако беозор кўринади, ҳатто, фойдали функцияларни тавсия этади. Аммо фойдаланувчи бундай дастурни компьютерига юклаб, ишга туширса, дастур билдирмай зарар келтирувчи функцияларни бажариши мумкин. Кўпинча троян дастурлар вирусларни дастлабки тарқатишда, Internet орқали масофадаги компьютердан фойдаланишда, маълумотларни ўғирлашда ёки уларни йўқ қилишда ишлатилади.

Мантикий бомба – маълум шароитларда зарар келтирувчи ҳаракатларни бажарувчи дастур ёки унинг алоҳида модуллари. Мантикий бомба, масалан, маълум сана келганда ёки маълумотлар базасида ёзув пайдо бўлганида ёки йўқ бўлганида ва ҳ. ишга тушиши мумкин. Бундай бомба вирусларга, троян дастурларга ва оддий дастурларга жойлаштирилиши мумкин.

Вируслар ва зарар келтирувчи дастурларни тарқатиш каналлари. Компьютерлар ва корпоратив тармоқларни химояловчи самарадор тизимни яратиш учун каердан хавф туғилишини аниқ тасаввур этиш лозим. Вируслар тарқалишнинг жуда хилма-хил каналларини топади. Бунинг устига эски усулларга янгиси қўшилади.

Тарқатишнинг классик (мумтоз) усуллари. Файл вируслари дастур файллари билан биргаликда дискетлар ва дастурлар алмашишда, тармоқ каталогларидан, Web- ёки FTP – серверлардан дастурлар юкланишида тарқатилади. Юклама вируслар компьютерга фойдаланувчи захарланган дискетани дисководда қолдириб, сўнгра операцион тизимни қайта юклашида тушиб қолади. Юклама вирус компьютерга вирусларнинг бошқа хили орқали киритилиши мумкин. Макрокоманда вируслари Microsoft Word, Excel, Access файллари каби офис ҳужжатларининг захарланган файллари алмашишида тарқалади.

Агар захарланган компьютер локал тармоққа уланган бўлса вирус осонгина файл-сервер дискларига тушиб қолиши, у ердан каталоглар орқали тармоқнинг барча компьютерларига ўтиши мумкин. Шу тарика вирус эпидемияси бошланади. Вирус тармоқда шу вирус тушиб қолган компьютер фойдаланувчиси ҳуқуқлари каби ҳуқуққа эга эканлигини тизим маъмури унутмаслиги лозим. Шунинг учун у фойдаланувчи фойдаланадиган барча каталогларга ту-

шиб қолиши мумкин. Агар вирус тармоқ маъмури ишчи станциясига тушиб қолса оқибати жуда оғир бўлиши мумкин.

Электрон почта.

Ҳозирда Internet глобал тармоғи вирусларнинг асосий манбаи ҳисобланади. Вируслар билан захарланишларнинг аксарияти Microsoft Word форматида хатлар алмашишда содир бўлади. Электрон почта макрокоманда вирусларини тарқатиш канали вазифасини ўтайди, чунки ахборотлар билан бир қаторда кўпинча офис ҳужжатлари жўнатилади.

Вируслар билан захарлаш билмасдан ва ёмон ниятда амалга оширилиши мумкин. Масалан, макровирус билан захарланган муҳаррирдан фойдаланувчи ўзи шубҳа қилмаган ҳолда, манзилатларга захарланган хатларни жўнатиши мумкин. Иккинчи тарафдан нияти бузук одам атайин электрон почта орқали ҳар қандай хавфли дастурий кодни жўнатиши мумкин.

Троян Web-сайтлар. Фойдаланувчилар вирусни ёки троян дастурни Internet сайтларининг оддий кузатишда, троян Web-сайтни кўрганида олиши мумкин. Фойдаланувчи браузерларидаги хатликлар кўпинча троян Web-сайтлари фаол компонентларининг фойдаланувчи компьютерларига зарар келтирувчи дастурларни киритишига сабаб бўлади. Троян сайтни кўришга таклифни фойдаланувчи оддий электрон хат орқали олиши мумкин.

Локал тармоқлар.

Локал тармоқлар ҳам тезликда захарланиш воситаси ҳисобланади. Агар химоянинг зарурий чоралари кўрилмаса, захарланган ишчи станция локал тармоққа киришда сервердаги бир ёки бир неча хизматчи файлларни захарлайди. Бундай файллар сифатида Login.com хизматчи файли, фирмада қўлланилувчи Excel-жадваллар ва стандарт ҳужжат-шаблонларни кўрсатиш мумкин. Фойдаланувчилар бу тармоққа киришида сервердан захарланган файлларни ишга туширади, натижада, вирус фойдаланувчи компьютеридан фойдалана олади.

Зарар келтирувчи дастурларни тарқатишнинг бошқа каналлари.

Вирусларни тарқатиш каналларидан бири дастурий таъминотнинг қарокчи нусхалари ҳисобланади. Дискетлар ва CD-дисклардаги ноқунуний нусхаларда кўпинча турли-туман вируслар билан захарланган файллар бўлади. Вирусларни тарқатиш манба-

ларига электрон анжуманлар ва FTP ва BBS файл-серверлар ҳам тааллуқли.

Ўқув юртларида ва Internet-марказларида ўрнатилган ва умум-фойдаланиш режимида ишловчи компьютерлар ҳам осонгина вирусларни тарқатиш манбаига айланиши мумкин. Агар бундай компьютерлардан бири навбатдаги фойдаланувчи дискетидан заҳарланган бўлса, шу компьютерда ишловчи бошқа фойдаланувчилар дискетлари ҳам заҳарланади.

Компьютер технологиясининг ривожланиши билан компьютер вируслари ҳам, ўзининг янги яшаш маконига мослашган ҳолда, такомиллашади. Ҳар қандай онда янги, олдин маълум бўлмаган ёки маълум бўлган, аммо янги компьютер асбоб-ускунасига мўлжалланган компьютер вируслари, троян дастурлари ва куртлар пайдо бўлиши мумкин. Янги вируслар маълум бўлмаган ёки олдин мавжуд бўлмаган тарқатиш каналларидан ҳамда компьютер тизимларга татбиқ этишнинг янги технологияларидан фойдаланиши мумкин. Вирусдан заҳарланиш хавфини йўқотиш учун корпоратив тармокнинг тизим маъмури, нафақат вирусга қарши усуллардан фойдаланиши, балки компьютер вируслари дунёсини доимо кузатиб бориши шарт.

9.5. Вирусга қарши дастурлар

Компьютер вирусларини аниқлаш ва улардан химояланиш учун махсус дастурларнинг бир неча хиллари ишлаб чиқилган бўлиб, бу дастурлар компьютер вирусларини аниқлаш ва йўқотишга имкон беради. Бундай дастурлар вирусга қарши дастурлар деб юритилади. Умуман, барча вирусга қарши дастурлар заҳарланган дастурларнинг ва юклама секторларнинг автоматик тарзда тикланишини таъминлайди.

Вирусларга қарши дастурлар фойдаланадиган вирусларни аниқлашнинг асосий усуллари куйидагилар:

- эталон билан таққослаш усули;
- эвристик таҳлил;
- вирусга қарши мониторинг;
- ўзгаришларни аниқловчи усул;
- компьютернинг киритиш-чиқариш базавий тизими (BIOS-га) вирусга қарши воситаларни ўрнатиш ва х.

Эталон билан таққослаш усули энг оддий усул бўлиб, маълум вирусларни кидиришда никоблардан фойдаланади. Вируснинг никоби-мана шу муайян вирусга хос коднинг қандайдир ўзгармас кетма-кетлигидир. Вирусга қарши дастур маълум вирус никобларини кидиришда текширилувчи файлларни кетма-кет кўриб чиқади (сканерлайди). Вирусга қарши сканерлар фақат никоб учун белгиланган, олдиндан маълум вирусларни топа олади. Оддий сканерлар компьютерни янги вирусларнинг суқилиб киришидан химояламайди. Янги дастурни ёки юклама секторини захарлашда коддини тўла ўзгартира олувчи шифрланувчи ва полиморф вируслар учун никоб ажратиш мумкин эмас. Шу сабабли сканер уларни аниқламайди.

Эвристик таҳлил. Компьютер вируси кўпайиши учун хотирада нусхаланиш, секторга ёзилиш каби қандайдир муайян ҳаракатларни амалга ошириши лозим. Эвристик таҳлиллагичда бундай ҳаракатларнинг рўйхати мавжуд. Эвристик таҳлиллагич дастурларни, диск ва дискет юклама секторларини, уларда вирусга хос кодларни аниқлашга уринган холда, текширади. Таҳлиллагич захарланган файлни топиб, монитор экранига ахборот чиқаради ва шахсий ёки тизимли журналга ёзади. Эвристик таҳлил олдин маълум бўлмаган вирусларни аниқлайди.

Вирусга қарши мониторинг. Ушбу усулнинг моҳияти шундан иборатки, компьютер хотирасида бошқа дастурлар томонидан бажарилувчи шубҳали ҳаракатларни мониторингловчи вирусга қарши дастур доимо бўлади. Вирусга қарши мониторинг барча ишга туширилувчи дастурларни, яратилувчи, очилувчи ва сақланувчи ҳужжатларни, Internet орқали олинган ёки дискетдан ёки ҳар қандай компакт-дискдан нусхаланган дастур ва ҳужжатларнинг файлларини текширишга имкон беради. Агар қандайдир дастур хавфли ҳаракатни қилишга уринмокчи бўлса, вирусга қарши монитор фойдаланувчига хабар беради.

Ўзгаришларни аниқловчи усул. Дискни тафтиш қилувчи деб аталувчи ушбу усулни амалга оширишда вирусга қарши дастур дискнинг ҳужумга дучор бўлиши мумкин бўлган барча соҳаларини олдиндан хотирлайди, сўнгра уларни вақти-вақти билан текширади. Вирус компьютерларни захарлаганида қаттиқ диск гаркибини ўзгартиради: масалан, дастур ёки ҳужжат файлига ўзининг коддини кўшиб кўяди. Autoexec.bat файлига дастур-вирусни чакиришни кўшади, юклама секторни ўзгартиради, файл-йўлдош яратади. Диск

соҳалари характеристикаларининг кийматлари солиштирилганида вирусга қарши дастур маълум ва ноъмалум вируслар томонидан қилинган ўзгаришларни аниқлаши мумкин.

*Компьютерларнинг киритиш-чиқариш базавий тизими*га (BIOSга) вирусга қарши воситаларни ўрнатиш. Компьютерларнинг тизимли платасига вируслардан химоялашнинг оддий воситалари ўрнатилади. Бу воситалар каттик дискларнинг бош юклама ёзувига ҳамда дисклар ва дискетларнинг юклама секторларига барча мурожаатларни назоратлашга имкон беради. Агар қандайдир дастур юклама секторлар таркибини ўзгартиришга уринса, химоя ишга тушади ва фойдаланувчи огоҳлантирилади. Аммо бу химоя жуда ҳам ишончли эмас.

Вирусга қарши дастурларнинг хиллари. Вирусга қарши дастурларнинг қуйидаги хиллари фаркланади:

- дастур-фаглар (вирусга қарши сканерлар);
- дастур-тафтишчилар (CRC-сканерлар);
- дастур-блокировка қилувчилар;
- дастур-иммунизаторлар.

Дастур-фаглар энг оммавий ва самарали вирусга қарши дастур ҳисобланади. Самарадорлиги ва оммавийлиги бўйича иккинчи ўринда дастур-тафтишчилар туради. Одатда, бу иккала дастур хиллари битта вирусга қарши дастурга бирлаштирилади, натижада, унинг қуввати анчагина ошади. Турли хил блокировка қилувчилар ва иммунизаторлар ҳам ишлатилади.

Дастур-фаглар (сканерлар) вирусларни аниқлашда эталон билан таққослаш усулидан, эвристик таҳлиллашдан ва бошқалардан фойдаланади. Дастур-фаглар оператив хотира ва файлларни сканерлаш йўли билан муайян вирусга характерли бўлган никобни қидиради. Дастур-фаглар нафақат вируслар билан захарланган файлларни топади, балки уларни даволайди ҳам, яъни файлдан дастур-вирус баданини олиб ташлаб, файлни дастлабки ҳолатига қайтаради. Дастур-фаглар аввал оператив хотирани сканерлайди, вирусларни аниқлайди ва уларни йўқотади, сўнгра файлларни даволашга киришади. Файллар ичида вирусларни катта сонини қидиришга ва йўқ қилишга аталган дастур-фаглар, яъни полифаглар ҳам мавжуд.

Дастур-фаглар иккита категорияга бўлинади: универсал ва ихтисослаштирилган сканерлар. Универсал сканерлар сканер ишлаши мўлжалланган операцион тизим хилига боғлиқ бўлмаган ҳолда,

вирусларнинг барча хилларини кидиришга ва зарарсизлантиришга мўлжалланган. Ихтисослаштирилган сканерлар вирусларнинг чегараланган сонини ёки уларнинг бир синфини, масалан макровирусларни зарарсизлантиришга аталган. Фақат макровирусларга мўлжалланган ихтисослаштирилган сканерлар MS WORD ва Excel муҳитларида ҳужжат алмашилиш тизимини химоялашда энг қулай ва ишончли ечим ҳисобланади.

Дастур-фаглар сканерлашни «бир зумда» бажарувчи мониторинглашнинг резидент воситаларига ва фақат сўров бўйича тизимни текширишни таъминловчи резидент бўлмаган сканерларга ҳам бўлинади. Мониторинглашнинг резидент воситалари тизимни ишончлироқ химоялашни таъминлайди, чунки улар вируслар пайдо бўлишига дарров реакция кўрсатади, резидент бўлмаган сканер эса вирусни аниқлаш қобилиятига фақат навбатдаги ишга туширилишида эга бўлади.

Дастур-фагларнинг афзаллиги сифатида уларнинг универсаллигини кўрсатиш мумкин. Дастур-фагларнинг камчилиги сифатида вирусларни кидириш тазлигининг нисбатан катта эмаслигини ва вирусга қарши базаларнинг нисбатан катта ўлчамларини кўрсатиш мумкин. Ундан ташқари: янги вирусларнинг доим пайдо бўлиши сабабли дастур-фаглар тездан эскиради ва улар версияларининг мунтазам янгиланиши талаб этилади.

Дастур-тафтишчилар (CRC-сканерлар) вирусларни кидиришда ўзгаришларни аниқловчи усулдан фойдаланади. CRC-сканерлар дискдаги файллар-тизимли сектордагилар учун CRC-йиғиндини (циклик назорат кодини) ҳисоблашга асосланган. Бу CRC-йиғиндилар вирусга қарши маълумотлар баъзасида файллар узунлиги, саналар ва охири модификацияси ва бошқа параметрлар хусусидаги қўшимча ахборотлар билан бир қаторда сакланади. CRC-сканерлар ишга туширилишида маълумотлар базасидаги маълумот билан реал ҳисобланган қийматларни таққослайди. Агар маълумотлар базасидаги ёзилган файл хусусидаги ахборот реал қийматларга мос келмаса, CRC-сканерлар файл ўзгартирилганлиги ёки вирус билан захарланганлиги хусусида хабар беради. Одатда, ҳолатларни таққослаш операцион тизим юкланишдан сўнг дарҳол ўтказилади.

CRC-сканерларнинг қамчилиги сифатида уларнинг янги файллардаги вирусларни аниқлай олмаслигини кўрсатиш мумкин, чунки уларнинг маълумотлар базасида бу файллар хусусидаги ахборот мавжуд эмас.

Дастур-блокировка қилувчилар вирусга қарши мониторинглаш усулини амалга оширади. Вирусга қарши блокировка қилувчилар резидент дастурлар бўлиб, вирус хавфи вазиятларини тўхтатиб қолиб, у хусусида фойдаланувчига хабар беради. Вирус хавфи вазиятларига вирусларнинг кўпайиши онларидаги характерли чакириқлар киради. Блокировка қилувчиларнинг афзалликлари сифатида вируслар кўпайишининг илк босқичида уларни тўхтатиб қолишини кўрсатиш мумкин. Бу айниқса, кўпдан бери маълум вируснинг мунтазам пайдо бўлишида муҳим ҳисобланади. Аммо, улар файл ва дискларни даволамайди. Блокировка қилувчиларнинг камчилиги сифатида улар химоясининг айланиб ўтиш йўлларининг мавжудлигини ва уларнинг «хираликликни» (масалан, улар бажаришчи файлларнинг ҳар қандай нусхаланишига уриниш хусусида мунтазам огоҳлантиради) кўрсатиш мумкин. Таъкидлаш лозимки, компьютер аппарат компоненти сифатида яратилган вирусга қарши блокировка қилувчилар мавжуд.

Дастур-иммунизаторлар – файллар захарланишини олдини олувчи дастурлар икки хилга бўлинади: захарланиш хусусида хабар берувчи ва вируснинг қандайдир хили бўйича захарланишни блокировка қилувчи. Биринчи хил иммунизаторлар, одатда, файл охирига ёзилади ва файл ишга туширилганда ҳар марта унинг ўзгаришини текширади. Бундай иммунизаторлар битта жиддий камчиликка эга. Улар стелс-вирус билан захарланишни аниқлай олмайди. Шу сабабли бу хил иммунизаторлар ҳозирда ишлатилмайди.

Иккинчи хил иммунизаторлар тизимни вируснинг маълум тури билан захарланишдан химоялайди. Бу иммунизатор дастур ёки дискни шундай модификациялайдики, бу модификациялаш уларнинг ишига таъсир этмайди, вирус эса уларни захарланган деб қабул қилади ва сукилиб қирмайди. Иммунизациялашнинг бу хили универсал бўлаолмайди, чунки файлларни барча маълум вируслардан иммунизациялаш мумкин эмас. Аммо бундай иммунизаторлар чала чора сифатида компьютерни янги ноъмаълум вирусдан, у вирусга қарши сканерлар томонидан аниқланишига қадар, ишончли химоялаши мумкин.

Вирусга қарши дастурнинг сифат мезонлари. Вирусга қарши дастурни бир неча мезонлар бўйича баҳолаш мумкин. Қуйида бу мезонлар муҳимлиги даражаси пасайиши тартибда келтирилган:

– ишончлилиги ва ишлаш қулайлиги фойдаланувчилардан махсус ҳаракатларни талаб этувчи техник муаммоларнинг йўқлиги; вирусга қарши дастурнинг ишончлилиги энг муҳим мезон ҳисобланади, чунки энг яхши вирусга қарши дастур сканерлаш жараёнини охиригача олиб бора олмаса, у бефойда ҳисобланади;

– вирусларни барча тарқалган хилларини аниқлаш фазилати, ички файл-ҳужжатлар/жадвалларни (MS Office), жойлаштирилган ва архивланган файлларни сканерлаш, вирусга қарши дастурнинг асосий вазифаси-100 % вирусларни аниқлаш ва уларни даволаш;

– барча оммавий платформалар (DOS, Windows 95/NT, Novell NetWare, OS/2, Alpha, Linux ва х.) учун вирусга қарши дастур версияларининг мавжудлиги;

– сўров бўйича сканерлаш ва «бир зумда» сканерлаш режимларининг борлиги, тармокни маъмурлаш имкониятли сервер версияларининг мавжудлиги. Вирусга қарши дастурнинг кўп платформалилиги муҳим мезон ҳисобланади, чунки муайян операцион тизимга мўлжалланган дастургина бу тизим функцияларидан тўла фойдаланиш мумкин. Файлларни «бир зумда» текшириш имконияти ҳам вирусга қарши дастурларнинг етарлича муҳим мезони ҳисобланади. Компьютерга келувчи файлларни ва қўйилувчи дискетларни бир лаҳзада ва мажбурий текшириш вирусдан заҳарланмасликка 100 %ли кафолат беради. Агар вирусга қарши дастурнинг сервер вариантыда тармокни маъмурлаш имконияти бўлса, унинг қиймати янада ошади.

Ишлаш тезлиги. Вирусга қарши дастурнинг ишлаш тезлиги ҳам унинг муҳим мезони ҳисобланади. Турли вирусга қарши дастурларда вирусни кидиришнинг ҳар хил алгоритмларидан фойдаланилади. Бир алгоритм тезкор ва сифатли бўлса, иккинчиси суст ва сифати паст бўлиши мумкин.

Химоянинг профилактика чоралари. Ҳар бир компьютерда вируслар билан заҳарланган файллар ва дискларни ўз вақтида аниқлаш, аниқланган вирусларни тамомила йўқотиш вирус эпидемиясининг бошқа компьютерларга тарқалишининг олдини олади. Ҳар қандай вирусни аниқлашни ва йўқ қилишни кафолатловчи

мутлак ишончли дастурлар мавжуд эмас. Компьютер вируслари билан курашишнинг муҳим усули ўз вақтидаги профилактика ҳисобланади.

Вирусдан захарланиш эҳтимоллигини жиддий камайтириш ва дисклардаги ахборотни ишончли сақланишини таъминлаш учун куйидаги профилактика чораларини бажариш лозим:

- факат конуний, расмий йўл билан олинган дастурий таъминотдан фойдаланиш;

- компьютерни замонавий вирусга қарши дастурлар билан таъминлаш ва улар версияларини доимо янгилаш;

- бошқа компьютерларда дискетда ёзилган ахборотни ўқишдан один бу дискетда вирус борлигини ўзининг компьютеридаги вирусга қарши дастур ёрдамида доимо текшириш;

- ахборотни иккилаш. Аввало дастурий таъминотнинг дистрибутив элгувчиларини сақлашга ва ишчи ахборотни сақланишига эътибор бериш;

- компьютер тармоқларидан олинувчи барча бажарилувчи файлларни назоратлашда вирусга қарши дастурдан фойдаланиш;

- компьютерни юклама вируслардан захарланишига йўл қўймаслик учун, операцион тизим ишга туширилганида ёки қайта юкланишида дисковод чўнтагида дискетани колдирмаслик.

Вирусга қарши дастурларнинг ҳар бири ўзининг афзалликларига ва камчиликларига эга. Факат вирусга қарши дастурларнинг бир неча хилини комплекс ишлатилиши мақбул натижага олиб келиши мумкин.

Куйида вирусдан захарланиш профилактикасига, вирусларни аниқлаш ва йўқотишга мўлжалланган баъзи дастурий комплекслар тавсифланган.

AVP (Антивирус Касперского Personal) – Россиянинг вирусга қарши пакети. Пакет таркибига куйидагилар қиради:

- Office Guard – блокировка қилувчи, макровирусдан 100 % химояланишни таъминлайди;

- Inspector – тафтишчи, компьютердаги барча ўзгаришларни кузатади, вирус фаоллиги аниқланганида дискнинг асл нусхасини

тиклашга ва зарар келтирувчи кодларни чиқариб ташлашга имкон беради;

– Monitor – вирусларни ушлаб қолувчи, компьютер хотирасида доимо ҳозир бўлиб, файллар ишга туширилганида, яратилишида ёки нусхаланишида уларни вирусга қарши текширади;

– Scanner – вирусга қарши модул, локал ва тармоқ дисклар таркибини кенг қўламли текшириш имконини беради. Сканерни қўл ёрдамида ёки берилган вақтда автоматик тарзда ишга тушириш мумкин.

Пакет ёрдамида электрон почтани вирусга қарши филтрлаш ва почта корреспонденциясини комплекс текшириш амалга оширилади. Вирусга қарши базани янгилаш Internet орқали бажарилади.

Dr.Web – Россиянинг вирусга қарши оммавий дастури. Windows 9x/NT/2000/XP учун мўлжалланган бўлиб, файлли, юклама ва файл-юклама вирусларни кидиради ва зарарсизлантиради. Дастур таркибида резидент қорувул SpIDer Guard, Internet орқали вирус базаларини янгилашнинг автоматик тизими ва автоматик текшириш жадвалини режалаштирувчи мавжуд. Почта файлларини текшириш амалга оширилган.

Dr.Web да ишлатилувчи алгоритмлар ҳақида маълум бўлган барча вирус хилларини аниқлашга имкон беради. Dr.Web дастурининг муҳим хусусияти – оддий сигнатурли кидириш натижа бермайдиган мураккаб шифрланган ва полиморф вирусларни аниқлаш имкониятидир.

Symantec Antivirus – Symantec компаниясининг корпоратив фойдаланувчиларга таклиф этган вирусга қарши маҳсулоти тўплами.

Symantec маҳсулотидан ишчи жойларининг умумий сони 100 ва ундан ортиқ бўлганида ва бўлмаганда битта Windows NT/2000/NetWare сервери мавжудлигида фойдаланиш мақсадга мувофиқ ҳисобланади. Ушбу пакетнинг башқалардан ажралиб турадиган хусусияти қуйидагилар:

– бошқаришнинг иерархик модели;

– янги вирус пайдо бўлишига реакция қилиш механизмининг мавжудлиги.

AntiVir Personal Edition – вирусга қарши дастур AVP, Dr.Web ва х.лар имкониятларидек имкониятларга эга. Дастур комплектига қуйидагилар киради:

- дискларни сканерловчи;
- резидент қоровул;
- бошқариш дастури;
- режалаштирувчи.

Дастур Internet дан юкланувчи файлларни сканерлайди. Internet орқали янгиланишларни автоматик тарзда текшириш ва юклаш функцияси ҳам мавжуд. Дастур хотирани, юкланиш секторини текширишда ва унда вируслар бўйича кенг қўламдаги маълумот-нома мавжуд.

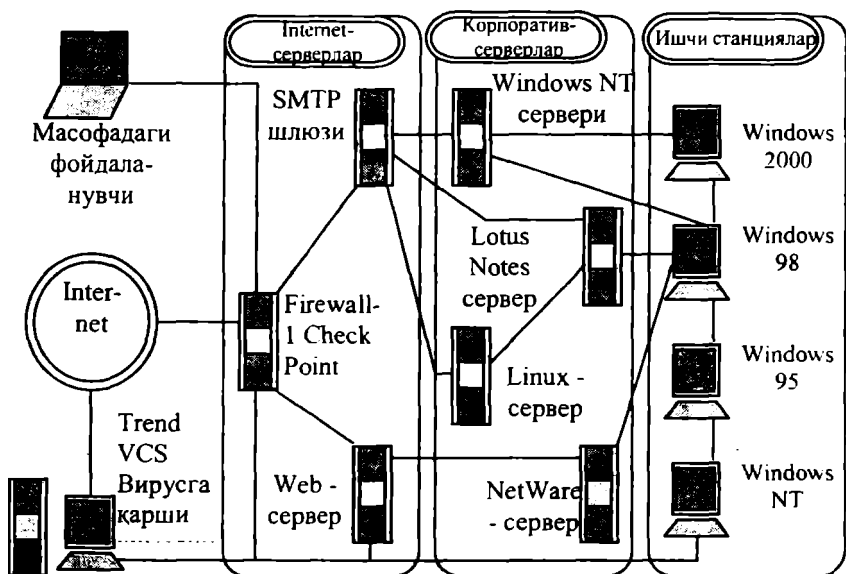
9.6. Вирусга қарши химоя тизимини қуриш

Ҳозирда ўртача компаниянинг корпоратив компьютер тармоғи таркибида ўнлаб ва юзлаб ишчи станциялари, ўнлаб серверлар, телекоммуникациянинг турли фаол ва пассив асбоб-ускуналари мавжуд бўлган етарлича мураккаб тузилмага эга (10.6-расм).

Корпоратив тармоқдан фойдаланувчилар тармоқка вирусларнинг сукилиб кириш файллари билан доимо тўқнашадилар. Internet/intranet корпоратив тизимларига вирус хужумлари мунтазам бўлиб туради, фойдаланувчи ишчи станциясининг захарланган ахборот элтувчиси томонидан захарланиши эса одат тусини олган.

Корпоратив тармоқ вируслар ва бошқа зарар келтирувчи дастурлар хужумларига дучор бўлганида тармоқнинг вирусга қарши химояси кўпинча вирусга қарши локал дастурий таъминот ёрдамида, сканерлаш ва қатор ишчи станцияларни даволаш билан тугайди ва химоя таъминланади дсб ҳисобланади. Аслида муаммонинг бундай локализациялаш минимал чора ҳисобланади ва корпоратив тармоқнинг кейинги барқарор ишлашини кафолатламайди. Бошқача айтганда, вирусга қарши локал ечимларнинг ишлатилиши

корхонани вирусдан самарали химоялаш учун зарурий, аммо етарли восита ҳисобланмайди.



9.6-рас.м. Корпоратив тармок намунавий архитектураси.

Вирусга қарши химоянинг самарали корпоратив тизими «мижоз-сервер» технологияси бўйича амалга оширилган, тармоқдаги ҳар қандай шубҳали ҳаракатни сезгирлик билан фахмлаб олувчи, тесқари боғланишли мосланувчан тизимдир. Бундай тизим корпоратив тармоқнинг ички тузилмаси доирасида вирусларнинг ва бошқа ғаним дастурларнинг тарқалишига йўл қўймайди. Вирусга қарши химоянинг самарали корпоратив тизими турли вирус ҳужумларини-маълумларини, ҳам номаълумларини, улар намоён бўлишининг дастлабки босқичида, аниқлайди ва бета-рафлаштиради.

Албатта, турли вазиятлар бўлиши мумкин, масалан, масофадан фойдаланувчининг захарланган компьютерини корпоратив серверга улаганда ёки макровируслар бўлган WORD ёки Excel файлли дискетлардан иш жойларида фойдаланишда тармоқ захарланиши мумкин. Аммо, сифатли қурилган вирусга қарши химоянинг кор-

поратив тизими учун бу жиддий эмас, чунки, биринчидан, захарланишнинг кўрсатилган ҳолатлари камдан-кам учрайди, иккинчидан, вируслар вақтида аниқланади ва бетарафлаштирилади. Натижада, уларнинг кўпайишига ва корпоратив тармок доирасида тарқалишига йўл қўйилмайди.

Уланадиган ишчи станциялари сони ошган сари корпоратив тармокнинг хизмат кўрсатиш нархи оша боради. Корпоратив тармокни вируслардан химоялаш харажатлари корхона умумий харажатлари рўйҳатида охириги бандни эгалламайди.

Ушбу харажатларни корпоратив тармокни вирусга қарши химоялашни вактнинг реал масштабида марказлаштирилган бошқариш орқали оптималлаштириш ва камайтириш мумкин. Бундай ечим корхона тармоғи маъмурларига вирусни барча сукилиб кириш нукталарини бошқаришнинг ягона консоли орқали кузатишга ва корпоратив тармокдаги барча вирусга қарши воситаларни самарали бошқаришга имкон беради. Вирусга қарши химояни марказлаштирилган бошқариш мақсади жуда оддий – вирусларнинг барча сукилиб кириш нукталарини блокировка қилиш. Қуйидаги сукилиб киришларни ва захарланишларни кўрсатиш мумкин:

- ташувчи манбалардан (флоппи-дисклар, компакт-дисклар, Zip, Jazz, Floptical ва х.) охириги захарланган файллардан фойдаланишда ишчи станцияларга вирусларнинг сукилиб кириши;

- Web ёки FTP Internetдан орқали олинган локал ишчи станциясида сақланган захарланган текин дастурий таъминот ёрдамида захарланиш;

- масофадаги ёки мобил фойдаланувчиларнинг захарланган ишчи станциялари корпоратив тармокка уланганида вирусларнинг сукилиб кириши;

- корпоратив тармокка уланган масофадаги сервердаги вируслар билан захарланиш;

- иловаларида макровируслар билан захарланган Excel ва Word файллар бўлган электрон почтанинг тарқалиши.

Вируслардан ва бошқа зарар келтирувчи дастурлардан химояловчи корпоратив тизимни қуриш қуйидаги босқичларни ўз ичига олади.

Биринчи босқичда химояланувчи тармокнинг ўзига хос хусусиятлари аниқланади ва бир неча вирусга қарши химоя вариантлари танланади ва асосланади. Бу босқичда қуйидагилар бажарилади:

– компьютер тизими ва вирусга қарши химоя воситаларининг аудити;

– ахборот тизимини текшириш ва *картирлаш*;

– вирусларнинг суқилиб кириши билан боғлиқ таҳдидларнинг амалга ошириш сценарийсини таҳлиллаш.

Натижада, вирусга қарши химоянинг умумий ҳолати баҳоланади.

Иккинчи босқичда вирусга қарши хавфсизлик сиёсати ишлаб чиқилади. Бу босқичда қуйидагилар бажарилади:

– ахборот ресурсларини туркумлашнинг тури;

– вирусга қарши хавфсизликни таъминловчи кучларни яратиш-ваколатларни тақсимлаш;

– вирусга қарши хавфсизликни ташкилий-ҳуқуқий мададлаш;

– вирусга қарши хавфсизлик инструментларига талабларни аниқлаш;

– вирусга қарши хавфсизликни таъминлаш харажатларини ҳисоблаш.

Натижада, корхонанинг вирусга қарши хавфсизлик сиёсати ишлаб чиқилади.

Учинчи босқичда дастурий воситалари, ахборот ресурсларини инвентаризациялаш ва мониторингини автоматлаштириш воситалари танланади. Вирусга қарши хавфсизликни таъминлаш бўйича ташкилий тадбирлар рўйхати ишлаб чиқилади.

Натижада корхонанинг вирусга қарши хавфсизлигини таъминловчи режа ишлаб чиқилади.

Тўртинчи босқичда вирусга қарши танланган ва тасдиқланган хавфсизлик режаси амалга оширилади. Бу босқичда вирусга қарши воситалар етказиб берилади, жорий этилади ва мададланади.

Натижада, корпоратив вирусга қарши химоялашнинг самарали тизими яратилишига имкон туғилади.

10.1. Маълумотларни узатиш тармоқларида ахборот ҳимоясини таъминлаш

Маълумотларни узатиш тармоқларида ахборот ҳимоясини таъминлаш масаласи маълумотлар узатиш тармоғининг муайян архитектурасини амалга оширувчи ва унинг барқарор ишлашини таъминловчи аппарат-дастурий воситалари билан боғлиқ ҳолда ечилиши лозим.

Маълумотларни узатиш тармоқларида ахборот хавфсизлигини таъминлашга куйидаги талаблар куйилади:

– маълумотларни узатиш тармоқларида ахборот хавфсизлигига бўладиган маълум таҳдидлардан ҳимоялаш хизмати ва механизмларини белгиловчи *функционал талаблар*;

– ахборот хавфсизлигига бўладиган маълум таҳдидлардан ҳимоялаш механизминини маълумотларни узатиш тармоғи архитектурасига қай тарзда жорий этилиши лозимлигини белгиловчи *архитектуравий талаблар*;

– бошқаришнинг қандай функциялари ишлаб чиқилиши ва улар қай тарзда маълумотларни узатиш тармоғига жорий этилишини белгиловчи *бошқариш (маъмураш) талаблари*.

Функционал талаблар. Маълумотларни узатиш тармоғи компонентларига ва архитектурасига реал таъсир этувчи умумий функционал талаблар куйидагилар:

– *фойдаланувчини аутентификациялаш*. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминловчи тизим ахборотни (маълумотларни) узатиш жараёнида иштирок этувчи компонентининг (объект, субъект ва фойдаланувчининг) ҳақиқийлигини аниқлаш имкониятини таъминлаши лозим;

– *назоратланувчи фойдаланиш*. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминловчи тизим тармоқ субъектлари ва фойдаланувчиларининг руҳсат этилмаган ахборот ресурсларидан фойдалана олмасликларини кафолатлаши лозим;

– *конфиденциалликни таъминлаш*. Конфиденциалликни таъминлаш хизмати асосан маълумотларни узатиш тармоғини ахборот мухитини очиш, ахборотдан рухсатсиз фойдаланиш ва ўғирлаш имкониятларидан ҳимоялаш учун зарур хисобланади;

– *маълумотлар яхлитлигини таъминлаш*. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминловчи тизим таркибида фойдаланувчи ва бошқариш ахбороти бўлган маълумотларнинг сақланиш ва узатилиш яхлитлигини кафолатлаши лозим. Маълумотларнинг бузилиши, сохталаштирилиши, кечиктирилиши, рухсатсиз қайталаниши ахборот узатилишининг блокировка қилинишига олиб келиши мумкин;

– *қатъий ҳисоб-китоб*. Маълумотларни узатиш тармоғи ресурсларидан фойдаланувчи ҳар қандай субъект бажарган ҳар қандай амаллари учун жавоб бериши лозим. Маълумотларни узатиш тармоғи устида қилинган барча ҳаракатлар ва тармоқда содир бўлган барча ходисалар хусусидаги ахборотнинг сақланиш имконияти таъминланиши лозим;

– *хавфни билдирувчи сигнални генерациялаш*. Маълумотларни узатиш тармоғи тармоқ ахборот хавфсизлиги объектлари томонидан хавфсизликнинг бузилиши хусусидаги сигнални генерациялаш имконини таъминлаши лозим;

– *аудит*. Аудит тизимни бошқаришнинг самарадорлигини баҳолаш ҳамда ахборот хавфсизлигининг бузилишини аниқлаш мақсадида тизимли ёзувларни ва амалларни мустақил таҳлиллаш ва тадқиқлаш сифатида кўрилиши лозим;

– *тиклаш*. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш тизими хавфсизликнинг бузилишини тиклаш қобилиятига эга бўлиши лозим. Ҳар доим, қачон ахборот хавфсизлигини бузишга уриниш содир бўлганида, тизим ушбу уриниш хусусидаги ахборотни шундай ишлаши лозимки, ушбу уриниш маълумотларни узатиш тармоғининг ўтказиш қобилиятини ва фойдаланувчанлигини жиддий пасайишига олиб келмасин;

– *мосланувчанлик*. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш тизимида қўйиладиган муҳим концептуал талаб-мосланувчанлик талаби, яъни алоқа тармоғининг тузилмаси, технологияси ва ишлаш шароити ўзгарганида мослашув қобилияти талабидир.

Архитектуравий талаблар. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш тизими ахборот хавф-

сизлигининг турли сиёсатини мададлаши, яъни мосланувчан бўлиши лозим. Тизимга қуйидаги асосий хизматлар киритилиши мумкин:

- шифрлаш калитларини ва паролларни шакллантириш, саклаш ва таксимлаш хизмати;
- шифрлаш хизмати;
- фойдаланувчиларни ва хабарларни аутентификациялаш хизмати;
- фойдаланишни бошқариш хизмати;
- хабарлар яхлитлигини таъминлаш хизмати;
- фойдаланувчанликни таъминлаш хизмати;
- етказилганликни тасдиқлаш хизмати;
- рад килмаслик хизмати;
- кўшимча трафикни шакллантириш хизмати;
- маъмурлаш хизмати.

Бу хизматларнинг ҳар бири ахборот хавфсизлигини таъминлаш бўйича масалаларни мустақил тарзда у ёки бу ҳимоя механизмларидан фойдаланиб ечилиши мумкин. Бунда ҳимоянинг битта механизми ахборот хавфсизлигининг турли хизматларида қўлланилиши мумкин.

Бошқариш (маъмурлаш) талаблари. Маълумотларни узатиш тармоғида ахборот хавфсизлигини маъмурлаш хизмати ҳимоянинг техник воситаларини тўлдирувчи ҳимоя чораларининг маълум комплексини ўз ичига олади. Бу ҳимоя чоралари бузғунчининг тармок ахборот хавфсизлигига таҳдидни кучайтиришга қаратилган у ёки бу таъсирни ўтказишини кийинлаштириш мақсадида мавжуд ҳимоя тизимига оператив тарзда ўзгартиришлар киритишга имкон яратади.

Маъмурлаш хизматининг асосий вазифалари қуйидагилар:

- ҳимоя хизмати ва механизмига зарур ахборотни тарқатиш;
- ҳимоя хизмати ва механизмининг ишлаши хусусидаги ахборотни йиғиш ва таҳлиллаш;
- ҳимояланувчи объектларни аниқлаш;
- хизмат функцияларини самарали амалга ошириш мақсадида ҳимоя механизмларини комбинациялаш;
- маълумотларни узатиш тармоғининг ишончли ва барқарор ишлашини таъминлаш хизматларига жавобгар бошқа маъмурлар билан ўзаро алоқа;

– маълумотларни узатувчи тармоқнинг бузилган ишлаш жа-
раёнини тиклаш.

Хавфсизлик маъмури маъмурлаш хизматининг муҳим элемен-
ти ҳисобланади. Ахборот хавфсизлигининг ҳар қандай воситалари-
дан фойдаланилмасин, маълумотларни узатиш тармоғида ахборот
хавфсизлигини таъминлаш сифати маъмурнинг қобилиятига, унинг
тиришишига, техник жиҳозланганлигига боғлиқ.

Таъкидлаш лозимки, бирорта ҳам реал химояланган маълумот-
ларни узатиш тармоғи мутлақ химояланган бўлмайди. Шунга
қарамасдан химоянинг адекват чоралари бузғунчи таъсири самара-
сини (зарар келтириш харажатиининг қутилаётган зарар ўлчамига
нисбатини) анчагина пасайтиради.

10.2. Алоқа каналларида маълумотларни химоялаш усуллари

Маълумотларни узатишни химоялаш масаласини ечиш усулла-
рининг учта асосий гуруҳи мавжуд: каналга мўлжалланган
химоялаш усуллари, чеккалараро химоялаш усуллари ва уланишга
мўлжалланган химоялаш усуллари. Биринчиси ҳар бир канал учун
мустақил равишда маълумотлар оқимини химоялашни таъминласа,
иккинчиси ҳар бир хабарни, уни манбадан манзилгача узатишда
умумий химоялашни таъминлайди. Учинчи усул иккинчи усулнинг
бир тури ҳисобланади.

Каналга мўлжалланган усуллар манба ва манзилга боғлиқ
бўлмаган ҳолда, алоҳида узеллар орасидаги алоҳида алоқа канали
бўйича узатилаётган хабарлар оқимини химоялашни таъминлайди.
Бу хил химояни таъминлашда бузғунчининг узелга (пакетни ком-
мутацияловчи марказга) қараганда каналга таъсир этиш қулайлиги
фараз қилинади. Ундан ташқари, маълумотларни узатиш
тармоғидаги узелларни фойдаланувчи терминалларини
химоялагандек химоялаш мумкин эмас ёки иктисод нуктаи назари-
дан фойдасиз. Ушбу гуруҳ усулларининг камчилиги-кисм тармоқ
узелларидан бирининг очилиши тармоқ орқали ўтаётган хабарлар
оқимининг талайгина қисмини очилишига олиб келиши мумкин.

Терминаллар ва тармоқлар ўртасидаги алоқа каналларини ка-
налга мўлжалланган химоялаш харажатлари бевосита дахлдор та-
рафлар томонидан қоплансада, маълумотларни узатиш қисм
тармоғи ичидаги каналга мўлжалланган химоялаш усулларининг

умумий нархи қисм тармоқдан фойдаланувчиларнинг барчаси ўртасида ҳисоблаб чиқилиши мумкин.

Чеккалараро ҳимоялаш усуллари хабарларни манба узеллари ва қабул қилувчи орасида узатиш жараёнида шундай ҳимоялайдики, манба ва манзилат орасидаги алоқа каналларидан бирининг очилиши хабарлар оқимининг очилишига олиб келмайди. Ушбу усулларнинг асосий афзаллиги – улардан фойдаланиш масаласи алоҳида фойдаланувчилар орасида, бошқа фойдаланувчиларни жалб этмасдан, ечилиши мумкин.

Уланишга мўлжалланган усуллар. Аксарият қўлланиш соҳаларида маълумотларни узатиш тармоғини манбадан манзилгача уланишни ёки виртуал канални ўрнатиш учун фойдаланувчига тақдим этилувчи муҳит сифатида тасаввур этиш мумкин. Бундай тасаввур этишда ҳимоянинг уланишга мўлжалланиши фараз қилинади, яъни, ҳар бир уланиш ёки виртуал канал алоҳида ҳимояланади. Шундай қилиб, уланишга мўлжалланган усуллар чеккалар аро ҳимоялаш усулларининг бир тури ҳисобланади. Уланишга мўлжалланган усуллар турли шароитларда умумий ҳимоянинг юқори даражасини таъминлайди ва ҳимояга қўйиладиган талаблар хусусидаги фойдаланувчининг идрокига мос келади. Чунки, уланишга мўлжалланган ахборот конфиденциаллигини ҳимоялаш усуллари асбоб-усқунани ҳимоялашни, масалан, фақат хабарлар манбаида ва қабул қилувчида ахборотдан руҳсатсиз фойдаланишдан ҳимоялашни кўзда тутаяди. Айни вақтда ҳимоялашнинг каналга мўлжалланган усуллари руҳсатсиз фойдаланишдан ҳимоялашнинг маълумотларни узатиш тармоғидаги ҳар бир узели томонидан таъминланишини талаб этиши мумкин. Аммо, баъзида иккала усулни қўллаганда ҳимоялашнинг тежамли даражасига эришилади.

Маълумотларни узатишни ҳимоялашнинг у ёки бу усулидан фойдаланишдаги асосий вазифалар қуйидагилар:

- хабарлар мазмунининг фош қилинишини олдини олиш;
- хабарлар оқимининг таҳлилланишини олдини олиш;
- хабарлар оқими ҳақиқийлигини бузилганлигини аниқлаш;
- ёлғон уланишни аниқлаш.

Ахборот тизимлари ёки маълумотларни узатиш тармоқларида ахборот хавфсизлигини таъминлаш мақсадида маълумотларни узатишни ҳимоялаш усулларидан нафақат бузғунчи таъсири оқибатларини аниқлашни, балки, агар оқибатлар вақтинча ҳарак-

терга эга бўлганида, узилган (бузилган) узатиш жараёнини автоматик тарзда тиклашни талаб этиш керак.

Ҳозирда юкорида келтирилган вазифаларнинг бажарилишини таъминловчи химоялашнинг стандартлаштирилган механизмлари мавжуд эмас. Ҳар бир муайян ҳолда маълумотларни узатиш хавфсизлиги масалалари ахборотларни криптографик ўзгартириш усуллари, ахборотларни хабарларга бардош кодлаш усуллари, хабарларнинг ҳақиқийлигини таъминловчи усуллар, тизимлар ишлашнинг ишончлилигини, яшовчанлигини ва барқарорлигини таъминловчи усулларга асосланган химоялашнинг турли механизмларини биргаликда ишлатиш орқали ҳал этилади.

Хабарлар мазмунининг фош қилинишини олдини олишда химоялашнинг каналга мўлжалланган ҳамда уланишга мўлжалланган усулларида фойдаланиш мумкин.

Юкорида айтиб ўтилганидек, каналли шифрлаш алоқа тармоғининг ҳар бир каналида мустақил тарзда бажарилиши мумкин. Каналли шифрлашда, одатда, окимли шифрлаш ишлатилади ва узеллар орасида шифрланган матн битларининг узлуксиз окими мададланади. Тармоқларда коммутациялаш (маршрутлаш) вазифалари фақат узелларда бажарилиши сабабли, алоқа каналида пакстнинг сарлавҳалари билан бирга ахборот қисмини ҳам шифрлаш мумкин.

Аммо маълумотлар фақат каналда (каналлар орқали уланган узелларда эмас) шифрланиши сабабли барча оралик узеллар химояланиши лозим. Бунинг устига узелларни нафақат физик химояланиши, балки бу узелларнинг аппарат-дастурий воситалари томонидан узеллар орқали ўтувчи ҳар бир уланишдаги ахборотни яқкалаши кафолатланиши зарур.

Чеккалараро шифрлашда маршрутизаторда ишланувчи ҳар бир хабар (сарлавҳанинг баъзи маълумотлари бундан истисно) йўл бошида шифрланади ва белгиланган жойга стмагунча расшифровка қилинмайди. Ҳар бир уланиш учун ўзининг калити ишлатилиши мумкин.

Хабарлар окимини таҳлиланишидан химоялаш, одатда, турли синфларга мансуб хабарлар узунлиги ва частотасининг қийматларини, манба манзилларини ва хабарлар окими манзилларини беркитишга йўл очилган. Агар каналли шифрлаш ишлатилса, узеллар орасида маълумотлар узатилганида шифрланган матн битларининг узлуксиз окими ўрнатилиши мумкин. Бу эса частота

кийматларини ва уланишнинг давомлигини беркитишга имкон беради. Бундай ёндашишда тармокнинг самарали ўтказиш қобилияти пасаймайди, чунки ҳеч қандай қўшимча ахборот талаб этилмайди. Аммо, узел очилса бу узел орқали ўтувчи хабарларнинг бутун оқими таҳлиллаш мавзуга айланади.

Ҳимоялашнинг чеккалараро усулларидан фойдаланилганда узатилувчи хабарларнинг ҳақиқий частотаси ва узунлигини беркитиш учун турли узунликдаги «бўш» хабарлар генерацияланиши, ҳақиқий хабар эса бўш символлар билан тўлдирилиши мумкин. Қабул қилувчи. бегона кенгайишларни ва «бўш» хабарларни аниқлашда хабардаги шифрланган хошиядан фойдаланиши мумкин.

Аксарият иловаларда оқимни таҳлиллаш орқали ахборотни чиқариб олиш иккинчи даражали хавф сифатида талкин қилиниши ва махсус қарши чоралар қўрилмаслиги мумкин.

Хабарлар сатҳида ҳақиқийликни тасдиқлаш хабарларни кечиктириш, уларни йўқ қилиш, алмаштириб қўйиш ёки қайталаш каби таъсирлардан ҳимоялашни таъминламайди. Шунга қарамадан, бундай таҳдидлардан ҳимоялашнинг турли усуллари мавжуд:

– хабарларни рақамлаш. Ҳар бир хабарни рақамлаб, рақамни хабар таркибига киритиб, демак, шифрлаб узатиш орқали хабарнинг ҳақиқийлигига ишонч ҳосил қилиш мумкин. Тармокнинг ҳар бир объекти у билан алоқада бўлувчи объектларнинг ҳар бири учун алоҳида санагичларга (счётчикларга) эга бўлиши лозимлиги бу муолажанинг камчилиги ҳисобланади.

– вақтни белгилаш. Қабул қилувчи ҳар бир узатилган хабарнинг куни ва вақтини билган ҳолда унинг адекватлигини текшириши мумкин. Бундай белгилашнинг интервали ва аниқлиги шундай танланиши лозимки, бир томондан хатоли хабарлар, иккинчи томондан узатиш каналига хос бўлган табиий кечикиш аниқланиши мумкин бўлсин.

– тасодифий сонлардан фойдаланиш. Вақтнинг реал масштабида икки томонлама алоқа ишлатилганида қабул қилувчи жўнатувчига хабар жўнатилмадан олдин тасодифий сон юборади. Жўнатувчи бу сонни шифрланган хабарга шундай ўрнатадики, қабул қилувчи уни текшириши мумкин бўлсин. Шу тарзда ёлгон хабарлар чиқариб ташланиши мумкин.

– ҳар бир уланиш учун алоҳида калитдан фойдаланиш. Натижада, олинган хабарда уланишнинг ошкор бўлмаган идентификацияланиши амалга оширилади.

Хабарлар оқими узилишини аниқлаш масаласини «сўров-жавоб» протоколидан фойдаланиб ҳал этиш мумкин. Бундай протоколнинг таркибида уланишнинг вақтинчалик яхлитлигини ва мақомини ўрнатувчи хабарлар жуфтани алмашиш муолажаси бўлади. Уланишнинг ҳар бир чеккасида «хабар-сўров» узатишни вақти-вақти билан ишга туширувчи таймер ишлатилади ва «хабар-сўров» узатишга уланишнинг бошқа чеккасида жавоб олинади. Ҳар бир «хабар-сўров»да передатчик ахбороти мавжуд бўлиб, бу ахборот уланишдаги хабар йўқотилишини аниқлашга имкон беради.

Ёлгон уланишни аниқлаш учун ҳар бир чеккадаги «уланишга жавобгар»нинг ҳақиқийлигини ва уланишнинг вақтинчалик яхлитлигини текширишга ишончли асосни таъминловчи қарши чоралар ишлаб чиқилган.

Уланиш бошланиши вақтида ҳар бир чеккада уланишга жавобгарнинг ҳақиқийлигини текшириш кейинги хабарлар оқимининг ҳақиқийлиги ҳусусида қарор қабул қилишга асос ҳисобланади.

Уланишнинг вақтинчалик яхлитлигини текшириш бузгунчининг олдинги қонуний уланиш ёзувидан фойдаланиб, фойдаланувчини хато фикрга солишидан ёки адаштиришидан, маълумотлар узатиш жараёнини бузишидан ҳимоялайди.

11.1. Симсиз тармоқ концепцияси ва тузилмаси

Симсиз тармоқ концепцияси. Симсиз тармоқлар одамларга симли уланишсиз ўзаро боғланишларига имкон беради. Бу силжиш эркинлигини ва уй, шаҳар қисмларидаги ёки дунёнинг олис бурчакларидаги иловалардан фойдаланиш имконини таъминлайди. Симсиз тармоқлар одамларга ўзларига қулай ва хоҳлаган жойларида электрон почтани олишларига ёки Web-саҳифаларни кўздан кечиришларига имкон беради.

Симсиз тармоқларнинг турли хиллари мавжуд, аммо уларнинг энг муҳим хусусияти боғланишнинг компьютер қурилмалари орасида амалга оширилишидир. Компьютер қурилмаларига шахсий рақамли ёрдамчилар (Personal digital assistance, PDA), ноутбуклар, шахсий компьютерлар, серверлар ва принтерлар тааллуқли. Одатда, уяли телефонларни компьютер қурилмалари каторига киритишмайди, аммо энг янги телефонлар ва ҳатто наушниклар маълум ҳисоблаш имкониятларига ва тармоқ адаптерларига эга. Яқин орада электрон қурилмаларнинг аксарияти симсиз тармоқларга уланиш имкониятини таъминлайди.

Боғланиш таъминланадиган физик ҳудуд ўлчамларига боғлиқ ҳолда симсиз тармоқларнинг қуйидаги категориялари фаркланади:

- симсиз шахсий тармоқ (Wireless personal-area network, PAN);
- симсиз локал тармоқ (Wireless local-area network, LAN);
- симсиз регионал тармоқ (Wireless metropolitan-area network, MAN);
- симсиз глобал тармоқ (Wireless Wide-area network, WAN).

Жадвалда Ушбу тармоқларнинг қисқача тавсифи келтирилган.

Симсиз шахсий тармоқлари узатишнинг катта бўлмаган масофаси билан (17 метргача) ажралиб туради ва катта бўлмаган бинода ишлатилади. Бундай тармоқларнинг характеристикалари ўртача бўлиб, узатиш тезлиги одатда 2Мб/с дан ошмайди.

Бундай тармок, масалан, фойдаланувчи PDA сида ва унинг шахсий компютерида ёки ноутбукида маълумотларни симсиз синхронлашни таъминлаши мумкин. Худди шу тарика принтер билан симсиз уланиш таъминланади. Компютерни ташки курилмалар билан уловчи симлар чигалликларининг йўқолиши етарлича жиддий афзаллик бўлиб, бунинг эвазига ташки курилмаларнинг бошланғич ўрнатилиши ва кейинги, зарурият туғилганда, жойининг ўзгартирилиши анчагина осонлашади.

Жадвал

Тармок хили	Таъсир доираси	Характеристикаси	Стандартлар	Қўлланиш соҳаси
Шахсий симсиз тармоқлар	Фойдаланувчидан бевосита яқинликда	ўртача	Bluetooth, IEEE. 802.15, IRDA	Ташки курилмалар кабелларининг ўрнида
Локал симсиз тармоқлар	Биолар ва кампуслар доирасида	юқори	IEEE 802.15, Wi-Fi, HyperLAN	Симли тармоқларни Мобил кенгайтириш
Регионал симсиз тармоқлар	Шаҳар доирасида	юқори	Патентли, IEEE 802.16, WIMAX	Биолар ва корхоналар ва Internet орасида белгиланган симсиз боғланиш
Глобал симсиз тармоқлар	Бутун дунё бўйича	паст	CDPD ва 2, 2.5 ва 3-авлод уяли телефон орқали тизимлар	Биодан ташқарида Internetдан мобил фойдаланиш

Симсиз шахсий тармоқларнинг аксарият узатувчи-кабул килувчиларнинг (transceiver) кам қувват исътемољ килиши ва ихчамлиги микропроцессорлар билан таъминланган, катта бўлмаган фойдаланувчи курилмаларини самарали мададлашга ҳамда ком-

пьютер курилмасини узок вақт мобайнида битта батареяда (ёки аккумуляторда) ишлашига имкон беради. Ундан ташқари, кам қувват истеъмол қилиниши симсиз шахсий тармоқларни уяли телефонларга, PDA ларга ва наушникларга татбиқ этишга сабаб бўлди.

Симсиз шахсий тармоқлар Internet га ва иловаларга уланишдан биргаликда фойдаланиш мақсадида ноутбуклар ва шахсий компьютерларнинг ўзаро алоқасини таъминлаши мумкин. Бу таъсир доираси битта хона билан чегараланган тармоқларга тўғри келади.

Симсиз локал тармоқлар офисларнинг ичида ва ташқарисида, ишлаб чиқариш биноларида узатишларнинг юқори характеристикаларини таъминлайди. Бундай тармоқлардан фойдаланувчилар одатда, ноутбукларни, шахсий компьютерларни ва катта ресурсларни талаб этувчи иловаларни бажаришга кодир процессорли ва катта экранли PDA ларни ишлатишади. Хизматчи тармоқ хизматларидан мажлислар залида ёки бинонинг бошқа хоналарида бўла туриб фойдаланиши мумкин. Бу хизматчига ўз вазифаларини самарали бажаришга имкон беради. Симсиз локал тармоқлар узатишнинг 54Мбит/сгача тезлигида барча офис ёки маиший иловалар талабларини қондириш имконига эга. Характеристикалари, компонентлари, нархи ва бажарадиган амаллари бўйича бундай тармоқлар Ethernet хилидаги анъанавий симли локал тармоқларига ўхшаш.

Симсиз регионал тармоқлар юзаси бўйича шаҳарга тенг бўлган ҳудудга хизмат қилади. Аксарият ҳолларда иловаларни бажаришда белгиланган уланиш талаб этилади, баъзида эса мобиллик зарур бўлади. Масалан, касалхонада бундай тармоқ асосий бино ва масофадаги клиникалар орасида маълумотларни узатишни таъминлайди. Ёки энергетик компания бундай тармоқдан шаҳар масштабида фойдаланиб, турли туманлардан бериладиган иш нарядларидан фойдаланишини таъминлайди. Натижада, симсиз регионал тармоқлар мавжуд тармоқ инфратузилмаларини бир ерга тўплайди ёки мобил фойдаланувчиларга мавжуд тармоқ инфратузилмалари билан уланишни ўрнатишга имкон беради.

Симсиз Internet хизматлари билан таъминловчилар (Wireless Internet Service Provider, WISP) уйда фойдаланувчилар ва компаниялар учун доимий симсиз уланишларни таъминлаш мақсадида шаҳарларда ва қишлоқ жойларда симсиз регионал тармоқларни мижозлар ихтиёрига тақдим этади. Бундай тармоқлар, кўпинча

симли уланишларни ётқизиш билан боғлиқ чегараланишларга эга бўлган оддий симли уланишларга нисбатан самарали ҳисобланади.

Симсиз регионал тармоқларнинг характеристикалари турлича. Уланишларда инфрақизил технологиянинг ишлатилиши маълумотларни узатиш тезлигининг 100 Гбит/с ва ундан катта бўлишини таъминлайди.

Симсиз глобал тармоқлар мобил иловаларнинг, улардан мамлакат ёки хатто континент масштабида фойдаланишни таъминлаш билан ишланишини таъминлайди. Иқтисодий мулоҳазаларга таянган ҳолда, телекоммуникация компаниялари кўпгина фойдаланувчилар учун узок масофадан уланишни таъминловчи симсиз глобал тармоқнинг нисбатан қиммат инфратузилмасини яратадилар. Бундай ечимнинг харажати барча фойдаланувчилар ўртасида тақсимланади, натижада, абонент тўлови унчалик юкори бўлмайди.

Кўпгина телекоммуникация компанияларининг кооперацияси туфайли симсиз глобал тармоқларининг таъсир доираси чегараланмаган. Телекоммуникация хизматини таъминловчиларнинг бирига тўлаб, симсиз глобал тармоқ орқали дунёнинг ҳар қандай нуқтасидан қатор Internet хизматидан фойдаланиш мумкин.

Симсиз глобал тармоқ характеристикалари нисбатан юкори эмас, маълумотларни узатишнинг тезлиги 56 Кбит/с ни, баъзида 170 Кбит/с ни ташкил этади.

Симсиз глобал тармоқларга хос иловалар Internet дан фойдаланишни, электрон почта хабарларини узатиш ва қабул қилишни, фойдаланувчи уйдан ёки офисдан ташқарида бўлганида корпоратив иловалардан фойдаланишни таъминловчи иловалардир. Абонентлар, масалан, таксида кетаётганларида ёки шаҳар бўйича сайр қилаётганларида уланишни ўрнатишлари мумкин. Умуман, симсиз глобал тармоқдан фойдаланувчилар ҳудудий чегараланмаганлар.

Симсиз глобал тармоқлар технологиясини татбиқ этишдаги муаммолардан бири унинг бино ичидаги фойдаланувчилар учун боғланишни таъминлай олмаслиги. Чунки бундай тармоқ инфратузилмалари бино ташқарисида жойлашган ва радиосигналлар бинода айтарлича сусаяди. симсиз глобал тармоқларни бино ичига ўрнатилиши эса қимматга тушади ва техник нуқтаи назаридан асосланмаган.

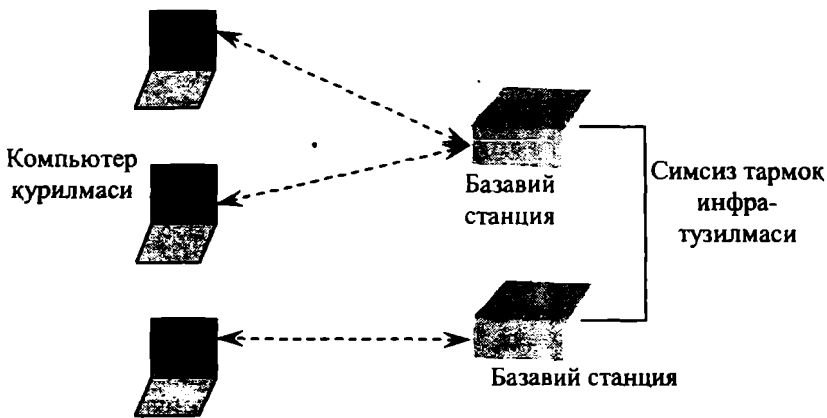
Симсиз шахсий, локал, регионал ва глобал тармоқлар бир-бирини тўлдирувчи бўлиб, турли талабларни қондиради. Аммо, баъзида бир тармоқни иккинчисидан фарқлаб бўлмайди. Масалан,

бино ичидаги симсиз локал тармоқ фойдаланувчи PDAси билан шахсий компьютерини симсиз шахсий тармоқ каби улашни таъминлаши мумкин. Турли симсиз тармоқлар орасидаги фарқни аниқлашда уларда ишлатиладиган технологиялар ва стандартлардан фойдаланишдади (жадвалга каралсин).

Агар фойдаланувчи нуктаи назаридан истиқбол хусусида сўз юритилса, симсиз тармоқлар орасида чегаранинг йўқолиши шарт. Турли хил симсиз тармоқ ишини мададловчи компьютер қурилмалари тармоғи интерфейсининг платалари пайдо бўлмоқда. Масалан, сайёҳда ёки тижоратчида ҳам симсиз локал ҳам симсиз глобал тармоқ билан ўзаро алоқа қилувчи замонавий уяли телефон бўлиши мумкин.

Симсиз тармоқ тузилмаси. Симсиз тармоқларда симли тармоқда ишлатиладиган компонентлар ишлатилади. Аммо, симсиз тармоқларда ахборот ҳаво муҳити (medium) орқали узатишга яроқли кўринишга ўзгартирилиши лозим.

11.1-расмда симсиз тармоқларда ишлатиладиган компонентларнинг асосийлари кўрсатилган. Уларга фойдаланувчилар, компьютер қурилмалари, базавий станциялар ва симсиз инфратузилма киради.



11.1-расм. Симсиз тармоқда ишлатиладиган асосий компонентлар.

Фойдаланувчилар. Симсиз тармоқ фойдаланувчига хизмат қилишлиги сабабали, фойдаланувчига симсиз тармоқнинг муҳим қисми сифатида қараш мумкин. Фойдаланувчи симсиз тармоқдан фойдаланиш жараёнини бошлайди ва унинг ўзи тугаллайди. Шу сабабли унга «охирги фойдаланувчи» атамаси жоиз ҳисобланади. Одатда, фойдаланувчи симсиз тармоқ билан ўзаро алоқани таъминлаш билан бир қаторда, муайян иловалар билан боғлиқ бошқа вазифаларни бажарувчи *компьютер қурилмалари (computer device)* билан иш кўради.

Мобиллик – симсиз тармоқнинг энг сезиларли афзалликларидан биридир. Масалан, мобиллик хусусиятидан қандайдир бино бўйича ҳаракатланувчи ва ўзининг PDAси ёрдамида электрон почтани олувчи ёки жўнатувчи одам фойдаланади. Бу ҳолда PDA симсиз тармоқ инфрагузилмасига узлуксиз ёки тез-тез тикланувчи ула-нишни таъминлаши лозим.

Баъзи фойдаланувчиларга фақат компьютер қурилмасининг портативлиги зарур, яъни улар вақтнинг маълум оралиғида симсиз тармоқ билан ишлаганида бир жойда бўладилар. Бундай фойдаланишга мисол тарикасида мажлислар залида симсиз тармоққа уланган ноутбукда ишловчи ходимни кўрсатиш мумкин.

Компьютер қурилмалари. Компьютер қурилмаларининг (баъзида уларни мижозлар деб аташади) кўпгина хиллари симсиз тармоқ билан ишлайолади. Баъзи компьютер қурилмалари фойдаланувчилар учун атайин қурилган бўлса, бошқалари охирги тизим ҳисобланади. 11.2-расмда симсиз тармоқларнинг компьютер қурилмалари келтирилган.



Принтер



Мобил телефон



Ноутбук



Маълумотлар
ни йиғувчи
қурилма



Шахсий
компьютер



PDA



Оддий телефон

11.2-расм. Симсиз тармоқларнинг компьютер қурилмалари.

Мобил иловалар ишини таъминлаш ва одамларга ўзлари билан узок вақт мобайнида олиб юришларида қулайлик туғдириш учун компьютер қурилмалари ихчам бўлиши лозим. Одатда, улар катта бўлмаган экранга, кам сонли тугмачаларга ва ўлчамлари кичик батареяга эга. Компьютер қурилмалари мобилликка эга бўлга ҳолда фақат баъзи иловаларни мададлайди. Нисбатан юқори характеристикаларни талаб этувчи иловаларни бажаришда катта экранга ва катта клавиатурага эга бўлган ўлчамлари катта компьютер қурилмаларидан фойдаланилади. Аммо улар массасининг катталиги ва бир жойдан иккинчи жойга кўчиришнинг ноқулайлиги муаммо ҳисобланади. Симсиз тармоқларнинг компьютер қурилмалари серверлар, маълумотлар базаси ва Web-узеллар каби охириги тизимларни ҳам ўз ичига олади.

Фойдаланувчилар мавжуд компьютер қурилмаларини симсиз тармоқда ишлатиш учун (масалан, симсиз тармоқ интерфейси платасини ноутбукка ўрнатиш орқали) мослаштиришлари мумкин. *Тармоқ интерфейси платаси ёки тармоқ адаптери* (network interface card) компьютер қурилмаси ва симсиз тармоқ инфратузилмаси орасида интерфейсни таъминлайди. Бу плата компьютер қурилмаси ичига ўрнатилади, баъзида ташқи тармоқ адаптери ҳам ишлатилади. Бундай адаптерлар, ишга туширилиши билан компьютер қурилмаси ташқарисида қолади.

Компьютер қурилмалари Windows-XP, Linux ёки MAC OS каби операцион тизимга ҳам эга бўлиб, бу операцион тизим симсиз тармоқ иловаларини амалга ошириш учун зарур бўлган дастурий таъминотни ишга туширади.

Ҳаво муҳити. Ҳаво компьютер қурилмалари ва симсиз инфратузилмага орасида ахборот оқимини узатиш канали ҳисобланади. Симсиз тармоқлар орқали алоқани нутк орқали мулоқотга ўхшатиш мумкин. Агар суҳбатдошлар орасидаги масофа ошаверса, улар бир-бирларини ёмон эшита бошлайдилар.

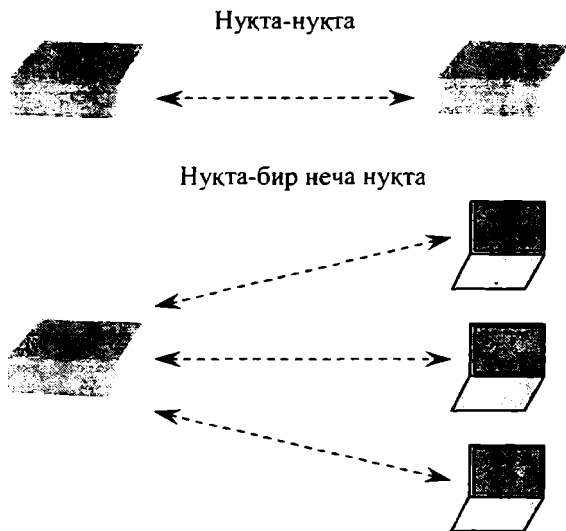
Симсиз тармоқларнинг ахборот сигналлари ҳам ҳаво орқали тарқалади, аммо ўзининг хусусияти эвазига нутк сигналарига караганда анчагина катта масофага тарқалиши мумкин. Бу сигналлар одамга эшитилмайди, шу сабабли уларни, сўзлашга ҳалақит беришидан қўрқмай, янада юқори сатҳларгача кучайтириш мумкин. Аммо алоқа сифати тўсиқларнинг мавжудлигига боғлиқ. Тўсиқлар сигналлар тарқалишига ҳалақит қилади ёки уларни сусайтиради, натижада сигналлар сатҳи пасаяди, уларнинг тарқалиш узоклиги камаяди.

Ёмғир, қор, туман, тутун (смог) симсиз тармоқларда ахборот сигналларини тарқалишига таъсир этувчи об-ҳаво шароитлари ҳисобланади. Масалан, кучли жала алоқа узунлигини икки мартага камайитириши мумкин. Бинолар ва дарахтлар каби бошқа тўсиқлар

тарқалиш шароитларига ва симсиз тармоқ характеристикаларига таъсир этиши мумкин. Симсиз регионал ва глобал тармоқларни жойлаштиришни режалаштиришда бу муаммоларнинг муҳимлиги ортади.

Симсиз тармоқ инфратузилмаси. Симсиз тармоқ инфратузилмаси фойдаланувчилар ва охириги тизимларнинг ўзаро симсиз алоқаларини таъминлайди. Уни базавий станциялар, фойдаланиш контроллерлари, уланиш ўрнатилишини таъминловчи иловаларнинг дастурий таъминоти ва тақсимловчи тизим ташкил этиши мумкин.

Базавий станция инфратузилманинг тарқалган компоненти ҳисобланади. У ҳаво мухити орқали тарқалувчи симсиз тармоқ аҳборот сигналларининг симли тармоққа узатилишини таъминлайди. Базавий станцияни баъзида *тақсимловчи тизим* деб ҳам юритишдади. Демак, базавий станция Web-саҳифаларни кўздан кечириш сервислари, электрон почта ва маълумотлар базаси каби тармоқ хизмати йўналишидан фойдаланишни таъминлайди. Базавий станцияда кўпинча симсиз тармоқ интерфейси платаси бўлиб, бу плата фойдаланувчи компютеридаги симсиз тармоқ интерфейси платасининг ишлаш принциpidан фойдаланади. Базавий станция «нукта-нукта» ёки «нукта-бир неча нукта» каби уланишларни мададлаши мумкин (11.3-расм).



11.3-расм. Базавий станциянинг «нукта-нукта» ва «нукта-бир неча нукта» уланишларини мададлаши.

«Нукта-нукта» тизими сигналлар оқимини бир базавий станциядан иккинчисига ёки бир компьютердан иккинчисига узатиш имкониятига эга. «Нукта-бир неча нукта» конфигурацияси ҳолида базавий станция биттадан ортик компьютер қурилмаси ёки бир неча базавий станциялар билан боғланиши мумкин. Бундай хил боғланишни, масалан, симсиз локал тармоқ таркибидаги фойдаланиш нуктаси таъминлайди. Фойдаланиш нуктаси битта қурилма бўлиб, кўпгина компьютер қурилмалари бир-бирлари билан ҳамда симсиз тармоқ инфратузилмасидаги тизимлар билан боғланиш мақсадида у билан уланишни ўрнатади.

Фойдаланиш контроллери. Фойдаланиш контроллерлари, одатда, тармоқнинг ўтказувчи қисмида, фойдаланиш нуктаси ва тармоқнинг химояланиш қисми орасида жойлашган аппарат узели ҳисобланади. Фойдаланиш контроллерлари очик симсиз тармоқ ва муҳим ресурслар орасида трафикни тартибга солиш мақсадида фойдаланиш нукталарини марказлаштирилган назоратини таъминлайди. Баъзи ҳолларда фойдаланишни бошқариш вазифасини фойдаланиш нуктаси бажаради.

Фойдаланиш контроллерлари кенг қўлланилади. Умумфойдаланувчи симсиз локал тармоқда, фойдаланиш контроллери фойдаланувчиларни аутентификациялаш ва авторизациялаш билан Internetдан фойдаланишни тартибга солади.

Уланиш ўрнатилишини таъминловчи иловаларнинг дастурий таъминоти. Internet дан ва электрон почтадан симсиз тармоқ орқали, одатда, осон фойдаланилади. Бунинг учун *мижоз қурилмасида* браузер ва электрон почта дастури ўрнатилиши лозим. Фойдаланувчилар вақти-вақти билан симсиз уланишдан маҳрум бўлишлари мумкин, аммо нисбатан мураккаб бўлмаган иловаларни бажаришда ишлатилувчи протоколлар етарлича барқарор ҳисобланади.

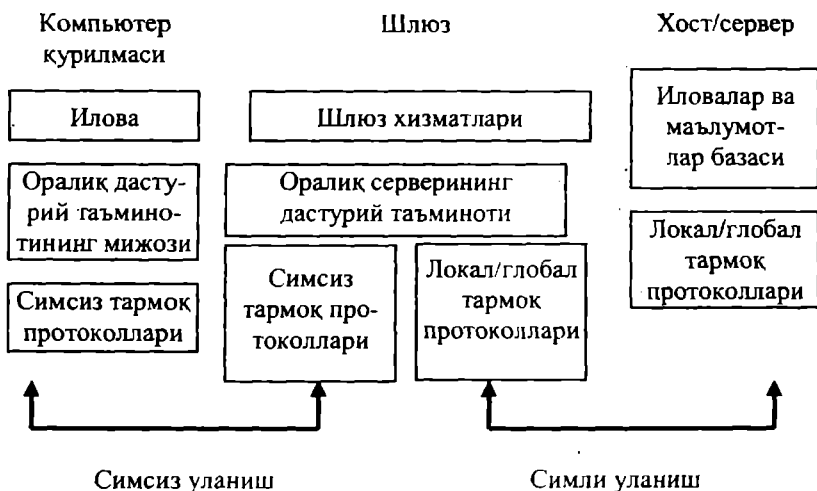
Аммо, бундай оддий иловалар билан бир қаторда махсус, янада мураккаб иловалар ишлашини таъминловчи дастурий таъминот зарур. Қуйида уланишни таъминловчи иловаларнинг асосийлари келтирилган.

Терминал эмулятори (terminal emulation). Терминал эмуляторининг дастурий таъминоти компьютер қурилмасида бажарилиб, уни фойдаланувчини нисбатан содда интерфейс билан таъминлашга имкон берувчи терминал каби ишлашга мажбур этади. Бу содда

интерфейс фойдаланувчига бошқа компьютерда бажарилувчи иловалар билан ўзаро алоқа қилишга имкон беради.

Маълумотлар базаси билан тўғридан-тўғри уланиш (direct database connectivity). Маълумотлар базаси билан тўғридан-тўғри уланишда (баъзида мижоз-сервер технологияси деб аталади) илова фойдаланувчи компьютерида бажарилади. Бундай конфигурацияда охириги фойдаланувчи қурилмасидаги дастурий таъминот иловлага юкланган барча вазифаларни бажаради ва, одатда, марказий серверда жойлашган маълумотлар базаси билан ўзаро алоқада бўлади.

Оралик дастурий таъминот (Wireless middleware). Оралик дастурий таъминот фойдаланувчининг компьютер қурилмаси ва илова дастурий таъминоти ёки сервердаги маълумотлар базаси орасида оралик уланишни амалга оширади (11.4-расм).



11.4-расм. Оралик дастурий таъминоти.

Оралик дастур симли тармоққа уланган қўшимча компьютерда (оралик шлюзида) бажарилади. У фойдаланувчининг компьютер қурилмаси ва серверлар орасида айланувчи пакетларни ишлайди. Бу дастурий таъминот симсиз тармоқда самарали ва ишончли боғланишни яратишга имкон беради, чунки маълумотлар базасига уланиш ва иловаларнинг дастурий таъминоти билан ўзаро алоқа

янада ишончли симли тармоқ орқали амалга оширилади. Баъзида бу технологияни чидамли боғланиш (session persistence) деб аташади.

Тақсимланган тизим. Симсиз тармоқ камдан-кам тўла маънода симсиз ишлатилади. Таркибида кўпинча симли уланишлар бўлган тақсимловчи тизим одатда фойдаланиш нукталарини, фойдаланиш контроллерларини ва серверларни бир бутунга бирлаштириш учун зарур бўлади. Аксарият ҳолларда тақсимловчи вазифасини оддий Internet тармоғи бажаради.

11.2. Симсиз тармоқлар хавфсизлигига таҳдидлар

Симсиз технологиядан фойдаланилиб жуда катта афзалликларга эришиш мумкин. Бу технология фойдаланувчиларга алоқани йўқотмасдан бемалол ҳаракатланиш ҳиссиётини берса, тармоқ яратувчиларига боғланишларни ташкил этиш учун катта имкониятларни яратади. Ундан ташқари, тармоқдан фойдаланиш учун кўпгина янги қурилмаларнинг пайдо бўлишига имкон беради. Аммо симсиз технология оддий симли тармоқларга караганда ўзида кўпроқ таҳдидларни элтади. Хавфсиз симсиз иловани яратиш учун симсиз «хужумлар» ўтувчи бўлиши мумкин бўлган барча йўналишларни аниқлаш лозим. Афсуски, иловалар ҳеч қачон бутунлай хавфсиз бўлмайди, аммо симсиз технологиялардаги хавфхатарни синчиклаб ўрганиш ҳар ҳолда ҳимояланиш даражасини ошишига ёрдам беради. Демак, мумкин бўлган таҳдидларни таҳлиллаб, тармоқни шундай қуриш лозимки, хужумларга ҳалакит бериш ва ностандарт «хужумлар»дан ҳимояланишга тайёр туриш имкони бўлсин.

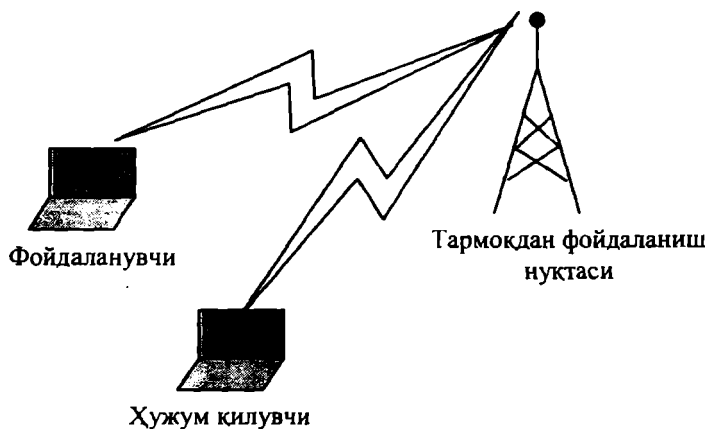
Назоратланмайдиган ҳудуд. Симли ва симсиз тармоқлар орасидаги асосий фарқ тармоқ четки нукталари орасидаги мутлако назоратланмайдиган зона билан боғлиқ. Уяли тармоқларнинг етарлича кенг маконида симсиз муҳит асло назоратланмайди. Замонавий симсиз технологиялар тармоқ маконини бошқариш воситаларининг чегараланган тўпламини тақдим этади. Бу симсиз тузилмаларнинг яқинидаги хужум қилувчиларга симли дунёда мумкин бўлмаган хужумларни амалга оширишга имкон беради.

Яширинча эшитиш. Симсиз тармоқлар каби очик ва бошқарилмайдиган муҳитда энг тарқалган муаммо – аноним хужумларнинг мумкинлиги. Аноним зарарқундалар 11.5-расмда

кўрсатилганидек радиосигналларни ушлаб қолиб, узатилувчи маълумотларни расшифровка қилиши мумкин.

Узатишни ушлаб қолиш учун нияти бузук одам узатгич (передатчик) олдида бўлиши лозим. Ушлаб қолишнинг бундай турларини умуман қайдлаш мумкин эмас ва уларга халакит бериш ундан ҳам қийин. Антенналар ва кучайтиргичлардан фойдаланиш, ушлаб қолиш жараёнида нияти бузук одамларга нишондан айтарлича узок масофада бўлишларига имкон беради.

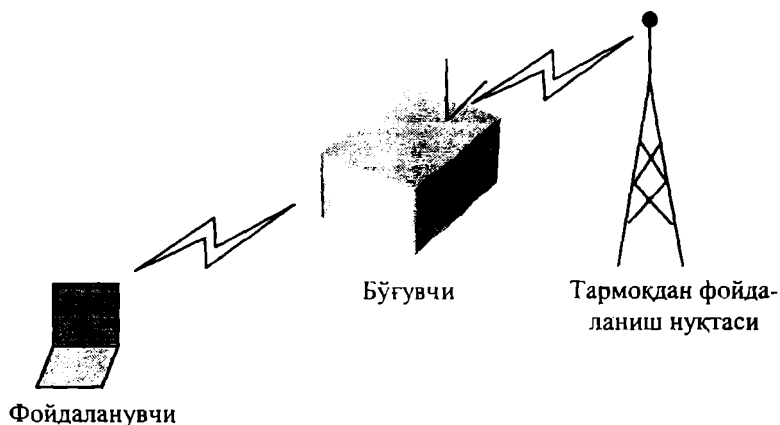
Яширинча эшитишнинг яна бир усули – симсиз тармоққа ула- ниш. Локал симсиз тармоқда яширинча фаол эшитиш одатда *Address Resolution Protocol (ARP)* протоколидан нотўғри фойдаланишга асосланган. Бошида бу технология тармоқни «эшитиш» мақсадида яратилган эди. Аслида, биз маълумотлар боғланиши сатҳида «man in the middle» (MITM – «ўртада одам», пастрокка қаралсин) хили- даги ҳужум билан иш кўраимиз. Ҳужум қилувчи локал симсиз тармоқнинг нишон станциясига сўралмаган ARP-жавобларни юбо- ради, нишон станцияси эса ҳужум қилувчига ўзидан ўтаётган барча трафикни жўнатади. Сўнгра нияти бузук одам пакетларни кўрсатилган манзилларга йўллайди. Шундай қилиб, симсиз станция бошқа симсиз мижознинг (ёки локал тармоқдаги симли мижознинг) трафигини ушлаб қолиши мумкин.



11.5-расм. Симсиз коммуникацияларда яширинча эшитиш.

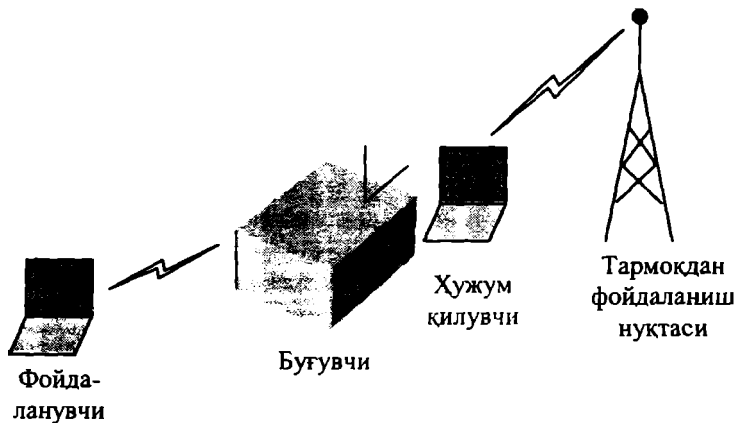
Бўғиш. Тармоқларда бўғиш атайин ёки атайин бўлмаган интерференциянинг алоқа каналидаги жўнатувчи ва қабул қилувчи имкониятидан ошганида содир бўлади. Натижада, бу канал ишдан чиқарилади. Хужум қилувчи бўғишнинг турли усулларидан фойдаланиши мумкин.

Хизмат кўрсатишдан воз кечиш. DoS (Denial of Service – хизмат кўрсатишдан воз кечиш) ҳилидаги хужум тармоқни бутунлай ишдан чиқариши мумкин. Бутун тармоқда, жумладан базавий станцияларда ва миждоз терминалларида, шундай кучли интерференция пайдо бўладики, станциялар бир-бирлари билан боғлана олмайдилар (11.6-расм). Бу хужум маълум доирадаги барча коммуникацияни ўчиради. Симсиз тармоққа бўладиган DoS хужумни олдини олиш ёки тўхтатиш қийин. Симсиз тармоқ технологияларининг аксарияти лицензияланмаган частоталардан фойдаланади, демак, бир канча электрон қурилмалардан интерференция бўлиши мумкин.



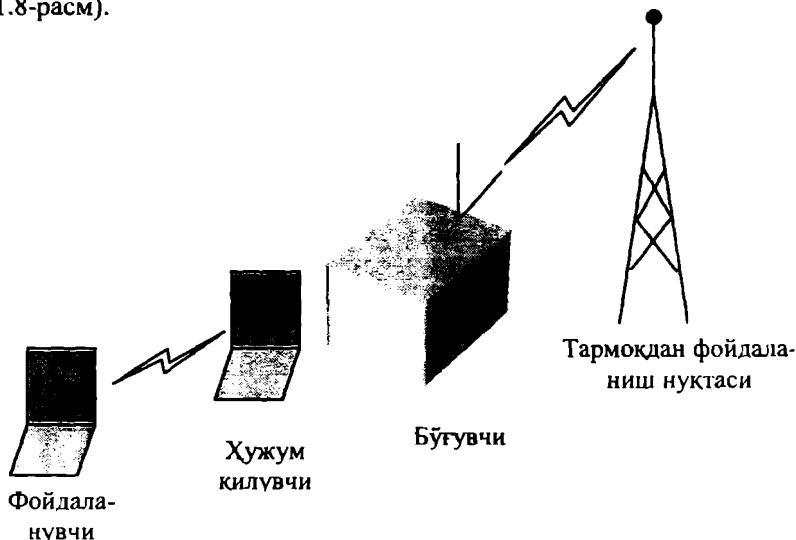
11.6-расм. Симсиз коммуникацияларда бўғиш хужумлари.

Миждозларни бўғиш. Миждоз станциясини бўғиш фирибгарга ўзини бўғилган миждоз ўрнига кўйишига имкон беради (11.7-расм). Миждоз уланишни амалга ошира олмасин деган мақсадда унга хизмат кўрсатишдан воз кечиш учун ҳам бўғишдан фойдаланилади. Жуда моҳирлик билан қилинган хужумлар нияти бузуқ одам станциясини базавий станцияга улаш мақсадида мавжуд уланишни узди.



11.7-расм. Уланишни ушлаб қолиш мақсадида мижозни бўғиш хужуми.

Базавий станцияни бўғиш. Базавий станцияни бўғиш уни хужум килувчи станция билан алмаштиришга имкон беради (11.8-расм).



11.8-расм. Уланишни ушлаб қолиш мақсадида базавий станцияни бўғиш хужуми.

Бундай бўғиш фойдаланувчиларни хизматлардан фойдаланишдан, телекоммуникация компанияларини эса фойдадан маҳрум қилади.

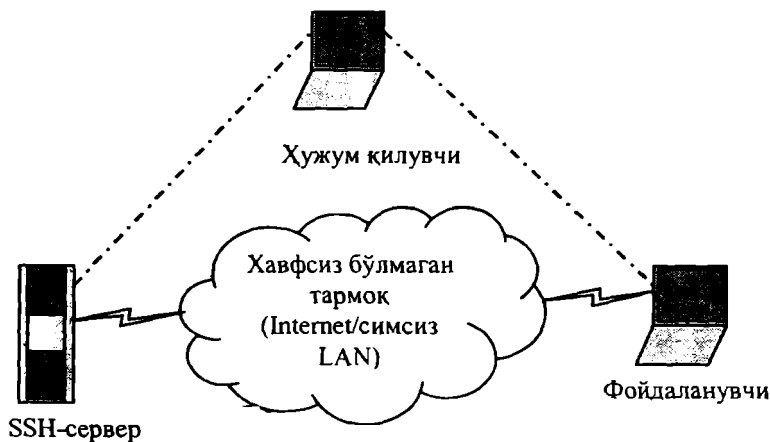
Юқорида кайд этилганидек, аксарият симсиз технологиялар лицензияланмаган частоталардан фойдаланади. Шу сабабли кўпгина қурилмалар – радиотелефонлар, кузатиш тизимлари ва микротўлқинли ўчоқлар – симсиз тармоқ ишига таъсир этиши ва симсиз уланишни бўғиши мумкин. Бундай атайин бўлмаган бўғиш ҳолларини олдини олиш учун, қимматбаҳо симсиз асбоб-ускунани сотиб олишдан аввал у ўрнатиладиган жойни синчиклаб таҳлиллаш лозим. Бундай таҳлил коммуникацияларга бегона қурилмаларнинг таъсир этмаслигига ишонч ҳосил қилишга имкон беради ва маъносиз харажатлардан асрайди.

Бостириб кириш ва маълумотларни модификациялаш. Нияти бузуқ одам уланишни ушлаб қолиш, маълумотларни ёки командаларни узатиш мақсадида маълумотларнинг мавжуд оқимида ахборотни кўшганида бостириб кириш содир бўлади. Хужум қилувчи пакетларни базавий станцияга юбориб бошқариш командалари ва ахборот оқимлари устида манипуляцияни амалга ошириши мумкин. Бошқариш командаларини керакли бошқариш каналига юбориш орқали фойдаланувчини тармоқдан узишга эришиш мумкин.

Бостириб кириш хизмат кўрсатишдан воз кечиш учун ишлатилиши мумкин. Хужум қилувчи тармоқдан фойдаланиш нукталарини уланиш командалари билан тўлиб-тоштиради. Натижада, бошқа фойдаланувчиларга тармоқдан фойдаланишга руҳсат берилмайди.

MITM(man in the middle) хужуми. MITM хужуми юқорида тавсифланган бостириб киришларга ўхшаш. Улар турли шаклларни олишлари мумкин ва алоқа сеансининг конфиденциаллигини ва яхлитлигини бузиш учун ишлатилади. MITM хужумлар анчагина мураккаб, чунки уларни амалга ошириш учун тармоқ хусусида батафсил ахборот талаб этилади. Нияти бузуқ одам, одатда, тармоқ ресурсларидан бирининг идентификациясини бажаради. Хужум қурбони уланишни бошлаганида, фирибгар уни ушлаб қолади ва исталган ресурс билан уланишни тугаллайди, сўнгра ушбу ресурс билан барча уланишларни ўзининг станцияси орқали ўтказди (11.9-расм). Бунда хужум қилувчи ахборотни жўнатиши,

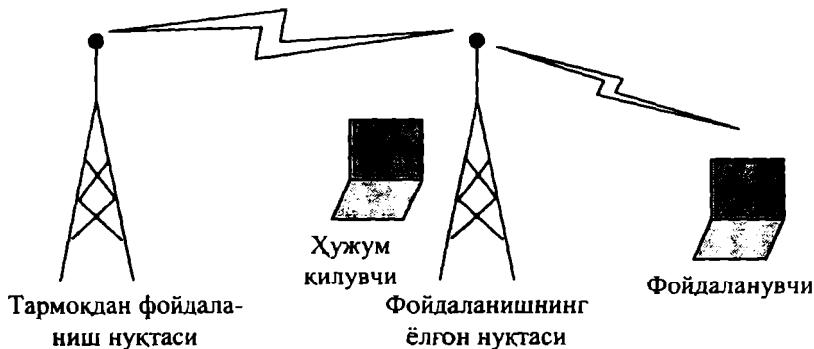
жўнатилганини ўзгартириши ёки барча музокараларни яширинча эшитиши ва сўнгра расшифровка қилиши мумкин.



11..9-расм. MITM ҳилидаги ҳужум.

Абонент-фирибгар. Тармоқ абонентининг ишини синчиклаб ўрганиб чикқан ҳужум қилувчи ўзини «тармоқ абоненти» қилиб кўрсатиб, тармоқ ва унинг хизматларидан фойдаланишга уринади. Ундан ташқари, фойдаланишда қўлланиладиган қурилманинг ўғирланиши тармоққа киришга етарли бўлади. Барча симсиз қурилмаларнинг хавфсизлигини таъминлаш осон иш эмас, чунки улар фойдаланувчиларнинг ҳаракатланишида қулайлик туғдириш мақсадида атайин кичкина қилиб яратилади.

Тармоқдан фойдаланишнинг ёлғон нукталари. Тажрибали ҳужум қилувчи тармоқ ресурсларини имитация қилиш билан фойдаланишнинг ёлғон нукталарини ташкил этиши мумкин. Абонентлар, ҳеч шубҳаланмасдан фойдаланишнинг ушбу ёлғон нуктасига мурожаат этадилар ва уни ўзининг муҳим реквизитларидан, масалан, аутентификация ахборотидан хабардор қиладилар. Ҳужумнинг бу хили тармоқдан фойдаланишнинг ҳақиқий нуктасини «бўғиш» мақсадида баъзида тўғридан-тўғри бўғиш билан биргаликда амалга оширилади (11.10-расм).



11.10-расм. Фойдаланишнинг ёлгон нуқтаси.

Симли тармоқдан фойдаланувчилар ҳам, билмасдан тармоқни хужумга очиб бериб фойдаланишнинг ёлгон нуқталарининг ўрнатилишига сабабчи бўлишлари мумкин. Баъзида фойдаланувчи, қулайликка интилиб, симсиз алоқа тақдим этувчи фойдаланишнинг симсиз нуқталарини ўрнатади, аммо хавфсизлик муаммосини ўйламайди. Бу нуқталар симли тармоққа кириш учун «орқа эшик» вазифасини бажариши мумкин, чунки улар турли хужумларга дучор бўладиган конфигурацияда ўрнатилади.

Хужумларнинг анонимлиги. Симсиз фойдаланиш хужумнинг тўлиқ анонимлигини таъминлайди. Ўрнатилган жойни аниқловчи мос тармоқ асбоб-ускунаси бўлмаса, хужум қилувчи анонимликни осонгина саклаши ва симсиз тармоқ таъсири ҳудудидаги ҳар қандай жойда беркиниши мумкин. Бундай ҳолда нияти бузук одамни тутиш қийин, ишни судга ошириш эса ундан ҳам қийин.

Таъкидлаш лозимки, аксарият фирибгарлар тармоқни, уларнинг ички ресурсларига хужум қилиш учун эмас, балки Internetдан текин аноним фойдаланиш учун ўрганадилар ва Internet химоясида бошқа тармоқларни хужумлайдилар.

«Мижоз-мижоз» хилидаги ҳужумлар. Тармокнинг барча абонентлари ҳужумланиши мумкин. Биринчи муваффақиятдан сўнг ҳужум қилувчи корпоратив ёки телекоммуникацион тармоқдан фойдаланиш ҳуқуқига эга бўлади. Аксарият тармок маъмурлари хавфсизлик режимига талабни оширишга ёки шахсий тармоқлараро экранларни (брандмауэрларни) ўрнатишга етарлича эътибор бермайдилар. Шу сабабли, симсиз тармок миждозларига муваффақиятли ҳужумлар нияти бузук одамларга фойдаланувчиларнинг исмини ва паролини очиш, демак, бошқа тармок ресурсларидан фойдаланиш имконини бериши мумкин.

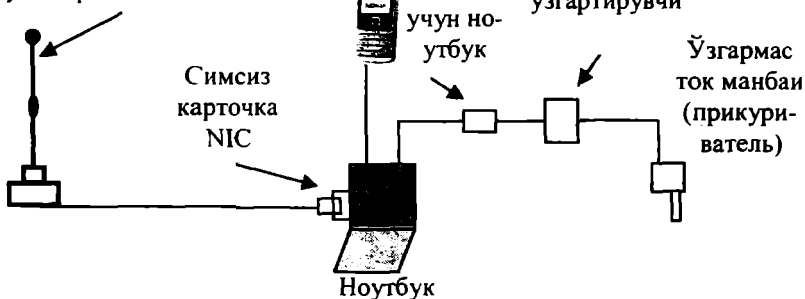
Тармок асбоб-ускуналарига ҳужумлар. Нотўғри конфигурацияланган асбоб-ускуналар ҳужум қилувчилар учун биринчи «хўрак» ҳисобланади ва тармоққа кейинги сукилиб киришга йўл очади. Ҳужумларнинг асосий объектлари – маршрутизаторлар, узиб-улагичлар, архивларни сакловчи серверлар ва фойдаланиш серверлари.

Махфий симсиз каналлар. Симсиз тармок фойдаланувчилари тармокни яратиш ёки баҳолаш жараёнида яна бир омилни ҳисобга олишлари зарур. Симсиз фойдаланиш нуктасининг нархи паст ҳамда дастурий таъминот, стандарт ноутбук ва NIC-карталар асосида фойдаланиш нуктасини яратиш етарлича осон бўлганлиги сабабли, ноқоррект конфигурацияланган ёки симли тармоқда ўйламасдан жойлаштирилган симсиз асбоб-ускунани зийраклик билан кузатиш талаб этилади. Бу асбоб-ускуна (11.11-расм) симли инфратузилмада жуда сезиларли «рахналар» ҳосил қилиши мумкин, улар тармоқдан бир неча километр узоқдаги ҳужум қилувчилар диққатини тортиши мумкин.

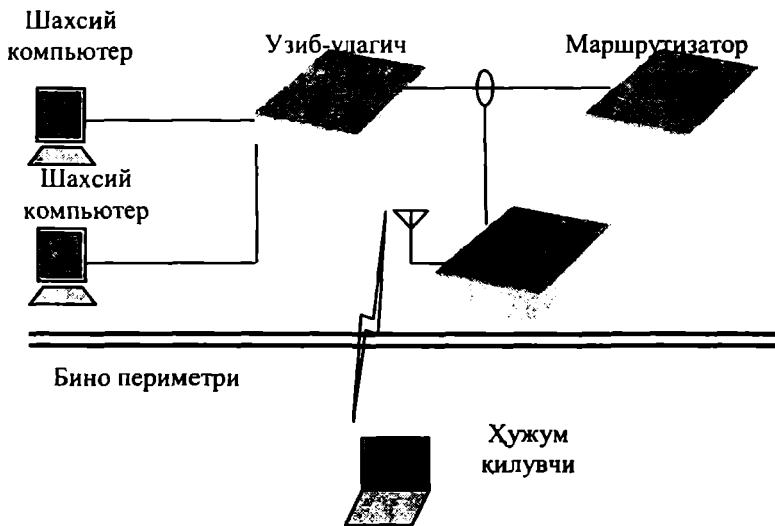
Худди шунга ўхшаш конструкция ёрдамида ўзига хос «симсиз кўприк» ўтказиш ва фойдаланиш нукталарининг бутун занжирини ташкил қилган ҳолда тармоқдан маълумотларни ҳимояланган бино ташқарисида чиқариб олиш мумкин (11.12-расм)

CDPD/GPRS имконият-
ли уяли телефон

Магнитли мададлайди-
ган 2.4ГГц частотадаги
5,5 дБ лик хар томонга
йўналтирилган антенна



11.11–расм. «Симсиз урушни» олиб бориш асбоб-ускунаси.



11.12–расм. «Орқа эшик» кўринишидаги тармоқдан фойдаланиш.

Роуминг муаммоси. Симсиз тармоқнинг симли тармоқдан яна бир муҳим фарқи фойдаланувчининг тармоқ билан алоқани узмасдан жойини ўзгартириш қобилиятидир. Роуминг концепцияси турли симсиз алоқа стандартлари CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) ва симсиз Ethernet учун бир хил. TCP/IPнинг кўпгина тармоқ иловалари сервер ва мижоз IP-манзилларининг ўзгармаслигини талаб этади, аммо тармоқдаги роуминг жараёнида абонент албатта унинг бир жойини тарк этиб, бошқа жойига кўшилади. Симсиз тармоқларда мобил IP-манзилларнинг ва бошқа роуминг механизмларининг ишлатилиши ушбу талабга асосланган.

Мобил IP-алоканинг асосий ғояси – фойдаланувчининг турган жойини қайдлаш ва трафикни қайта йўналтириш. Абонент турган жойига боғлиқ бўлмаган манзил TCP/IP – уланишни мададлайди, фойдаланувчи турган жойига боғлиқ бўлган вақтинча манзил эса локал тармоқ ресурслари билан уланишни таъминлайди. IP мобил тизими учун учта тартибга солувчи талаблар мавжуд: мобил узели (фойдаланувчининг симсиз қурилмаси), уй агенти (уй тармоғида жойлашган сервер) ва ажнабий агент (роуминг узатиувчи тармоқда жойлашган сервер). Мобил узели янги тармоққа ўтганида, у турган жойига боғлиқ бўлган вақтинча IP-манзилни олади ва ажнабий агентда қайдланади. Сўнгра ажнабий агент уй агенти билан боғланиб мобил агентнинг ўзига боғланганлигини хабар қилади. Шу ондан бошлаб барча пакетлар ажнабий агент-роуминг орқали уй агентига йўналтирилади.

Криптоҳимоялаш таҳдидлари. CDMA, GSM уяли тармоқларда ва симсиз Ethernet-тармоқда ахборотнинг конфиденциаллигини ва яхлитлигини таъминлаш мақсадида криптографик воситалар ишлатилади. Аммо хатоликларга йўл қўйиш коммуникациянинг бузилишига ва ахборотнинг ёмон ниятда ишлатилишига олиб келади.

WEP(Wired Equivalent Privacy – симсиз тармоқ даражасидаги махфийлик) – 802.11 хилидаги тармоқ хавфсизлигини таъминлаш учун яратилган криптографик механизм. WEPни татбиқ этишдаги хатоликлар ва бошқариш муаммолари уни бефойда қилиб қўйди. Ушбу механизм барча фойдаланувчилар ишлатадиган ягона статик калитга эга. Internet тармоқда нияти бузук одамга бир неча соат мобайнида калитни тиклашга имкон берувчи воситалар мавжуд. Шу сабабли, WEPга аутентификация ва конфиденциаллик воситаси

сифатида ишониш мумкин эмас. Тавсифланган криптографик усулларни ишлатилгани, умуман ишлатилмаганига караганда яхшироқ, аммо юкорида келтирилган хужумлардан химоялашнинг бошқа усуллари зарур.

11.3. Симсиз тармоқлар хавфсизлиги протоколлари

SSL/TLS протоколлари. Химояланган уланишлар протоколи – Secure Sockets Layer (SSL) Internet браузерларининг хавфсизлиги муаммосини ечиш учун яратилган. SSL таклиф этган биринчи браузер – Netscape Navigator тижорат транзакциялари учун Internet тармоғини хавфсиз қилди, натижада, маълумотларни узатиш учун хавфсиз канал пайдо бўлди. SSL протоколи шаффоф, яъни маълумотлар тайинланган жойга шифрлаш ва расшифровка қилиш жараёнида ўзгармасдан келади. Шу сабабли, SSL кўпгина иловалар учун ишлатилиши мумкин.

SSL ўзидан кейинги TLS (Transport Layer Security – транспорт сатхи химояси протоколи) билан Internet да кенг тарқалган хавфсизлик протоколдир. Netscape компанияси томонидан 1994 йили татбиқ этилган SSL/TLS ҳозирда ҳар бир браузерга ва электрон почтанинг кўпгина дастурларига ўрнатилади. SSL/TLS хавфсизликнинг бошқа протоколлари, масалан, Private Communication Technology (PCT – хусусий коммуникация технологияси), Secure Transport Layer Protocol (STLP хавфсиз сатхнинг транспорт протоколи) ва Wireless Transport Layer Security (WTLS – симсиз муҳитда транспорт сатхини химоялаш протоколи) учун асос вазифасини ўтайди.

SSL/TLSнинг асосий вазифаси тармоқ трафигини ёки гиперматрни узатиш протоколи HTTPни химоялашдир. SSL/TLS алоқа жараёнининг асосида ётади. Оддий HTTP-коммуникацияларда TCP уланиш ўрнатилади, хужжат хусусида сўров юборилади, сўнгра хужжатнинг ўзи юборилади.

SSL/TLS уланишларни аутентификациялаш ва шифрлаш учун ишлатилади. Бу жараёнларда симметрик ва асимметрик алгоритмларга асосланган турли технологиялар комбинациялари иштирок этади. SSL/TLSда мижозни ва серверни идентификациялаш мавжуд, аммо аксарият ҳолларда сервер аутентификацияланади.

SSL/TLS турли тармоқ коммуникациялар хавфсизлигини таъминлаши мумкин. Протоколнинг жуда кенг тарқалиши электрон

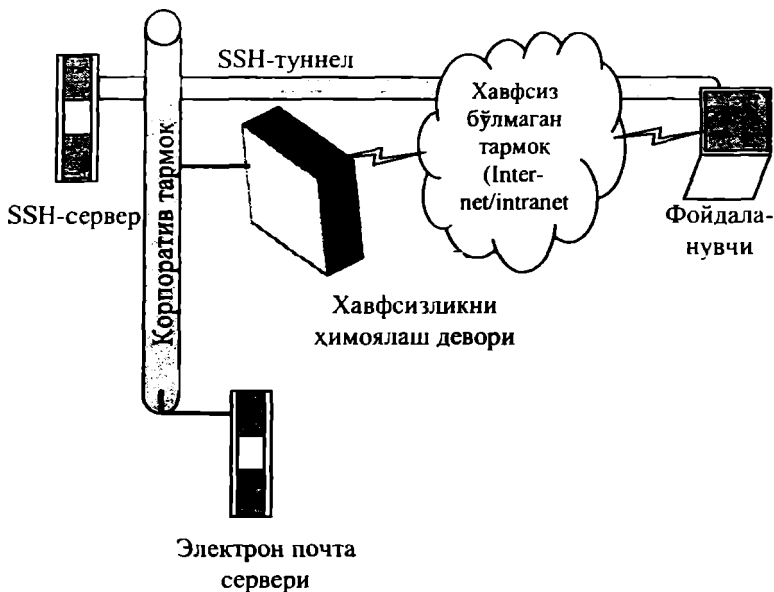
почта, янгиликлар, Telnet ва FTP (File Transfer Protocol – файлларни узатиш протоколи) каби машхур TCP-коммуникациялар билан боғлиқ. Аксарият ҳолларда SSL/TLS ёрдамида коммуникация учун алоҳида портлар ишлатилади.

SSH протоколи. Secure Shell протоколи, SSL/TLS каби коммуникацияларни химоялаш учун 1995 йили яратилган. Ўзининг мосланувчанлиги ва ишлатилишининг соддалиги туфайли SSH оммавий хавфсизлик протоколига айланди ва ҳозирда аксарият операцияларда стандарт илова ҳисобланади.

SSHда алоқа сеанси жараёнида маълумотларни узатиш учун симметрик калидан фойдаланилади. Серверни, ҳам мижозни аутентификациялаш учун SSHни осонгина қайта конфигурациялаш мумкин.

Кўпинча SSH тармоқ хостларини бошқаришда ишлатиладиган, кўп тармқалган илова – telnet ни алмаштириш учун ишлатилади.

Баъзида ишлаб чиқарувчилар SSHни telnet ёки FTPни алмаштирувчи сифатида мададламайдилар. Бундай ҳолларда SSHни telnet, FTP, POP (Post Office Protocol – почта хабарлари протоколи) ёки ҳатто HTTP каби хавфсиз бўлмаган иловалар хавфсизлигини таъминлаш учун ишлатиш мумкин. 11.13-расмда трафикни хавфсиз бўлмаган тармоқдан SSH серверга ўтказиш учун конфигурацияланган брандмауэр келтирилган.



11.13-расм. SSH-туннел.

Хавфсиз бўлмаган тармоқдан SSH серверга ва аксинча ҳеч қандай трафик ўтказилмайди. SSH-сервернинг SSH дан терминал фойдаланишидан ташқари, портнинг қайта йўналтирилиши электрон почта трафигини SSH-серверга хавфсиз тармоқ бўйича узатилишини таъминлаши мумкин. Сўнгра SSH-сервер пакетларни электрон почта серверига қайта йўналтиради. Электрон почта серверига трафик SSH-сервердан келганидек туюлади ва пакетлар SSH-серверга, фойдаланувчига туннеллаш учун юборилади.

WLTS протоколи. SSL/TLSга асосланган WLTS протоколи WAP (Wireless Application Protocol – симсиз иловалар протоколи) қурилмаларида, масалан, уяли телефонларда ва чўнтак компьютерларида ишлатилади. SSL ва WLTS бир-биридан транспорт сатҳи билан фарқланади. SSL йўқолган пакетларни қайта узатишда ёки ностандарт пакетларни узатишда TCP ишига ишонади. WLTSдан фойдаланувчи WAP қурилмалари ўз функцияларини бажаришида TCPни қўллай олмайдилар, чунки фақат UDP (user Datagram Protocol) бўйича ишлайдилар. UDP протоколи эса уланишга мўлжалланмаган, шу сабабли бу функциялар WLTSга киритилиши лозим.

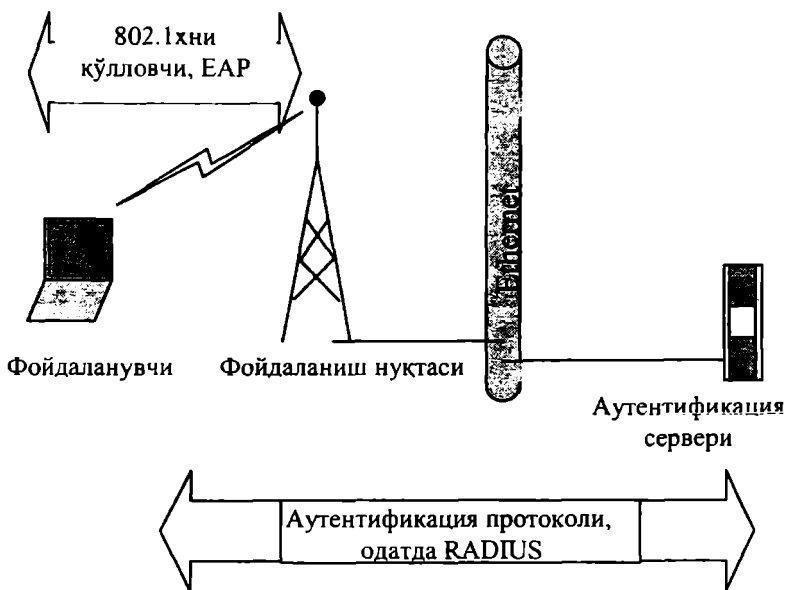
«Кўл бериб кўришиш» жараёнида қуйидаги учта синф фаоллашиши мумкин:

- WLTS – 1-синф. Сертификатсиз;
- WLTS – 2-синф. Сертификатлар серверда;
- WLTS – 3-синф. Сертификатлар серверда ва мижозда.

1-синфда аутентификациялаш бажарилмайди, протокол эса шифрланган канални ташкил этишда ишлатилади. 2-синфда мижоз (одатда фойдаланувчи терминал) серверни аутентификациялайди, аксарият ҳолларда сертификатлар терминалнинг дастурий таъминотига киритилади. 3-синфда мижоз ва сервер аутентификацияланади.

802.1x протоколи. Бу протоколнинг асосий вазифаси – аутентификациялашдир; баъзи ҳолларда протоколдан шифрловчи калитларни ўрнатишда фойдаланиш мумкин. Уланиш ўрнатилганидан сўнг ундан фақат 802.1x. трафиги ўтади, яъни DHCP (Dynamic Host Configuration Protocol – ҳостларни динамик конфигурациялаш протоколи), IP ва х. каби протоколларга руҳсат берилмайди. Extensible Authentication Protocol (EAP) (RFC 2284) фойдаланувчиларни аутентификациялашда ишлатилади. Бошланишида EAP «нукта-нукта» (PPP, Point-to-Point Protocol) протоколи ёрдамида аутенти-

фикациялашнинг баъзи муаммоларини ҳал этиш учун ишлаб чиқилган эди. аммо унинг асосий вазифаси симсиз алоқа муаммоларини ҳал этишга қаратилиши лозим. ЕАРнинг аутентификациялаш пакетлари фойдаланувчи маълумотларини киритган фойдаланиш нуқтасига юборилади; аксарият ҳолларда бу маълумотлар фойдаланувчи исми (login) ва паролдан иборат бўлади. Фойдаланиш нуқтаси тармоқ яратувчиси танлаган воситаларнинг бири билан фойдаланувчини идентификациялаши мумкин. Фойдаланувчи идентификацияланганидан ва шифрлаш учун канал ўрнатилганидан сўнг алоқа мумкин бўлади ва DHCP каби протоколларнинг ўтишига рухсат берилади (11.14-расм).

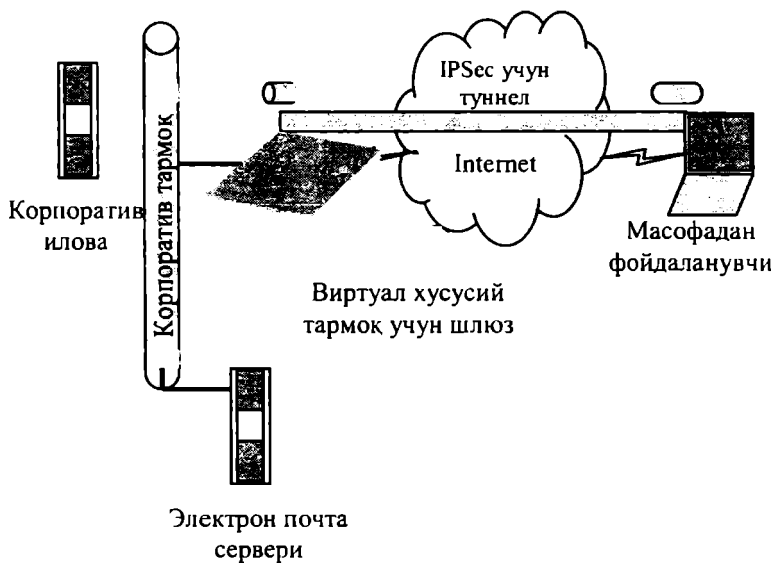


11.14-расм. 802.1x протоколининг кўриниши.

IPSec протоколи. Протоколлар стекида IPSec протоколи SSL/TLS, SSH ёки WTLS протоколларидан пастда жойлашган. Хавфсизликни таъминлаш IP-сатҳида ва Internet-моделда амалга оширилади. IPSec ни татбиқ қилиш усулларидан кўп тарқалгани туннеллаш бўлиб, у битта сессияда IP-трафикни шифрлаш ва аутентификациялаш имконини беради. IPSec ҳозирда Internet да иш-

латилувчи аксарият виртуал хусусий тармоқлардаги (VPN-Virtual Private Network) асосий технология ҳисобланади. IPSecнинг мослашувчанлиги ва иловалар танланишининг кенглиги сабабли, кўпчилик айнан бу схемадан симсиз иловалар хавфсизлигини таъминлашда фойдаланади.

IPSecни иловаларга асосланган қўлланишининг жуда кўп имкониятлари мавжуд. Хавфсиз коммуникациялар учун IPSecнинг қўлланиши кўпинча Internet орқали масофадан фойдаланиш виртуал хусусий тармоғи VPN билан боғлиқ. Қачонки умумфойдаланувчи тармоқ хусусий тармоқ функцияларини амалга ошириш учун ишлатилса, уни VPN деб аташ мумкин. Бундай таърифга ATM (Asynchronous Transfer Mode – узатишнинг асинхрон усули), Frame Relay ва X.25 каби тармоқ технологиялари ҳам тушади. аммо аксарият одамлар Internet бўйича шифрланган канални ташкил этиш хусусида гап кетганида VPN атамасини ишлатишади. Корпоратив тармоқ периметри бўйича 11.15-расмда кўрсатилганидек шлюзлар ўрнатилади ва IPSec-туннел орқали шлюздан масофадан фойдаланиш амалга оширилади.



11.15-расм. IPSec VPN-туннел.

11.4. Симсиз қурилмалар хавфсизлиги муаммолари

Симсиз қурилмаларни тўртта категорияга ажратиш мумкин: ноутбуклар, чўнтак компьютерлари (PDA), симсиз инфратузилма (кўприклар, фойдаланиш нуқталари ва ҳ.) ва уяли телефонлар.

Ноутбуклар – корпоратив симсиз тармоқларда ва SOHO (Small Office Home Office – кичик ва уй офислари) тармоқларида кенг тарқалган қурилма.

Физик хавфсизлик ноутбуклар учун жиддий муаммо ҳисобланади. Бундай компьютерларни харид қилишдаги параметрлардан бири-унинг ўлчами. Ноутбук қанчалик кичкина бўлса, у шунчалик қиммат туради. Бошқа тарафдан, ноутбук қанчалик кичкина бўлса, уни ўғирлаш шунчалик осонлашади. Шифрлаш қалитларининг, масалан, WEP-қалитлар (Wired Equivalent Privacy), дастурий қалитлар, пароллар ёки шахсий қалитларнинг (PGP, Pretty Good Privacy кабилар) йўқотилиши катта муаммо ҳисобланади ва уни иловалар яратилиши босқичидаёқ ҳисобга олиш зарур. Нияти бузук одам ноутбукни ўз ихтиёрига олганидан сўнг аксарият хавфсизлик механизмлари бузилиши мумкин.

Ноутбукларнинг мобиллиги уларнинг корпоратив тармоқлараро экранлар (брандмауэрлар) билан ҳимояланмаган бошқа тармоқлар билан уланиш эҳтимоллигини оширади. Бу Internet-уланишлар, фойдаланувчи тармоқлар, асбоб-ускуна ишлаб чиқарувчиларининг тармоғи ёки ракиблар ҳам жойланувчи меҳмонхона ёки кўрғазмалардаги умумфойдаланувчи тармоқлар бўлиши мумкин. Бундай ҳолларда мобил компьютерларнинг ахборот хавфсизлиги хусусида жиддий ўйланиш лозим.

Ноутбукларнинг физик сақланишларини таъминлаш усуллари-дан бири-хавфсизлик кабелидан фойдаланиш. Ушбу кабел ноутбукни столга ёки бошқа йирик предметга «бойлаб» қўйишга мўлжалланган. Албатта, бу юз фоизлик қафолатни бермайди, аммо ҳар ҳолда ўғрининг анчагина куч сарф қилишига тўғри келади.

Ноутбукларнинг тез-тез ўғирланиши сабабли, ахборотни архивлашнинг хавфсизликни таъминлашга нисбатан муҳимлиги кам эмас. Шифрлаш дастурлари файллар хавфсизлигини таъминлашда ёки қаттиқ дискларда шифрланган маълумотлар ҳажмини яратишда ишлатилади. Бу маълумотларни расшифровка қилиш учун, одатда, паролни киритиш ёки шахсий қалитларни ишлатиш талаб этилади. Барча ахборотларни шифрланган файлларда ёки архивларда

сакланиши керакли файллар тўпламини архив учун нусхалашни энгиллаштиради, чунки улар энди маълум жойда жойлашган бўлади.

Ўғрилар учун ноутбуклар «биринчи ракамли нишон» эканлигини фойдаланувчилар тушуниб етишлари ва уларни қаровсиз қолдирмасликлари зарур. Ҳатто офисларда ноутбукни кечага қолдириш мумкин эмас, чунки офисга кўп кишилар (компания ходимлари, фаррошлар, мижозлар) ташриф буюрадилар.

Ахборотнинг чиқиб кетиши ноутбук эгасининг кўп одамлар тўпланган жойларда ҳам содир бўлиши мумкин. Самолет – компания менежерлари фойдаланадиган одатдаги транспорт воситасидир. Самолётда кўшни креслодаги йўловчи ноутбук эгасининг елкаси устидан муҳим ахборотни ўқиб олиши мумкин. Ҳатто «уш шайроитидаги» ноутбуклар ҳам химояланиши зарур. Бу ҳолда компьютернинг химояси сервер химоясидан фарқланмайди. Жуда ҳам зарур бўлмаган сервисларнинг ўчирилиши қуролма ишлатини яхшилайти.

Ўзининг дастурий таъминотини ноутбукка ўрнатган нияти бузук одам хавфсизликнинг барча механизмларини четлаб ўтиш имкониятига эга бўлади. Компьютерни ўз ихтиёрига олган ўғри унга ўзининг дастурини ўрнатганида уни тўхтатиб бўлмайди. BIOSда (Basic Input/Output System-киритиш/чиқаришнинг базавий тизими) ва қаттиқ дискда ўрнатилган пароллар ўғриланган ноутбукдан фойдаланишга тўсқинлик қилиши мумкин.

Ушбу барча воситалар, афсуски, тажрибали ҳақер учун тўсик бўлаолмайди.

Чўнтак компьютерлари. PDA(Personal Digital Assistans «шахсий ракамли ёрдамчилар»)нинг кўпгина хилларидан симсиз иловалар билан ишлашда фойдаланилади. Махсус қурилган PDAларда тиббиёт, саноат ёки авиация иловалари ишга туширилади. Чўнтак компьютерлари ҳам мавжуд бўлиб, уларда симсиз алоқа учун ўрнатилган карточка, штрих кодларнинг сканери, хизмат муддати узок бўлган батареялар ёки магнит хошияли карталарни ўқувчи қуролма каби қўшимча қуролмалар билан биргаликда Palm OS ёки Windows SE операцион тизим ўрнатилган. Бундай компьютерлардан фойдаланиш учун махсус техник тайёргарлик талаб этилмайди. Шунга ўхшаш қуролмаларни ёки иловаларни химоялаш айниқса мураккаб масала ҳисобланади.

PDAдан фойдаланишга хошиш билдирган хужум килувчи учун ундаги ахборот киритиш механизмларининг барчаси нишон хисобланади. Ундан ташқари, аксарият чўнтак компьютерлари шундай ишлаб чиқилганки, уларни ишлаб чикувчилари учун иловалардаги хаголикларни осонгина аниқлаш йўллари таъминланган. Хаголикларни аниқлашда ишлатилувчи интерфейслар нияти бузук одамлар учун хақиқий «тешик» хизматини ўташи мумкин.

Чўнтак компьютери ишлайдиган ахборотни химоялаш учун ахборотни чўнтак компьютерида эмас, балки маълумотларнинг хавфсиз резерв базасида сақлаш лозим. Яна бир вариант – JAVA тили иловасидан ёки фойдаланувчи учун махсус яратилган иловалардан фойдаланиш. Бу ҳолда ахборот қурилмада сақланмайди, аммо, PDAнинг дисплейида акелантирилади. Бошқача айтганда, симсиз иловалардан фақат симсиз тармоқдан фойдаланиш мавжуд бўлган жойларда фойдаланиш мумкин.

Аксарият PDAларда парол ёрдамида блокировка ва разблокировка қилиш имконияти мавжуд. Бу усулларга бугунлай ишонмаслик лозим, аммо улар нияти бузук одамларни вақтинча тўхтатиб туриши мумкин. Ундан ташқари, PDAни блокировка қилиш гизими қурилмадаги иловалардан ёки ахборотдан нияти бузук одамларнинг фойдаланишни қийинлаштиради. PDAнинг зарур бўлмаган барча функцияларини ўчириб қуйиш лозим, чунки ҳар бир ўчирилган киритиш механизми бўлиши мумкин бўлган хужумлар сонини камайтиради.

Чўнтак компьютерида муҳим ахборотни сақлаш учун шифрлашни қўллаш ва унга қўшимча сифатида манбани улаш ва экранни блокировка қилиш учун пароллар ўрнатиш тавсия этилади.

Симсиз инфратузилма. Симсиз инфратузилма қурилмалари одатда одамлар йиғилган ерда жойлаштирилади. Уларга кафелар, аэропортлар, корпоратив тадбирларни ўтказиш жойлари ва ҳ. қироди. Турли хил одамлар EAP(Extensible Authentication Protocol – аутентификациялашнинг кенгайтирилувчи протоколи) ёки WEP каби хавфсизлик воситаларини ишдан чиқариш ёки тармоққа сукилиб кириш учун тармоқ конфигурацияси хусусидаги ахборотни қўлга киритиш мақсадида ушбу компонентлардан фойдаланишни хоҳлашлари мумкин.

Симсиз инфратузилма қурилмаларида тармоқни бошқариш функцияларининг хавфсизлигини таъминлаш учун улардан фойдаланишда SSH, SSL (Secure Sockets Layer) ёки SNMP3 (Simple Net-

work Management Protocol 3 – тармокни оддий бошқариш протоколи, 3-версия) каби хавфсиз протоколлардан фойдаланиш лозим. Ундан ташқари telnet, HTTP даги тўғри матн, ва SNMP (биринчи версия) каби хавфсизлик етарли даражасини мададламайдиган протоколлар ўчирилиши лозим. Хавфсиз бошқаришни таъминлаш иложи бўлмаса, фойдаланишнинг баъзи бир нукталарини кетма-кет портлар орқали бошқариш мантиқан тўғри ҳисобланади. Фойдаланиш нукталарини юқорига қўл етмайдиган жойга маҳкамлаб қўйиш ҳам уларни ўғирланишдан сақлайди.

Уяли телефонлар. Уяли телефонлар учун хавфсизлик мулоҳазалари ноутбук ва PDAларга нисбатан келтирилган мулоҳазаларга ўхшаш. Курилмаларнинг ўзи ва мос дастурий таъминот учун хавфсизлик муаммоси ҳам ҳеч нимаси билан фарқ қилмайди.

Уяли телефонлар ҳам бошқа симсиз курилмаларга бўладиган ҳужумларга дучор бўладилар. Одатда, буфернинг тўлиб-тошиши, катор форматига ҳужумлаш, грамматик хатоликлар ишлатилади, натижада ҳужум қилувчи ўғирланган курилмада ўзининг дастурини ишга туширишга эришади. Мисол сифатида SMSнинг қисқа хабарларини кўрсатиш мумкин. Ўзининг телефони орқали SMS жўнатган фойдаланувчига ҳужумга дучор бўлиши хавфи туғилади. Бу ҳужум натижасида хизмат қилиш тўхтатилади ёки фойдаланувчи терминалида бегонанинг командалари бажарилади.

Ундан ташқари, SIM-карталарни (Subscriber Identity Module – абонент идентификацияси модули) ишлаб чиқарувчилари курилмаларига уяли телефонга симсиз интерфейс орқали юкланилиши руҳсат этиладиган қўшимча функцияларни кирита бошладилар. Мисол тариқасида Sim Toolkit ва MEХЕни кўрсатиш мумкин. Зарарли иловаларни бошқа фойдаланувчига узатишни олдини олувчи усуллар ташқи ҳужумларга дучор бўлади. Бундай иловаларнинг моҳияти шундаки у нияти бузук одамга фойданувчининг манзил китобини ёки телефондаги бутун SMS рўйхатини узатиши мумкин. Баъзи счимлар DES стандарти асосида ишлайди, аммо худди шундай DES-калитлар ҳар бир SIM-карталар учун ишлатилади.

Терминаллар учун парол ёки PIN-кодларни ишлатиш тавсия этилади. GSM(Global System for Mobile Communications – мобил коммуникацияларнинг глобал тизими) тармоқларида ишловчи телефонлар хавфсизлигини таъминлашда SIM PIN керак бўлади. Бу функциядан максимал фойдаланиш учун барча бўлиши мумкин

бўлган PINлардан фойдаланиш ҳамда IMEI (International Mobile Equipment Identity – мобил қурилманинг халқаро рақам)нинг ишончли жойда ёзилиши тавсия этилади.

Мухим ахборотни узатиш учун терминалдан фойдаланишда ахборотни албатта шифрлаш зарур. Кредит карточкалар номерларини ёки бошқа шахсий ахборотни узатиш учун албатта SSL-химояли WTLS-уланиш хизматидан фойдаланиш зарур. Ундан ташқари, GSM ичидаги алгоритмларга бўладиган аксарият ҳужумлар нияти бузук одамга фойдаланувчининг телефон рақамини ўйлаб чиқаришга (клонировка) имкон беради. Бу ҳужумлар одатда телефон мавжудлигини талаб қилади, шу сабабли телефонни хавфсиз жойда сақлаш, йўқотилган ёки ўғирланган ҳолда тезлик билан операторга хабар бериш лозим.

12.1. Бошқаришнинг функционал масалалари

Замонавий ахборот технологияларидан муваффақиятли фойдаланиш учун нафақат тармоқларнинг ўзини, балки тармоқ хавфсизлиги воситаларини ҳам ишончли ва самарали бошқариш зарур. Ҳозирги вақтда компаниянинг бутун инфратузилмасини камраб олувчи бошқаришнинг комплекс тизимини яратиш биринчи галдаги вазифа ҳисобланади. Бундай бошқариш тизими ахборот тизимининг мураккаблиги ва масштабидан қатъий назар, қуйидагиларга имкон яратади:

- бутун ахборот инфратузилмасига марказлаштирилган ва оператив бошқариш таъсирни кўрсатиш;
- оператив ечимларни қабул қилиш учун ахборот хавфсизлиги ҳолати хусусидаги объектив ахборотни берувчи мунтазам аудит ва кенг қўламдаги мониторинг ўтказиш;
- ахборот инфратузилмаси ривожини башоратлаш учун унинг ишлаши хусусидаги статистик маълумотларни тўплаш.

Ахборот тизимларини бошқаришнинг ITIL методологияси.

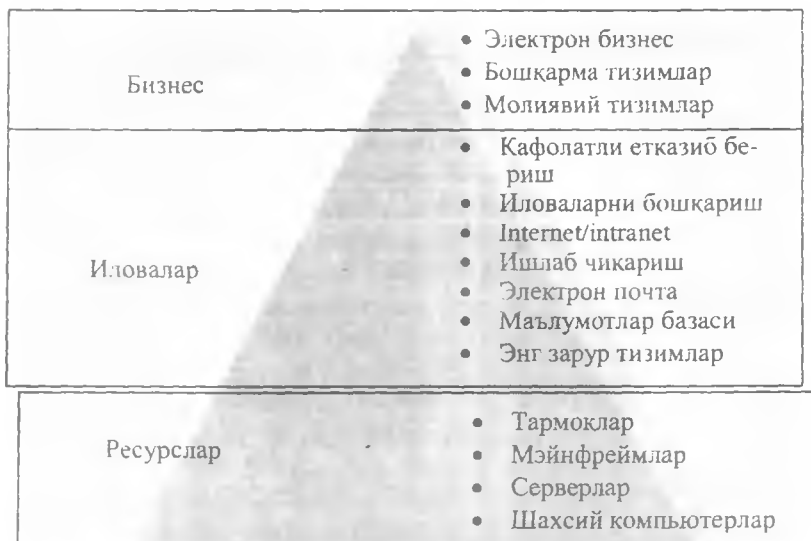
ITIL (IT Infrastructure Library) методологиясига мувофиқ ахборот тизими иккита йирик блокдан – ахборот инфратузилмаси ва ахборот сервисларидан иборат (12.1-расм).



12.1-расм. ITIL методологияси нуқтаи назаридан ахборот тизимининг кўриниши.

Ахборот инфратузилмаси ахборот сервислари ишловчи моддий асос, мухит ҳисобланади. Ахборот сервисларига Internet-сервислар, иловалар сервиси, бошқариш, ечим қабул қилиш сервислари ва ҳ. киради. Ахборот инфратузилмаси сервислар ишлашини таъминловчи техник воситалар, алоқа линиялари, муолажалар, меъёрий ҳужжатлар ва ҳ. мажмуидир. Ахборот сервисларининг сифати бевосита ахборот инфратузилмаси ва уни бошқариш сифатига боғлиқ.

Ахборот инфратузилмасини асосида ахборот ресурслари (ҳисоблаш платформалари, серверлар, шахсий компьютерлар, маълумотларни узатиш тармоқлари, алоқа линиялари) ётувчи пирамида сифатида тасаввур этиш мумкин (12.2-расм).

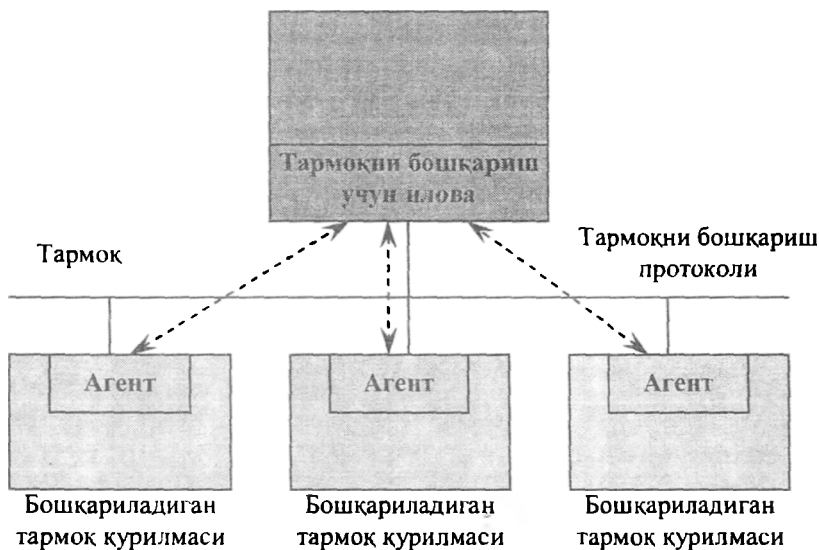


12.2-расм. Ахборот инфратузилмасини ташкил этувчилари.

Пирамиданинг иккинчи сатҳини гурли иловалар ташкил этади. Бу иловалар биринчи сатҳ ресурсларидан фойдаланиб татбикий дастур таъминоти, электрон почта, кафолатланган етказиш тизими, маълумотлар базаси, Web-серверлар ва ҳ. каби муайян иловалар

ишлашни таъминлайди. Ва ниҳоят, энг юкори сатҳда бизнес ва ишлаб чиқариш жараёнларининг ўтишини таъминловчи иловалар ишлайди. Иккала пастки сатҳдан фойдаланувчи бу иловалар ишлаб чиқаришни бошқариш, буюртмачилар ва таъминловчи билан ўзаро алоқа, молиявий ҳисоб ва ечимни қабул қилишни мададлаш каби бизнес – масалаларни ечишга йўналтирилган.

Умумий ҳолда, тармоқни бошқариш тизимининг архитектура-си 12.3-расмда келтирилган кўринишга эга. Тармоқни бошқариш иловаси тармоқ маъмурининг иш жойида ёки бошқа компьютерда бажарилиши мумкин. Унинг вазифаси бошқарилувчи қурилмаларда бажариладиган агент – иловалардан ёки операцион тизим сервисларидан келувчи бошқарилувчи объект хусусидаги ахборотни йиғиш.



12.3-расм. Тармоқни бошқариш тизимининг умумлаштирилган архитектураси.

Бундай иловаларни агентлар билан ўзаро алоқаси учун одатда, SNMP (Simple Network Management Protocol) ёки CMIP (Common Management Information Protocol) протоколларидан фойдаланилади. Биринчиси, одатда, локал тармоқда ишлатилса, иккинчиси теле-

коммуникациядан фойдаланувчи таксимланган тармоқларда ишлатилади. Аммо дастур таъминотини баъзи ишлаб чиқарувчилари тармоқни бошқаришда хусусий тармоқ протоколларидан фойдаланишади.

Тармоқни бошқарувчи замонавий воситалар қуйидаги вазифаларни бажара олади:

- бошқарилувчи компьютер ва қурилмалардаги бузилишларни кузатиш, сабабларни аниқлаш ва бартараф этиш (кўпинча автоматик тарзда), оқибатларини тузатиш ва бузилишларни олдини олиш (масалан ташхислаш амалини бажариш орқали);

- компьютерларнинг ва тармоқ қурилмаларининг конфигурацияланишини бошқариш (хусусан, инициализациялаш, қайта конфигурациялаш ва тармоқ қурилмалари ва компьютерларни узиб қўйиш);

- фойдаланувчилар ва фойдаланувчилар гуруҳи томонидан тармоқ ресурсларидан фойдаланишни тартибга солиш (масалан, диски ва бошқа квоталарни тартибга солиш);

- тармоқ қурилмалари ва сервислар унумдорлиги даражасини бошқариш (тармоқ қурилмалари ишлатилиши жадаллиги статистикасини ва хатоликлар частотасини йиғиш ва таҳлиллаш ҳамда олинган маълумотлар асосида улар унумдорлиги даражасини сунъий тарзда ўрнатиш);

олдиндан белгиланган хавфсизлик сиёсати асосида тармоқ ресурсларидан фойдаланишни назоратлашдан фойдаланиб маълумотлар ҳимоясини бошқариш ва уларни бузишга уринишлардан маъмурни хабардор этиш.

Корхона ахборот хавфсизлиги тизими корпоратив тармоқни бошқариш тизимининг энг муҳим компоненти ҳисобланади. Корхона масштабидаги таксимланган тармоқда ахборотни ҳимоялаш воситаларини бошқарувчи тизим қуйидаги вазифаларни бажариши лозим:

- корхона тармоғи доирасида хавфсизлик сиёсатини бошқариш, алоҳида қурилмалар хавфсизлигининг локал сиёсатини шакллантириш ва уни ахборотни ҳимояловчи барча қурилмаларга етказиш;

- фойдаланиш объектларини ва субъектларини конфигурациялашни бошқариш; ҳимоя қурилмалари ва дастурий таъминоти таркибини, версиясини, компонентларини бошқаришни ўз ичига олади;

– таксимланган татбиқий тизимларга химоя сервисларини тақдим этиш, химояланган иловалар ва улар ресурсларини рўйхатга олиш. Иловаларнинг бу гуруҳи, аввало, татбиқий тизимлар томонидан химоя сервисларини бошқариш учун интерфейсни таъминлаш лозим;

– криптовоситаларни бошқариш, хусусан, калитли бошқариш (калитли инфраструктура). Калитли инфратузилма инфратузилма хизмати таркибида ишлаши лозим;

– ходисавий протоколлаш; турли қурилмаларга *логларни* беришни соzлашни, логларни деталлаштириш сатҳини бошқаришни, протокол олиб борилувчи ходисаларни таркибини бошқаришни ўз ичига олади:

– ахборот тизими хавфсизлигини аудитлаш; ахборот тизимлари химояланишининг жорий ҳолати хусусидаги объектив маълумотларни баҳолашни таъминлайди;

– тизим хавфсизлигини мониторинглаш; қурилмалар ва қурилмаларда кечувчи ходисалар (химоялаш контексти бўйича) ҳолати, фаоллиги хусусида, масалан, бўлиши мумкин бўлган хужумлар хусусида реал вақтда ахборот олиншини таъминлайди;

– махсус химояланган иловалар, масалан амаллар устидан нотариал назорат ишини таъминлаш ҳамда регламентда кўзда тутилган тадбирларни (калитларни, паролларни, химоя қурилмаларини алмаштириш, смарт-карталарни ишлаб чиқариш ва ҳ.) мададлаш;

– иловаларнинг лойиха-инвентаризациялаш гуруҳи ишини таъминлаш. Иловаларнинг бу гуруҳи корхона тармоғига химоя воситаларини ўрнатишни, кўлланиладиган химоя воситаларини ҳисобга олишни, химоя воситаларининг модул таркибини назоратлашни, химоя воситалари ҳолатини назоратлашни ва ҳ. бажаради.

Тармоқларни анъанавий бошқариш тизими ва тармоқдаги ахборотни химоялаш воситаларини бошқариш тизими орасида ўзаро алоқани комплекслаш ва ташкил этиш муаммоси мавжуд.

12.2. Хавфсизлик воситаларини бошқариш архитектураси

Компания таксимланган ахборот тизимида хавфсизлик сиёсатини муваффақиятли амалга ошириши учун хавфсизликни бошқариш марказлиштирилган бўлиши ва ишлатиладиган операциялар тизимга ва татбиқий тизимларга боғлиқ бўлмаслиги лозим. Ундан ташқари, корпоратив ахборот тизимида кечувчи жараёнлар-

ни (рухсатсиз фойдаланиш, фойдаланувчилар имтиёзини ўзгариши ва х.) рўйхатга олиш тизими ягона бўлиши ва маъмурга корпоратив ахборот тизимидаги барча ўзгаришларнинг тўлиқ кўринишини тасаввур этишига имкон бериши лозим.

Корпоратив ахборот тизими хавфсизлигини марказлаштирилган бошқариш асосида глобал бошқариш концепцияси GSM (Global Security Management) ётади. Ушбу концепция корхона ахборот ресурсларини қуйидаги хусусиятларга эга бўлган комплекс бошқариш тизимини қуришга имкон беради:

- корхонанинг барча ресурслари (хавфсизлик сиёсати объектлари) учун химоялашнинг яхлитлигини, зиддиятлик эмаслигини ва қоидалар тўпламининг тўлаллигини таъминловчи, барча мавжуд химоя воситаларини корхона хавфсизлиги сиёсати асосида бошқариш;

- ресурсларни тавсифловчи шахсий воситалар ҳамда корхонанинг бошқа каталоглари билан алоқаси бўйича фаоллашувчи корхона муҳитининг ягона (таксимланган) каталоги орқали корхонанинг барча ресурсларини аниқлаш;

- хавфсизлик сиёсатига асосланиб, ахборотни химоялашнинг локал воситаларини марказлаштирилган бошқариш;

- корхона муҳитида сиёсат объектларини токенлар ва очиқ калитлар инфратузилмасидан фойдаланиб катъий аутентификациялаш;

- каталогда белгиланган корхона ресурсларидан ёки бутун каталог қисмларидан фойдаланишни маъмурулашнинг кенгайтирилган имкониятлари;

- ҳисоб-китобликни (корпоратив тармок масштабида тизимнинг таксимланган объектларининг ўзаро алоқасидаги барча амалларини рўйхатга олиш) ва аудитни, хавфсизлик мониторингини, хавотирли сигнализацияни таъминлаш;

- умумий бошқариш тизимлари ва хавфсизликнинг инфратузилма тизимлари билан интеграцияланиши.

Ушбу концепция доирасида «хавфсизлик сиёсатига асосланган PBM (Policy Based Management) бошқариш» деганда корхона бизнес-объекти учун таърифланган қоидалар тўплами тушунилади. Бу қоидалар тўплами объектларнинг бизнес-соҳани тўлиқ камраб олишини ва ишлатилувчи бошқариш қоидаларининг зиддиятлик эмаслигини кафолатлайди.

РВМ принципларига асосланган, корхона хавфсизлигини бошқаришга мўлжалланган GSM бошқариш тизими қуйидаги талабларга жавоб беради:

- корхона хавфсизлиги сиёсати мантиқий ва семантик боғланган, шаклланувчи, таҳрирланувчи ва таҳлилланувчи маълумотларнинг бир бутун тузилмасидан иборат;

- корхона хавфсизлиги сиёсати ягона контекстда химоянинг барча сатҳлари учун химоянинг тармок сиёсати ва корхона ахборот ресурслари хавфсизлик сиёсатининг бир бутуни сифатида белгиланади;

- корхона ресурсларини ва хавфсизлик сиёсатини маъмурлашни энгиллаштириш мақсадида сиёсат параметрлари сони минималлаштирилади.

GSM бошқариш тизими хавфсизлик сиёсатининг корхона хавфсизлиги концепцияси моделига мослигини текширувчи кўп мезонли воситалар эвазига хавфсизлик сиёсатини таҳлиллашнинг турли-туман механизмларини таъминлайди.

Хавфсизликнинг глобал ва локал сиёсатлари

Корхона хавфсизлигининг глобал сиёсати ахборот хавфсизлиги контекстида корпоратив тармок объектлари ўзаро алоқасининг параметрларини тавсифловчи хавфсизлик қоидаларининг чекли гўшламидир.

Бунда хавфсизликнинг глобал сиёсати объекти сифатида алоҳида ишчи станциялари ва қисм тармоқлар ҳамда ўз ичига компаниянинг бутун тузилмавий бўлимларини олувчи (масалан, маркетинг бўлими ёки молиявий департамент) объектлар гуруҳи ёки хатто алоҳида компания кўрилиши мумкин.

Хавфсизликнинг глобал сиёсати тармокдаги ўзаро алоқага, ҳамда тизимнинг назоратлаш ва бошқариш функцияларига тааллуқли бўлиши мумкин. Бажарадиган функциялари бўйича хавфсизликнинг глобал сиёсати қуйидаги гуруҳларга бўлинади:

- *VPN қоидалари*. Қоидаларнинг бу гуруҳи IPSec протоколлари ёрдамида амалга оширилади;

- *пакетли филтрлаш қоидалари*. Бу қоидалар Stateful ва Stateless ҳилидаги пакетли филтрлашни таъминлайди.

- *proxy-қоидалар*. Бу қоидалар берилган татбиқий протоколлар бошқарувида узатилувчи трафикни филтрлашга жавоб беради;

- *аутентификацияланган/авторизацияланган фойдаланиш қоидалари*;

– *сигнализацияга ва ҳодисавий протоколлашга жавоб берувчи қоидалар.*

Хавфсизликнинг глобал сиёсати тармоқ сатҳида хавфсизлик сиёсатининг мантикий яхлит ва семантик тўлик гавсифи бўлиб. унинг асосида алоҳида қурилмалар хавфсизлигининг локал сиёсати қурилиши мумкин.

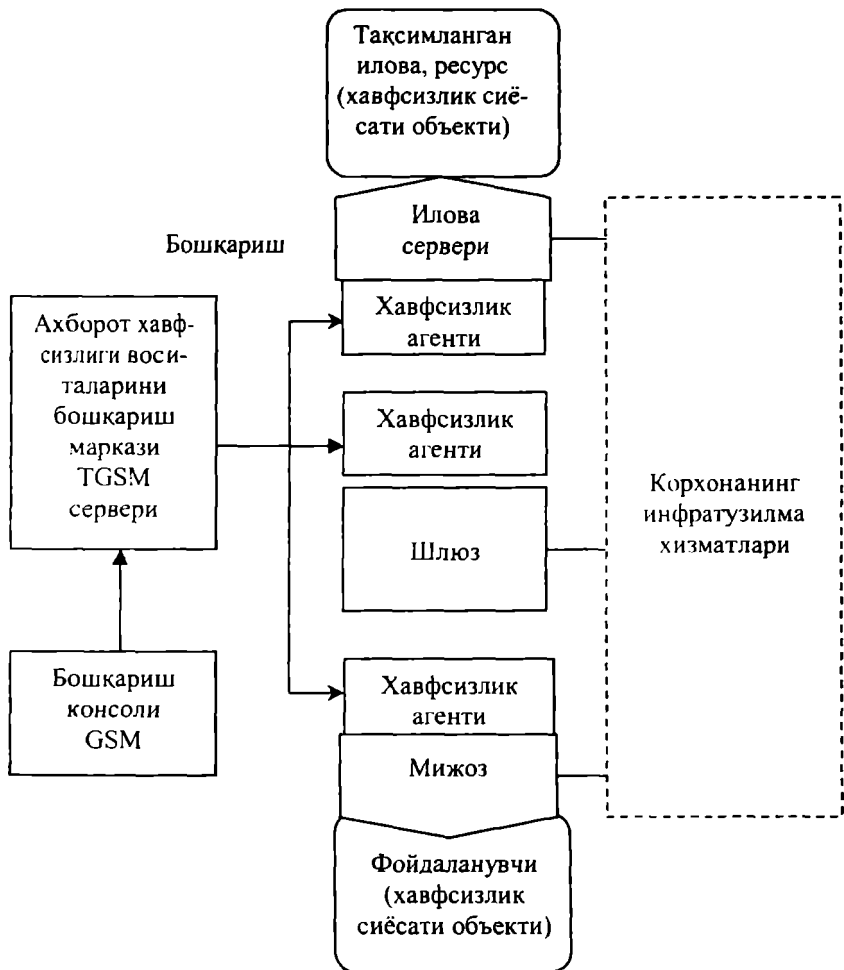
Хавфсизликнинг локал сиёсати ахборот хавфсизлигининг кандайдир сервисини амалга оширувчи ҳар қандай химоялаш воситасига зарур ҳисобланади. Анъанавий ёндашишда маъмурга ҳар бир химоя воситасини алоҳида созлашга ёки энг оддий созлашни узелларнинг катта сонига қайтаришга (репликациялашга) тўғри келар эди. Равшанки, бу маъмурлашнинг катта сонли хатолигига олиб келар ва натижада корпоратив тармоқнинг химояланиш даражаси жиддий пасаяр эди.

Маъмур томонидан хавфсизликнинг глобал сиёсати шакллантирилганидан сўнг бошқариш маркази унинг асосида ҳар бир химоя воситаси учун автоматик тарзда химоялашнинг алоҳида локал сиёсатини ҳисоблайди ва мос химоя воситасининг бошқариш модулига зарурий созлашларни автоматик тарзда юклайди.

Тармоқда хавфсизликнинг глобал сиёсатини ва муайян қурилмада хавфсизликнинг локал сиёсатини амалга ошириш қоидаларининг бир-биридан фарқи шундаки, хавфсизликнинг глобал сиёсатидаги қоидалардан фойдаланиш объектлари ва субъектлари тармоқ чегарасида ихтиёрий равишда тақсимланиши мумкин, хавфсизликнинг локал сиёсатидаги қоидалардан эса фақат тармоқ қурилмаларидан бирининг мухити чегарасида фойдаланиш мумкин.

Ахборот хавфсизлиги воситаларини бошқариш тизимининг умумий тузилма схемаси 12.4–расмда келтирилган. Асосий хавфсизлик воситаларининг вазибалари қуйидагича. Мижоз шахсий компьютерида ўрнатилган *хавфсизлик агенти* одатда, «мижоз-сервер» иловаларида мижоз сифатида катнашувчи алоҳида фойдаланувчини химоялашга мўлжалланган.

Иловалар серверига ўрнатилган *хавфсизлик агенти* тақсимланган иловаларнинг сервер компоненти хавфсизлигини таъминлашга мўлжалланган. Шлюз компьютерига ўрнатилган *хавфсизлик агенти* турли тармоқ хавфсизлиги сиёсатини мувофиқлаштириш масаласини ечган ҳолда, корхона ичида ёки корхоналар орасида тармоқ агентларини ажратилишини таъминлайди.



12.4-расм. Ахборот хавфсизлиги воситаларини бошқариш тизимининг умумий тузилма схемаси.

Бошқариш маркази тармоқ масштабида хавфсизликнинг глобал сиёсатини тавсифлашни, глобал сиёсатни химоялаш қурилмаси хавфсизлигининг локал сиёсатига трансляциялашни, химоялаш қурилмасини юклашни ва тизимнинг барча агентлари ҳолатини назоратлашни таъминлайди.

Бошқариш консоли маъмур (маъмурлар) иш жойини ташкил этишга мўлжалланган. GSMнинг ҳар бир сервери учун бир неча консоллар ўрнатилиши мумкин.

Хавфсизликнинг локал агенти охириги курилмада (мижозда, серверда, шлюзда) жойлаштирилувчи дастур бўлиб, куйидаги функцияларни бажаради:

- хавфсизлик сиёсати объектларини аутентификациялаш, жумладан, аутентификациялашнинг турли сервисларини интеграциялаш;

- тизимдаги фойдаланувчини ва у билан боғлиқ ҳодисаларни аниқлаш;

- хавфсизлик воситаларини марказлаштирилган бошқаришни ва фойдаланиш назоратини таъминлаш;

- иловалар манфаати учун ресурсларни бошқариш, гатбикий сатҳ ресурсларидан фойдаланишни бошқаришни мададлаш;

 - трафикни ҳимоялаш ва аутентификациялаш;

 - графикни филтрлаш;

- ходисавий протоколлаш, мониторинг, хавотирли сигнализация.

Локал агентнинг марказий элементи – хавфсизликнинг локал сиёсатининг процессори (LSP processor) хавфсизликнинг локал сиёсатини изоҳлайди ва бошқа компонентлар орасида чакиришларни таксимлайди.

12.3. Ахборот тизимларининг аудити ва мониторинги

Ахборот хавфсизлиги тизими амалга оширилганида тармок инфратузилмасини мураккаблиги, маълумотлар ва иловаларнинг турли-гуманлиги сабабли кўпгина гаҳдидлар хавфсизлик маъмури-нинг эъгиборидан четда қолиши мумкин. Шунинг учун ахборот тизимларининг мунтазам аудити ва доимий мониторинги амалга оширилиши зарур.

Ахборот тизимлари хавфсизлигининг аудити. Аудит-корхонанинг алоҳида соҳаларини мустакил экспертизаси. Корхона аудитининг ташкил этувчиларидан бири унинг ахборот тизими аудити ҳисобланади. Ахборот тизимларининг аудити – ахборот тизими ҳимояланишининг жорий ҳолаги, ундаги ҳаракатлар ва хо-

дисалар хусусидаги объектив маълумотларни олиш ва баҳолаш, улар сатҳининг белгиланган мезонга мослигини аниқловчи тизимли жараёндир. Аудит ўтказилиши ахборот тизимининг жорий хавфсизлигини баҳолашга, хавф-хатарни баҳолашга, уларнинг ташкилот бизнес-жараёнларига таъсирини башоратлашга ва бошқаришга, ташкилот ахборот ресурслари хавфсизлигини таъминлаш масаласига асосли ёндашишга имкон беради.

Ахборот тизимлари хавфсизлигининг аудити куйидаги босқичларни ўз ичига олади:

- аудит муолажасининг бошланиши;
- аудит ахборотини йиғиш;
- аудит маълумотларини таҳлиллаш;
- тавсиялар ишлаб чиқиш;
- ҳисобот тайёрлаш.

Аудит босқичларининг бажарилиш кетма-кетлиги 12.5-расмда келтирилган.

Аудит муолажасининг бошланиши. Аудит, бу масалада манфаатдор ҳисобланувчи, компания раҳбарияти ташаббуси билан ўтказилади. Аудит тадбирларнинг комплекси бўлиб, унда аудитор билан бирга компаниянинг аксарият тузилмавий бўлинмаларининг вакиллари катнашади. Бу жараёнда иштирок этувчиларининг ҳаракатлари аниқ мувофиқлаштирилиши шарт. Шу сабабли, аудит муолажасининг бошланиши босқичида аудит ўтказиш режасини тайёрлаш ва тасдиқлаш, аудитор ҳуқуқи ва мажбуриятини белгилаш билан боғлиқ ташкилий масалалар ечилиши лозим.

Аудит муолажасининг бошланиши босқичида текшириш доираси аниқланиши лозим. Компаниянинг ахборот қисми тизимининг бирини конфиденциаллик нуқтаи назаридан аудитга тортиб бўлмаса, иккинчисини, етарлича жиддий бўлмаганлиги сабабли, аудит доирасидан чиқариш мумкин.



12.5-расм. Аудит босқичларининг бажарилиш кетма-кетлиги.

Аудит ахборотини йиғиш. Бу босқич энг мураккаб ва узок давом этади. Бунга сабаб, ахборот тизимига керакли ҳужжатларнинг йўқлиги ва аудиторнинг ташкилотнинг кўпгина лавозимли шахслари билан бевосита ўзаро мулоқотда бўлиши зарурияти. Аудитор ташкилот, ахборот тизимининг ишлаши ва жорий холаги хусусидаги ахборотни компаниянинг жавобгар шахслари билан махсус ташкил этилган суҳбат орқали, техникавий ва ташкилий-бошқариш ҳужжатларни ўрганиш йўли билан, ҳамда ихтисослаштирилган дастурий воситалар ёрдамида ахборот тизимини тадқиқлаш орқали олади.

Аудит маълумотларини таҳлиллаш. Таҳлиллаш ахборот тизимларининг аудитида энг масъулиятли босқич ҳисобланади. Таҳлиллашда ноаниқ, эскирган маълумотлардан фойдаланиш ножоиздир, шу сабабли маълумотларга аниқлик киритилиши ва ахбо-

ротлар жиддий йиғилиши мумкин. Аудит маълумотларини таҳлиллашда қуйидаги учта ёндашишдан фойдаланилади.

Биринчи ёндашиш хавф-хатарларни таҳлиллашга асосланади. Хавф-хатарларни таҳлиллашдан мақсад мавжуд хавф-хатарларни аниқлаш ва улар катталигини баҳолаш (уларга сифатий ва миқдорий баҳо бериш). Ушбу ёндашиш жуда мураккаб бўлиб, кўп меҳнат сарф этилади ва аудиторнинг энг юқори малакасини талаб қилади.

Иккинчи ёндашиш ахборот хавфсизлиги стандартларидан фойдаланишга асосланган. Стандартлар ахборот тизимларининг кенг синфи учун дунё амалиётини умумлаштириш натижасида шаклланган хавфсизлик талабларининг базавий гўпламини белгилайди. Бу ҳолда аудитордан, берилган ахборот тизими учун стандарт талаблари гўплами тўғри танлаш талаб этилади. Содаллиги ва ишончилиги туфайли бу ёндашиш амалда кенг қўлланилади. У ресурсларнинг минимал сарфида ахборот тизими хусусида асосланган хулосалар қилишга имкон беради.

Учинчи ёндашиш олдинги иккала ёндашишни комбинациялашни кўзда тутаяди. Ахборот тизимига қўйиладиган хавфсизликнинг базавий талаблари стандарт орқали аниқланса, берилган ахборот тизими ишлашининг хусусиятларини ҳисобга олувчи қўшимча талаблар хавф-хатарларни таҳлиллаш асосида шакллантирилади.

Тавсиялар ишлаб чиқиш. Таҳлиллаш натижалари тавсиялар ишлаб чиқиш учун асос бўлади. Аудитор тавсиялари муайян ва берилган ахборот тизимига қўлланиладиган, иккисодий асосланган, исботланган (таҳлиллаш натижалари билан қувватланган) ва муҳимлик даражаси бўйича рутбаланган бўлиши шарт. Аудитнинг мунтазам ўтказилиши ахборот тизимининг барқарор ишлашини кафолатлайди. Шунинг учун профессионал аудит натижаларидан бири кейинги текширишларни ўтказиш рсжа-графикини шакллантиришдан иборат.

Ҳисобот тайёрлаш. Аудитор ҳисоботи аудит ўтказишнинг асосий ҳужжати ҳисобланади ва унинг сифати аудитор ишининг сифатини характерлайди.

Ҳисобот таркибида аудит ўтказиш мақсадининг тавсифи, текширилувчи ахборот тизимининг характеристикаси, аудит ўтказиш доираси ва ишлатилувчи усуллар бўйича кўрсатма, аудит-маълумотлари таҳлилининг натижаси, бу натижаларни умумлаштирувчи ва ахборот тизими ҳимояланиш сатҳининг стандарт талаб-

ларига жавоб бериши бўйича хулосалар ва албатта, мавжуд камчиликларни бартараф этиш ва химоя тизимини такомиллаштириш бўйича тавсиялар бўлиши лозим.

Ахборот тизимлари хавфсизлигининг мониторинги

Ҳозирда тармоқлараро экран, виртуал хусусий тармоқ, рухсатсиз фойдаланишдан химоялаш воситалари каби химоянинг анъанавий воситалари ишончли ва самарали ахборот хавфсизлиги тизимини куришга зарур бўлсада, етарли эмас. Чунки бу анъанавий воситалар фақат хужумни блокировка қилишга қодир, аммо хужумларни олдини олиш ва оқибатларини аниқлаш имконияти уларда мавжуд эмас.

Ушбу муаммонинг ечими асосланган ёндашиш фаол аудит технологияси ёки хавфсизликни фаол (адаптив) бошқариш технологияси номини олган. Хавфсизликни фаол бошқариш технологияси қуйидаги компонентларни ўз ичига олади:

– ишчи станциялари, серверлар, маълумотлар базасини бошқарувчи тизимлар, тармоқ уланишлари ва Internet ва бошқа глобал тармоқларга уланиш нукталари каби ахборот тизими объектлари химояланишини таҳлилловчи ва заифликларини кидирувчи воситалар;

– хужумларни аниқлаш ва таҳлиллаш воситалари;

– инфратузилма ўзгаришида ёки хужумларда химоялаш воситаларини вақтнинг реал режимида соzлашларни мослаштириш ва бошқариш воситалари.

Ахборот хавфсизлиги тизими мониторинги вазифаларини химояланишни таҳлиллаш ва хужумларни аниқлаш воситалари ба-жаради. Ҳимояланишни таҳлиллаш воситалари ишчи станцияларида ва серверларда, маълумотлар базасида операцион тизим химояси элементларининг соzланишини тадқиқлайди. Улар тармоқ топологиясини тадқиқлайди, химояланмаган ёки нотўғри тармоқ уланишларини кидиради, тармоқлараро экранлар соzланишини таҳлиллайди. Ҳимояланишни таҳлиллаш воситаларини, уларнинг ишлаши бўйича хавфсизлик сканерлари деб ҳам юритишади. Таҳлиллаш натижасида сканер маъмурга юборилувчи, таркибида аниқланган заифликлар ва уларни йўқотиш коидалари бўлган ҳисоботни шаклантиради. Агар сканер таркибида хавфсизлик воситалари соzланишини бошқарувчи воситалар бўлса, у мустақил тарзда уларни қайта конфигурациялаши мумкин.

Ташкилотнинг замонавий инфратузилмасини ҳисобга олган ҳолда айтиш мумкинки, бундай сканерларнинг мавжудлиги ахборот тизимлари хавфсизлиги мониторингининг муҳим элементи ҳисобланади. Таъкидлаш лозимки, бу воситалар химояни ҳужум содир бўлишидан аввал амалга оширади.

Ахборот тизими хавфсизлиги мониторингининг яна бир зарур элементи ҳужумларни аникловчи воситалардир. Ҳужумларни аниклаш корпоратив тармоқда кечувчи шубҳали ҳаракатларни баҳолаш жараёнидир. Ҳужумларни аниклаш вақтнинг реал режимида тармоқ графигини, ҳамда операцион тизим ва иловаларнинг рўйхатга олиш журналларини таҳлиллаш орқали амалга оширилади. Ҳужумларни аниклаш тизимининг компонентлари агентлар деб аталади, ва ишчи станцияларда, серверларда жойлаштирилади ёки тармоқнинг қандайдир сегментини ёки бутун тармоқни қоплайди. Агентлар ўзларининг ишида сканерлар каби маълум заифликлар рўйхатидан фойдаланиб, ҳодисаларни ушбу заифликлар билан такқослайди. Қандайдир узелда шубҳали фаолият аникланганида ҳужумларни аниклаш тизими ушбу фаолият фаоллиги хусусидаги огоҳлантиришни маъмурга жўнатади. У огоҳлантиришни узелнинг ўзига жўнатиши ёки узел ишини блокировка қилиш мумкин. Ушбу тизимнинг фарқли хусусияти – унинг бўлиб ўтган ҳужумларни аниклаш учун ҳодисалар журналани таҳлиллашидир.

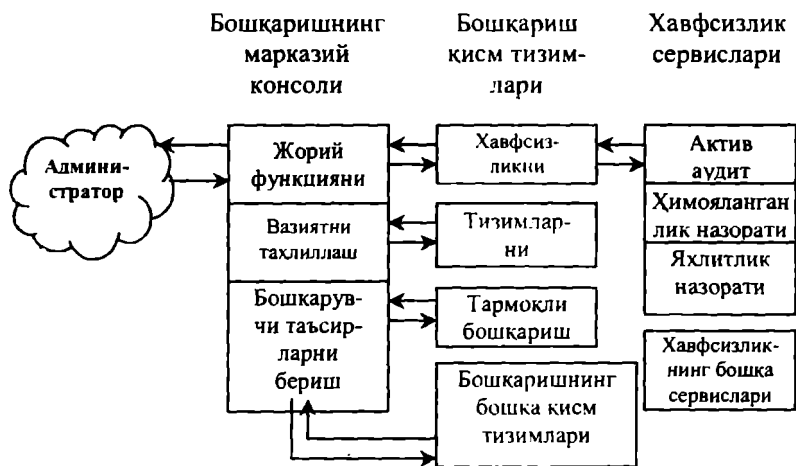
Хавфсизлик воситаларини бошқариш шакли бўйича пассив ва фаол (актив) бўлиши мумкин. Пассив бошқаришда тармоқни бошқариш тизимига ёки маъмурга фақат хабар берилса, фаол бошқаришда ҳужумловчи узел ёки фойдаланувчи билан мустақил тарзда сессия тугалланади.

Бундан ташқари, бу тизимнинг вазифасига тармоқдаги, иловалардаги ёки ташкилот ахборот тизимининг бошқа компонентларидаги заифликларни йўқотиш бўйича маъмурга тавсиялар ишлаб чиқиш қиради.

Фаол аудит тизими (мониторинги) ва умумий бошқариш ўртасида ўзаро алокани ташкил этиш муҳим масалалардан ҳисобланади. Фаол аудит намунавий бошқариш функцияларини, яъни ахборот тизимидаги фаоллик хусусидаги маълумотларни таҳлиллашни, жорий вазиятни акслантиришни, шубҳали фаолликка автоматик тарзда реакция кўрсатилишини бажаради. Тармоқни бошқариш тизими худди шунга ўхшаш ишлайди. Фаол аудит ва умумий бошқаришни умумий дастурий-техник ва ташкилий ечим-

лардан фойдаланиб интеграциялаш максадга мувофик ҳисобланади. Бу интеграцияланган тизимга яхлитликни назоратлаш ҳамда ахборот тизими хатти-ҳаракатларининг ўзига хос жихатларини кузатувчи бошқа йўналишдаги агентлар ҳам киритилиши мумкин (12.6-расм).

Бошқаришнинг марказий консולי мавжуд бўлиб, унда фаол аудит (мониторинг) яхлитликни назоратлаш, бошқа жихатлар бўйича тизим ва тармоқларни назоратлаш тизимларидан маълумотлар тўпланади. Бу консолда жорий вазият акслантирилади, ундан автоматик тарзда ёки қўлда бошқариш командалари берилади. Техник ёки ташкилий сабабларга кўра бу консол бир неча ишчи жойи кўринишида физик амалга оширилиши мумкин (хавфсизлик маъмурига жой ажратиш билан).



12.6-расм. Хавфсизлик сервислари ва бошқариш тизимининг интеграцияси.

Тармоқ хавфсизлигини адаптив бошқариш моделидан фойдаланиш барча таҳдидларни назоратлаш ва уларга ўз вақтида реакция кўрсатиш, нафақат таҳдидларни амалга оширишга шароит яратувчи заифликларни йўқотиш, балки заифликларни пайдо бўлиш шароитларини таҳлиллаш имконини беради.

12.4. Хавф-хатарларни таҳлиллаш ва бошқариш

Хавф-хатарларни таҳлиллаш ва бошқариш ахборот тизимидаги таҳдидлар, заифликлар ва хавф-хатарларни баҳолаш ҳамда ушбу ахборот тизими хавфсизлигининг старли даражасини таъминловчи карши чораларни аниқлаш учун ишлатилади.

Хавф-хатарларни таҳлиллаш-таҳдидларни, заифликларни ва корпоратив ахборот тизими хавфсизлигига бўлиши мумкин бўлган зарарларни аниқлаш жараёни. Хавф-хатарларни таҳлиллашдан мақсад мавжуд хавф-хатарларни аниқлаш ва улар метёрини баҳолаш (уларга миқдорий баҳо бериш). Хавф-хатарларни таҳлиллаш компьютер ахборот тизими хавфсизлигини текшириш бўйича тадбирни ўз ичига олади. Бу тадбирга биноан қайси ресурсларни қайси таҳдидлардан ҳимоялаш зарурлиги ҳамда у ёки бу ресурслар қандай даражада ҳимояга муҳтож эканлиги аниқланади.

Хавф-хатарларни таҳлиллашга турли ёндашишлар мавжуд. Ёндашишни танлаш ташкилотда ахборот хавфсизлиги режимида кўйиладиган талаблар даражасига ва эътиборга олинувчи таҳдидлар характерида (таҳдидлар таъсири спектрига) боғлиқ. Талабларнинг иккита даражаси фарқланади:

- ахборот хавфсизлиги режимида минимал талаблар;
- ахборот хавфсизлиги режимида оширилган талаблар.

Ахборот хавфсизлиги режимида минимал талаблар *ахборот хавфсизлигининг базавий даражасига* мос келади. Бу даражадан, одатда, намунавий лойиҳа счимларида фойдаланилади. Хавф-хатарларни таҳлиллаш соддалаштирилган схема бўйича ўтказилади: хавфсизликка таҳдидларнинг кўп тарқалган тўплами уларнинг эҳтимоллигини баҳоламасдан кўрилади. Вируслар, асбоб-ускуналарнинг бузилиши, рухсатсиз фойдаланиш ва х. каби эҳтимоллиги юқори таҳдидларнинг минимал тўплами кўриладиган катор стандартлар ва спецификациялар мавжуд. Бундай таҳдидларни бетарафлаштириш учун уларнинг амалга оширилиши эҳтимоллиги ва ресурсларнинг заифлигидан катъий назар, карши чоралар кўрилиши лозим, яъни базавий даражада таҳдидлар характеристикаларини кўриш шарт эмас.

Ахборот хавфсизлиги режимида оширилган талаблар, ахборот хавфсизлиги режимида бузилиши оғир оқибатларга сабаб бўлганида ва ахборот хавфсизлиги режимида минимал талаблар старли бўлмаганида ишлатилади.

Ахборот хавфсизлиги режимига оширилган талабларни таърифлаш учун ресурслар ахамиятини аниклаш, тадқиқланувчи ахборот тизими учун долзарб бўлган таҳдидлар рўйхати билан стандарт тўпламини тўлдириш, таҳдидлар эҳтимолигини баҳолаш ва ресурслар заифлигини аниклаш зарур.

Хавф-хатарни таҳлиллаш жараёнини қуйидаги босқичларга ажратиш мумкин:

- корпоратив ахборот тизимининг таянч ресурсларини идентификациялаш;
- у ёки бу ресурснинг муҳимлигини аниклаш;
- таҳдидларнинг амалга оширилишига имкон берувчи мавжуд хавфсизлик таҳдидларни ва заифликларни идентификациялаш;
- хавфсизликка таҳдидларни амалга оширилиши билан боғлиқ хавф-хатарларни ҳисоблаш.

Ресурслар учта категорияга ахборот ресурсларига, дастурий таъминотга ва техник воситаларга (файл серверлари, ишчи станциялар, кўприklar, маршрутизаторлар ва х.) бўлинади. Ҳар бир категория ичида ресурсларни синфларга ва қисм синфларга ажратиш мумкин. Фақат корпоратив ахборот тизими функционаллигини белгиловчи ва хавфсизликни таъминлаш нуқтаи назаридан муҳим бўлган ресурслар идентификацияланиши лозим.

Ресурснинг муҳимлиги (нархи) бу ресурснинг конфиденциаллиги, яхлитлиги ёки фойдаланувчанлиги бузилганида етказилган зарар миқдори билан белгиланади. Ресурслар нарҳини баҳолашда ресурсларининг ҳар бир категорияси учун бўлиши мумкин бўлган зарар миқдори белгиланади.

Намунавий хавфсизлик таҳдидларига корпоратив ахборот тизими ресурсларига локал масофадан ҳужумлар, табиий офат, ходимлар ҳатоси, дастурий таъминотдаги хатолик ёки аппаратуранинг носозлиги сабаб бўлувчи корпоратив ахборот тизим ишидаги бузилишлар тааллуқли. Таҳдид даражаси деганда унинг амалга оширилиши эҳтимолиги тушунилади.

Ҳимоянинг бўшлиги корпоратив ахборот тизимидаги заифликларга сабаб бўлади. Заифликларни баҳолаш хавфсизлик

тахдидларининг муваффақиятли амалга оширилиш эҳтимоллигини аниқлашни назарда тутди. Шундай қилиб, зарар етказиш эҳтимоллиги тахдидларнинг амалга оширилиши эҳтимоллиги ва заифлик миқдори орқали аниқланади.

Хавф-хатар даражаси ресурс нархи, тахдид даражаси ва заифлик миқдори асосида аниқланади. Ресурс нархи, тахдид даражаси ва заифлик миқдори ошиши билан хавф-хатар даражаси ҳам ошади. Хавф-хатарлар даражасини баҳолаш асосида хавфсизлик талаблари белгиланади.

Хавф-хатарларни бошқариш масаласи, хавф-хатар даражасини мақбул миқдоргача камайтиришга имкон берувчи қарши чораларни асосли танлашни ва амалга ошириш нархини баҳолашни ўз ичига олади. Табиийки, қарши чораларни амалга ошириш нархи бўлиши мумкин бўлган зарар миқдоридан кам бўлиши керак.

12.7-расмда хавф-хатарларни бошқариш технологиясининг босқичлари келтирилган.

Ахборот хавфсизлиги сиёсатини аниқлаш. Бу босқичда ахборот хавфсизлиги соҳасидаги қўлланма-хужжатлар, стандартлар, ахборот хавфсизлигининг асосий қоидалари, хавф-хатарларни бошқаришга ёндашишлар аниқланади ҳамда қарши чоралар структуризацияланади ва корпоратив ахборот тизимини сертификациялаш тартиби белгиланади.

Корпоратив ахборот тизимини (КАТ) тавсифлаш. Ушбу босқичда ахборот хавфсизлиги соҳасидаги халқаро, давлат ва корпоратив стандартларга биноан корпоратив ахборот тизимнинг функционал вазифалари тавсифланади. Компаниянинг критик ахборот ресурслари, жараёнлари ва сервислари тавсифланади; корпоратив ахборот тизимининг чегаралари ҳамда бошқариш ва маълумотлар бўйича энг муҳим компонентларининг таркиби ва боғланишлари аниқланади.



12.7-расм. Хавф-хатарларни бошқариш технологиясининг варианты.

Таҳдидларни идентификациялаш. Ушбу боскичда таҳдидлар рўйхати тузилади ва уларнинг даражаси баҳоланади. Бунда турли ташкилотларнинг таҳдидлар синфлари рўйхатидан ҳамда берилган таҳдидни амалга ошириш эҳтимоллигининг рейтинги ёки ўртача кийматидан фойдаланиш мумкин.

Заифликларни идентификациялаш. Ушбу боскичда берилган корпоратив ахборот тизимининг заифликлари рўйхати, уларнинг амалга оширилишидаги жоиш натижалар кўрсатилган ҳолда тузилади. Мавжуд корпоратив ахборот тизими учун рўйхатлар қатор манбалардан фойдаланилиб тузилади. Бу манбаларга заифликларни гармок сканерлари, турли ташкилотларнинг заифликлар каталоги, хавф-хатарларни таҳлилловчи ихтисослаштирилган усуллар киради.

Корпоратив ахборот тизимининг бошқариш тизimini таҳлиллаш. Ушбу боскичда бошқариш, тизими, аниқланган таҳдидларга ва заифликларга жоиш бўлган таъсир нуқтаи назаридан таҳлилланади.

Таҳдидлар параметрларини баҳолаш. Ушбу боскичда ходисага олиб келувчи заифликнинг амалга оширилиши имконияти баҳоланади. Баҳолашнинг намунавий шкаласи – бир неча рутбали (масалан, паст, ўрта, ва юқори сатх) сифатий (балли) шкаладир. Бундай баҳо эксперт томонидан мавжуд объектив факторларни ҳисобга олган ҳолда берилади.

Ахборот хавфсизлиги режимининг бузилиши оқибатларини таҳлиллаш. Ушбу боскичда ахборот хавфсизлиги режимининг бузилиши баҳоси аниқланади. Бузилиш оқибатлари молиявий йўқотишларга, обрўсизланишга, расмий тузилмалар томонидан кўнгилсизликларга ва х. сабаб бўлиши мумкин. Бузилиш оқибатларини баҳолаш учун мезонлар тизими танланади ва оқибатлар оғирлигини баҳолаш учун интеграцияланган шкала белгиланади.

Хавф-хатарларни баҳолаш. Ушбу боскичда ахборот ресурслари хавфсизлигининг бузилиши хавф-хатар даражаси баҳоланади. Хавф-хатар даражаси киймати таҳдидлар, заифликлар даражасига ва бўлиши мумкин бўлган оқибатлар оғирлигига боғлиқ. Хавф-хатарларни баҳолашда сифатий ва миқдорий усуллардан фойдаланилади. Сифатий усул ишлатилганда ахборот хавфсизлиги бузилишининг бўлиши мумкин бўлган хавф-хатарлар хавфлиги даражаси бўйича рутбаланиши лозим. Миқдорий усул ишлатилганда хавф-хатарлар миқдорий шкалаларда баҳоланиши мумкин. Бу тав-

сия этилаётган қарши чораларнинг нархи-самарадорлигини таҳлил-лашни осонлаштиради. Аммо бу ҳолда дастлабки маълумотларни ўлчаш шкалаларига ва ишлатилаётган моделнинг адекватлигига жуда юқори талаблар қўйилади. Оддий ҳолда хавф-хатарни баҳолашда иккита омил-ходиса эҳтимоллиги ва бўлиши мумкин бўлган оқибатлар оғирлиги ишлатилиши мумкин.

Хавф-хатарларни бошқариш бўйича тавсияларни ишлаб чиқиш. Ушбу босқичда турли сатҳлар (ташкилий, дастурий-техник) ва хавфсизликнинг алоҳида жиҳатлари бўйича структуризацияланган қарши чораларнинг комплекс тавсия этилиши лозим. Таклиф этилувчи қарши чоралар комплекси хавф-хатарларни бошқаришнинг танланган стратегиясига биноан қурилади.

Ҳисобот ҳужжатларни ишлаб чиқиш. Ушбу босқичда хавф-хатарларни таҳлиллаш ва бошқаришнинг барча босқичлари бўйича иш натижалари аксантирилган ҳисобот ҳужжатлари тайёрланади.

Таъкидлаш лозимки, ҳозирда ахборот хавф-хатарларини баҳолашни автоматлаштириш мақсадида дастурий маҳсулотлар ишлаб чиқилган.

12.5. Ахборот хавфсизлиги тизимини қуриш методологияси

Ахборот хавфсизлиги моделини қуриш. Корхонадаги ахборот хавфсизлиги бўйича тадбирлар қонун чиқариш, ташкилий ва дастурий-техник характерга эга бўлган катор жиҳатларни камраб олади. Уларнинг ҳар бирида корхона ахборот хавфсизлигини таъминлаш учун бажарилиши зарур бўлган катор масалалар таърифланади. Масалаларни ҳал этишда ахборот хавфсизлиги соҳасидаги халқаро стандартларга асосланган корхона ахборот хавфсизлигининг концептуал моделидан фойдаланиш мумкин.

Қуйидаги халқаро стандартлар корпоратив ахборот тизими химояланишини баҳолаш мезонини ва химоялаш механизмларига қўйиладиган талабларни аниқловчи энг муҳим меъёрий ҳужжатлар ҳисобланади:

- ахборот технологиялари хавфсизлигини баҳолашнинг умумий мезонлари ISO/IEC 15408 (The Common Criteria For Information Technology Security Evaluation);

- ахборот хавфсизлигини бошқаришнинг амалий қоидалари ISO/IEC 17799 (Code of practice for Information Security Management).

Ушбу халқаро стандартларга тўла мос равишда тузилган корхона ахборот хавфсизлигининг концептуал модели 12.8-расмда келтирилган.



Асосий белгилашлар

—————> Бошқарувчи таъсирлар

- - - - -> Табiiй таъсирлар

12.8-расм. Корхона ахборот хавфсизлиги тизимининг концептуаль модели.

Корхона ахборот хавфсизлигининг концептуал моделида куйидаги омиллар ҳисобга олинган:

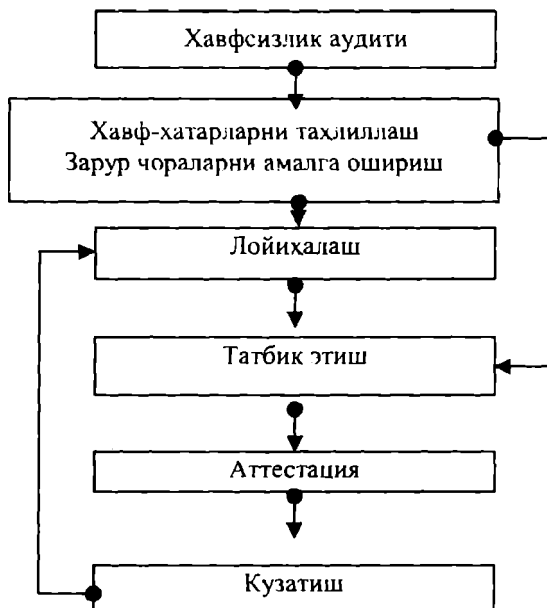
– пайдо бўлиш эҳтимоллиги ва амалга оширилиш эҳтимоллиги билан характерланувчи ахборот хавфсизлиги таҳдидлари;

– таҳдидларнинг амалга оширилиши эҳтимоллигига таъсир этувчи ахборот тизими ёки қарши чора тизими (ахборот хавфсизлиги тизими) *заифликлари*;

– ахборот хавфсизлигига таҳдидлар амалга оширилиши натижасида корхонага етказилувчи зарарни акслантирувчи *омил-хавф-хатар*.

Бу моделнинг ҳаракатдаги субъектлари – Бузғунчи (таҳдидлар манбаини ифодаловчи) ва Эга (корхона маъмури) объект-Ресурсга қарама-қарши мақсадларда таъсир қиладилар. Ресурс-корхонанинг моддий ва ахборот ресурсларини ва ахборот хавфсизлиги ҳолатини ифодалайди.

Ахборот хавфсизлиги тизимини қуриш босқичлари. Ахборот хавфсизлиги тизимини қуриш босқичлар қуйидаги стандартлаштирилган кетма-кетликда амалга оширилади: хавфсизлик аудити; хавф-хатарларни таҳлиллаш, тизимни лойиҳалаш, жорий этиш, аттестациялаш ва қузатиш (12.9-расм).



12.9-расм. Ахборот хавфсизлиги тизимини қуриш босқичлари.

Хавфсизлик аудити. Ҳозирда «хавфсизлик аудити» тушунчаси етарлича кенг талқин этилади. Аудитнинг куйидаги кўринишлари фаркланади.

- ахборот хавфсизлигини тестли бузиш;
- экспресс-текшириш;
- тизимни аттестациялаш;
- лойиҳагача текшириш.

Ахборот хавфсизлиги тестли бузиш корпоратив ахборот тизимининг химояланиш даражасини аниқлаш нуктаи назаридан самарали ҳисобланмайди. «Бузувчи»нинг асосий мақсади бир икки заифликларни топиб, уларни тизимдан фойдаланишда ишлатиш. Агар «тестли бузиш» муваффақиятли чикса, ушбу муайян «бузиш»нинг мумкин бўлган сценарийси ривожини олдини олиб, заифликларни кидиришда давом этиш керак. «Тестли бузиш»нинг муваффақиятсизлигини баббаравар тестланувчи тизимнинг химояланганлиги ва тестларнинг етишмаслиги каби талқин қилиш мумкин.

Экспресс-текшириш доирасида, одатда, кўп вақт сарфини талаб этмайдиган, стандартизацияланган текширишлар асосида корпоратив ахборот тизими хавфсизлик воситаларининг умумий ҳолати баҳоланади. Экспресс-текшириш одатда, ахборот ресурсларининг минимал химояланиш даражасини таъминловчи устувор йўналишларни аниқлаш зарурияти туғилганда ўтказилади.

Тизимни аттестациялаш тизимнинг ахборот ресурсларининг химояланиш талабларига мослигини текшириш мақсадида амалга оширилиди. Бунда ҳам ташкилий, ҳам техник жиҳатдан талаблар тўплами расмий текширилади, хавфсизлик воситаларининг амалга оширилишининг тўлиқлиги ва етарлилиги кўрилади.

Лойиҳагача текшириш аудитнинг энг кўп меҳнат талаб қиладиган варианты ҳисобланади. Бундай аудит ахборот ресурслари иловаларида корхона ташкилий тузилмасини ва ходимларнинг у ёки бу иловалардан фойдаланиш қондаларини таҳлил этишни кўзда тутди. Сўнгра иловаларнинг ўзи таҳлилланади. Ундан кейин бир сатҳдан иккинчи сатҳнинг фойдаланишдаги муайян хизматлар ҳамда ахборот алмашишга зарур бўлган хизматлар таҳлилланиши лозим. Сўнгра хавфсизликнинг ўрнатилган воситаларини таҳлиллаш билан тасаввур тўлдирилади.

Хавф-хатарларни таҳлиллаш 12.4-бўлимда батафсил кўрилган. Ахборот хавфсизлиги бузилганда лойиҳагача текшириш, хавф-

хатарларни таҳлиллаш билан биргаликда ахборот тизимидаги мавжуд хавф-хатарларни рутбалашга ва адекват чораларни ишлаб чиқишга имкон беради.

Тизимни лойиҳалаш. Ҳимояни ташкил этиш стратегияси нуктаи назаридан ресурсли ва сервисли ёндашиш фаркланади. Ресурсли ёндашишда тизим ресурслар тўплами сифатида кўрилади ва ахборот хавфсизлиги тизимнинг компонентлари бу ресурсларга боғланади. Ресурсли ёндашиш амалга оширилганида ахборотни химоялаш масаласи хизматлар тузилмасига кўшимча чеклашларсиз ечилади. Бу эса бир жинсли бўлмаган тизим шароитида мумкин эмас. Сервисли ёндашишда тизим фойдаланувчиларга тақдим этилувчи хизматлар тўплами каби талқин қилинади. Ҳозирги вақтда сервисли ёндашиш афзалроқ ҳисобланади, чунки у тизимда амалга оширилган хизматларга боғланади ва «ортикча» хизматларни рад этиш ҳисобига катор таҳдидларни истисно қилинишига имкон беради. Бу эса тизимни янада мантқан асосланган тизимга айлантиради. Айнан сервис ёндашиш хавфсизликнинг замонавий стандартлари, хусусан ISO/IEC 15408 асосида ётади.

Ахборот хавфсизлиги тизимни қуришнинг иккита асосий сценарийси мавжуд: маҳсулотли ва лойиҳали. Маҳсулотли сценарий (ёндашиш) доирасида аввал химоя воситалари тўплами танланади, уларнинг функциялари таҳлилланади, сўнгра функциялар таҳлили асосида ахборот ресурсларидан фойдаланиш сиёсати белгиланади.

Лойиҳага харажатлар нуктаи назаридан маҳсулотли сценарий энг арзон ҳисобланади. Ундан ташқари, ечимларнинг танқислиги шароитида кўпинча маҳсулотли ёндашиш ягона ҳисобланади (масалан, криптографик химояда фақат шу ёндашиш қўлланилади).

Лойиҳали сценарийда аввал хавфсизлик сиёсати ишлаб чиқилади, унинг асосида хавфсизлик сиёсатини амалга оширишда зарур бўлган функциялар аниқланади, сўнгра бу функциялар бажарилишини таъминловчи химоя воситалари танланади.

Лойиҳали сценарий асосида қурилган тизимлар яхшироқ оптимизацияланган ва аттестациянинг юқори натижаларини беради. Ушбу ёндашиш маҳсулотли ёндашишдан фаркли равишда бошидан у ёки бу платформа билан боғланмаганлиги туфайли, катта гетероген тизимларни қуришда афзал ҳисобланади. Ундан ташқари, узок муддатга мўлжалланган ечимларни таъминлайди, чунки хавфсизлик сиёсатини ўзгартирмасдан ечимларни ва химоя воситаларини алмаштиришга имкон беради.

Ахборот хавфсизлиги тизими архитектурасини танлаш нуктаи назаридан объектли, татбикий ёки аралаш ёндашишдан фойдаланилади. Объектли ёндашиш ахборот хавфсизлигини у ёки бу объект (бўлинма, филиал, ташкилот) тузилмаси асосида яратади. Объектли ёндашишнинг кўлланиши ташкилий чораларнинг бир жинсли тўпламини мададловчи хавфсизлик механизмлари учун универсал ечимлар тўпламидан фойдаланишни кўзда тутади. Бундай ёндашишга мисол тарикасида ташки ахборот алмашиш, локал тармоқ, телекоммуникация тизимларининг ва х. химояланган инфратузилмаларини куришни кўрсатиш мумкин. Объектли ёндашишнинг камчилиги унинг универсал механизмларининг, айникса, ўзаро мураккаб боғланишли катта сонли иловаларга эга бўлган ташкилотлар учун тугал эмаслиги.

Татбикий ёндашиш хавфсизлик механизмини муайян иловага боғлаб яратади. Татбикий ёндашишга мисол тарикасида автоматлаштиришнинг алоҳида масаласи (бухгалтерия, кадрлар ва х.) учун қисм тизимларнинг химоясини кўрсатиш мумкин. Ушбу ёндашишнинг камчилиги – маъмурлаш ва ишлатиш харажатларини минималлаштириш мақсадида хавфсизликнинг турли воситаларини уйғунлаштириш зарурияти.

Аралаш ёндашиш юкорида тавсифланган иккита ёндашишни комбинациялашни кўзда тутади. Бундай ёндашиш лойиҳалаш босқичида кўпроқ меҳнат галаб қилсада, ахборот хавфсизлиги тизимини жорий этиш ва ишлатиш нархи бўйича афзалликларни бериши мумкин.

Жорий этиш. Жорий этиш босқичи қуйидаги кетма-кет ўтказилувчи тадбирларни ўз ичига олади:

- химоя воситаларини ўрнатиш ва конфигурациялаш;
- ходимларни химоя воситалари билан ишлашга ўргатиш;
- дастлабки синовни ўтказиш;
- тажрибавий ишлатишга топшириш.

Тажрибавий ишлатиш, ахборот хавфсизлиги тизимини ишчи режимига туширишдан аввал, унинг ишлашидаги мумкин бўлган камчиликларни аниқлашга ва йўқотишга имкон беради. Агар тажрибавий ишлатиш жараёнида компонентларнинг тўғри ишламаслиги фактлари аниқланса, химоя воситалари созланишига ва уларнинг ишлаш режимларига ва х. тузатишлар киритилади.

Тизимни аттестациялаш. Ахборот хавфсизлиги тизимини ваколатли идора томонидан аттестациялаш унинг функционал

тўлиқлигини ва корпоратив ахборот тизими химоясининг талаб қилинган даражаси таъминланганлигини тасдиқлашга имкон беради. Тизимнинг аттестацияси хавфсизлик аудитининг бир кўриниши ҳисобланади ва ишлатилувчи чоралар комплекси ва химоя воситаларининг хавфсизлик даражаси талабларига мослигини баҳолаш мақсадида химояланувчи корxonани ишлатишнинг реал шароитларида комплекс текширишни кўзда тутлади.

Аттестация натижасида ҳисобот ҳужжати тайёрланади ва мослик аттестати берилади. Бу аттестат конфиденциал ахборот билан аттестатда кўрсатилган вақт мобайнида ишлаш ҳуқуқини беради.

Кузатиш. Ахборот хавфсизлиги тизимининг ишга лаёқатлигини ва ўз вазифаларини текис бажарилишини мададлаш учун хавфсизлик тизимининг дастурий ва аппарат таъминотини техник мададлаш ва кузатиш бўйича тадбирлар комплекси кўзда тутилиши лозим. Ахборот хавфсизлиги тизимини техник мададлаш ва кузатиш хизматчи ходимларнинг билими ва кўникмаларини талаб этади ва химояланувчи тизим эгаси – ташкилот штатидаги ахборот хавфсизлигига жавоб берувчи ходимлар томонидан ёки ихтисослаштирилган ташкилот ходимлари томонидан амалга оширилиши мумкин.

Кўрилган методология қоидаларидан фойдаланиш корпоратив ахборот тизимининг умумий ривожини билан бирга ривожлантирилиши ва модификацияланиши мумкин бўлган ахборот хавфсизлигининг самарали ва ишончли тизимини куришга имкон беради.

ФҲЙДАЛАНИЛГАН АДАБИЁТЛАР

1. С.С.Қосимов. Ахборот технологиялари. Ўқув кўлланма. – Т., Алоқачи, 2006.
2. С.К.Ғаниев, М.М. Каримов. Ҳисоблаш системалари ва тармоқларида информация химояси. Олий ўқув юрт.талаб. учун ўқув кўлланма. – Т., Давлат техника университети, 2003.
3. В.И. Завгородний. Комплексная защита информации в компьютерных системах: Учебное пособие. –М: Логос; ПБОЮЛ Н.А.Егоров, 2001.
4. Г.Н. Устинов. Основы Информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». –М.: СИНТЕГ, 2000.
5. Мерит Максим, Девид Поллино. Безопасность беспроводных сетей. Информационные технологии для инженеров. –М., 2004.
6. А. Соколов, О. Степанюк. Защита от компьютерного терроризма. Справочное пособие. БХВ-Петербург. Арлит, 2002.
7. А.М. Астахов. Аудит безопасности информационных систем. //Конфидент. – 2003. – №1,2.
8. А.В. Беляев. Методы и средства защиты информации // http://www.citforum.ru/internet/infsecure/its2000_01.shtml.
9. Вэк Дж., Карнахан Л. Безопасность корпоративной сети при работе с Интернетом. Введение в межсетевые экраны //Конфидент. – 2000. – №4-5.
10. А. Галатенко. Активный аудит//JetInfo. –1999. –№8.
11. А.В. Лукацкий. Адаптивная безопасность сети// Компьютер-Пресс. – 1999. – №8.
12. А.В. Лукацкий. Обнаружение атак.– СПб.: БХВ-Петербург, 2001.
13. Р.Норман. Выбираем протокол VPN//Windows 2000 Magazine. –2001. –№7.
14. В.Г. Олифер. Защита информации при работе в Интернет// Connect. – 2002. –№11.

15. Н.А. Олифер. Дифференцированная защита трафика средствами IPsec //LAN.-2001.-№04; <http://www.osp.ru/lan/2001/04/024.htm>.

16. Н.А. Олифер. Протоколы IPsec. //LAN.-2001.-№03; <http://www.osp.ru/lan/2001/03/024.htm>.

17. С.А. Петренко. Построение эффективной системы антивирусной защиты // Конфидент.-2002.-№3.

18. С.А. Петренко. Централизованное управление антивирусной защитой корпоративных сетей Internet/Intranet // Конфидент.-2001.-№2.

19. А.А. Петров. Компьютерная безопасность. Криптографические методы защиты. –М.: ДМК Пресс, 2000.

20. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Уч.пособие для ВУЗов/ Авт.: П.Ю. Белкин и др. –М.: Радио и связь, 1999.

21. Н. Прокофьев. Антивирусная защита сети // Компьютер – Пресс.-2001. –№12.

22. Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. Защита информации в компьютерных системах и сетях: 2-е изд., перераб. и доп. – М.: Радио и связь, 2001.

23. С.В. Симонов. Анализ рисков в информационных системах. Практические советы // Конфидент. -2001. -№2.

24. А.В. Соколов, В.Ф. Шаньгин. Защита информации в распределенных корпоративных сетях и системах. –М.: ДМК Пресс, 2002.

25. Типовые решения по применению средств VPN для защиты информационных ресурсов / ООО «Конфидент». –СПб., 2001.

26. Типовые решения по применению технологии межсетевых экранов для защиты информационных ресурсов / ООО «Конфидент». –СПб., 2001.

27. Типовые решения по применению технологии централизованного управления антивирусной защитой предприятия/ ООО «Конфидент». –СПб., 2002.

28. «Ахборот технологияси. Маълумотларни криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари». Ўзбекистон Давлат стандарти. О`з DSt 1092:2005.

29. «Ахборот технологияси. Ахборотларни криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми». Ўзбекистон Давлат стандарти. O'zDSt 1105:2006.

30. «Ахборот технологияси. Ахборотларни криптографик муҳофазаси. Хэшлаш функцияси». Ўзбекистон Давлат стандарти. O'zDSt 1106:2006.

31. «Ахборот технологияси. Очик тизимлар ўзаро боғлиқлиги. Электрон рақамли имзо очик калити сертификати ва атрибут сертификатининг тузилмаси». Ўзбекистон Давлат стандарти. O'zDSt 1108:2006.

32. «Ахборот технологиялари. Ахборот хавфсизлиги. Атамалар ва таърифлар». Ўзбекистон Давлат стандарти. O'z DSt ISO/IEC 2382-8:2007.

33. www.nasa.gov/statistics/

34. www.security.uz

35. www.cert.uz

36. www.uzinfocofm.uz

Қисқартirilган сўзлар

ACK	Acknowledgement – тасдиқлаш
AES	Advanced Encryption Standard – американинг янги шифрлаш стандарти
AH	Authentication Header – аутентификацияловчи сарлавҳа
ANS	Adaptive Network Security – хавфсизликни адаптив бошқариш модели
ANSI	American National Standard Institute – АҚШнинг миллий стандартлаштириш институти
AS	Authentication Server – аутентификациялаш сервери
ASA	Adaptive Security Algorithm – хавфсизликнинг адаптив алгоритми
ASP	Applications Service Providing – серверда истеъмолчидан масофада жойлашган иловаларга Internet ёки хусусий тармоқ орқали хизмат кўрсатиш
B2B	Business to Business – «бизнес-бизнес» схемаси
B2C	Business to Consumer – «бизнес – истеъмолчи» схемаси
CA	Certification Authorities – сертификациялаш маркази
CEK	Content Encryption Key – маълумотларни шифрлаш калити
CHAP	Challenge Handshake Authentication Protocol – «кўл узатиш» муолажаси асосида аутентификациялаш протоколи
DDoS	Distributed Denial of Service – хизмат кўрсатишдан бош тортишга ундайдиган тақсимланган ҳужум
DHCP	Dynamic Host Configuration Protocol – хостларни динамик конфигурациялаш протоколи
DNS	Domain Name Server – доменли исмлар хизмати
e business	electronic business – электрон бизнес
e commerce	electronic commerce – электрон тижорат
ESP	Encryption Control Protocol – шифрлашни бошқариш протоколи
ESP	Encapsulated Security Payload – киритилган узатиладиган химоялаган маълумотлар
FTP	File Transfer Protocol – файлларни узатиш протоколи

GSM	Global System for Mobile Communications – мобилъ алоканинг глобал тизими
GSP	Global Security Policy – VPN учун глобал хавфсизлик сиёсати
HDLC	High level Data Link Control – юкори сатҳдаги маълумотларни узатиш каналини бошқариш
HMAC	Hashing for Message Authentication – калитларни хэшлаш орқали хабарларни аутентификациялаш
HTML	HyperText Markup Language – Web-саҳифаларни гиперматнни белгиловчи тил
HTTP	HyperText Transfer Protocol – гиперматнли файлларни узатиш протоколи
ICMP	Internet Control Message Protocol – Internet тармоғида хабарларни бошқариш протоколи
IETF	Internet Engineering Task Force – Internetни лойиҳалаш муаммолари гуруҳи
IKE	Internet Key Exchange – Internetда калитларни алмашиш протоколи
IP	Internet Protocol – тармоқлараро маълумотларни алмашинишнинг Internet протоколи
IPSec	Internet Security Protocol – тармоқлараро маълумотларни хавфсиз алмашиниш Internet протоколи
IRC	Internet Relay Chat – Internet да чат-анжуманларни ташкил этиш хизмати
ISO	International Standards Organization – халқаро стандартлаштириш ташкилоти
ISP	Internet Service Provider – Internet хизматларини таъминотчиси
KDC	Key Distribution Center – калитларни тақсимлаш маркази
KEK	Key Encryption Key – калитларни шифрлаш учун калит
KS	Kerberos Server – kerberos тизими сервери
L2F	Layer2 Forwarding – иккинчи (канал) сатҳда маълумотларни узатиш протоколи
L2TP	Layer2 Tunneling Protocol – канал сатҳида маълумотларни туннеллаш протоколи
LAC	L2TP Access Concentrator – L2TP руҳсатлар концентратори
LAN	Local Access Network – маҳаллий тармоқ
LCP	Link Control Protocol – уланишларни бошқариш

LDAP	Lightweight Directory Access Protocol – каталоглардан фойдаланишларни соддалаштирилган протоколи
LNS	L2TP Network Server – L2TP тармоқ сервери
LSP	Local Security Policy – маҳаллий хавфсизлик сиёсати (мижоз учун)
MAC	Message Authentication Code – хабарларни аутентификациялаш коди
MD	Message Digest – хабарлар дайджести
NAT	Network Address Translation – тармоқ манзилларини трансляциялаш
NCP	Network Control Protocol – Тармоқни бошқариш протоколи
NIST	National Institute of Standards and Technology – АҚШнинг стандартлар ва технологиялари миллий институти
NNTP	Network News Transfer Protocol – тармоқ янгиликларини узатиш протоколи
OSI	Open Systems Interconnection – очик тизимлар ўзаро боғлиқлиги
ОТК	One Time Key – Бир маротабалик калит.
P2P	Peer to Peer или Partner to Partner – бизнес муносабатининг «тенг-тенг» схемаси
PAP	Password Authentication Protocol – парол бўйича аутентификациялаш протоколи
PIN	Personal Identification Number – шахсий идентификация коди
PKD	Public Key Directory – очик калитлар каталоги
PKI	Public Key Infrastructure – очик калитларни бошқариш инфратузими
PPP	Point to point Protocol – икки нуктали боғланиш протоколи
PPTP	Point to Point Tunneling Protocol – икки нуктали боғланиш учун туннеллаш протоколи
POP	Post Office Protocol – фойдаланувчи ўзига келган электрон хабарлардан фойдаланишига имкон берувчи протокол
RADIUS	Remote Authentication Dial In User Service – фойдаланувчиларни боғланадиган линиялар бўйича масофадан аутентификациялаш тизими
RAS	Remote Access Service – масофадан фойдаланаш хизмати
RFC	Request For Comments – изоҳларни сўрови

RMON	Remote MONitoring – тармок ускуналарини масофадан мониторинглашнинг стандарт спецификацияси
RSA	Rivest, Shamir, Adleman – Райвест, Шамир, Адлеман. Асимметрик криптоалгоритм
SHA	Secure Hash Algorithm – химояланган хэшлаш алгоритми
SKIP	Simple Key management for Internet Protocols – internet протоколи учун калитларни оддий бошқариш
SMTP	Simple Mail Transfer Protocol – электрон почтанин оддий протоколи
SNMP	Simple Network Management Protocol – тармокни бошқаришнинг оддий протоколи
SPD	Security Policy Database – хавфсизлик қоидаларининг маълумотлар базаси
TACACS	Terminal Access Controller Access Control System – Масофадан фойдаланишни марказлаштирилган назоратлаш протоколи
TCP	Transport Control Protocol – узатишларни бошқариш протоколи
TELNET	Виртуал терминал протоколи – масофадаги компютерда дастурни бажаришга мўлжалланган протокол
TFN	Tribble Flood Net – DDoS хужумлар учун инструментал воситалардан бири
TGS	Ticket Granting Server – мандатларни таркатиш сервери
TLS	Transport Layer Security – транспорт сатҳининг химояси
UDP	User Data Protocol – фойдаланувчининг маълумотларини узатиш протоколи
VPN	Virtual Private Network – химояланган виртуал тармок
WAN	Wide Area Network – глобал тармок
WWW	World Wide Web – Интернетнинг гиперматнли ахборотлар хизмати
XML	Extended Mark-up Language – белгилашнинг кенгайтирилган тили
МББТ	Маълумотлар базасини бошқариш тизими

С.ҒАНИЕВ, М.КАРИМОВ, К. ТАШЕВ

АХБОРОТ ХАВҒСИЗЛИГИ

**(АХБОРОТ-КОММУНИКАЦИОН ТИЗИМЛАР
ХАВҒСИЗЛИГИ)**

Тошкент - «АЛОҚАСИ» - 2008

Мухаррир: М.Миркомиллов

Тех.мухарири: А.Мойдинов

Мусаххиха: Г.Каримова

Комп. саҳифаловчи: Г.Арифходжаева

Босишга рухсат этилди 00.05.2008 йил. Бичими 60x84 ¹/₁₆.
«Times Uz» гарнитураси. Офсет усулида босилди.
Шартли босма табоғи 24,5. Нашр табоғи 24,0. Адади 1000.
Бюртма № 237.

«Aloqachi matbaa markazi» босмахонасида чоп этилди. 700000,
Тошкент шаҳри, А.Темур, 108-уй.

