

**Ғаниев 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 маҳсус таълим вазирлиги томонидан  
техника олий ўқув юртлари бакалавриат босқиччи  
талабалари учун ўқув қўлланма сифатига тавсия  
этилган*

**Фаниев Салим Каримович, Каримов Мажид Маликович,  
Ташев Комил Ахматович.** Ахборот хавфсизлиги. Ахборот-  
коммуникацион тизимлар хавфсизлиги. Ўкув кўлланма Т., «Aloqachī»,  
2008, 382 бет.

Ушбу кўлланма компьютер тармоқлари ва корпоратив ахборот тизимларини яратища ва ишлатища ахборотни химоялашнинг долзарб муаммоларига багишланган. Компьютер тармоқлари ва тизимларига таҳдид хиллари ҳамда локал ва корпоратив тармоқларни Internet-атакалардан химоялаш усуллари ва воситалари мухокама этилади. Электрон бизнес ва электрон тижоратда ахборот хавфсизлигини тъминлаш муаммосига алоҳида ўтибор берилади. Ахборот хавфсизлиги концепцияси таърифланади ва тармоқларда хавфсизлик сиёсати аникланади.

Маълумотларни химоялаш технологияси, тармоқ хавфсизлигинг базавий технологияси, сукилиб киришларни ва тармоқ хавфсизлигини бошқариш таҳлилланади. Хусусан, ахборотни замонавий криптографик химоялаш воситаларининг принциплари, алгоритмлари ва протоколлари кўрилади; тармоқларо экранларнинг турли хиллари гавсифланади ва уларни ишлатиш бўйича тавсиялар берилади; Internet хилидаги глобал очик тармоқларнинг очик коммуникациялари оркали криптохимояланган виртуал туннелларни шакллантириш усуллари ва воситалари мухокама этилади; корхона ахборот ресурсларидан масоғадан хавфсиз фойдаланишни тъминлаш 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 тизимиń куриш методологияси таърифланади.

Кўлланма олий ўкув 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 лиц, 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-инжениринг» ИТИ етакчи илмий ходими, т.ф.д., проф;  
проф. **Орипов М.М.** – Мирзо Улугбек номли Ўзбекистон Миллий университети «Информатика ва татбикӣ дастурлаш» кафедраси мудири, физика-математика фанлари доктори.

**ISBN 978-9943-326-20-0**

© «ALOQACHI», 2008

# МУНДАРИЖА

<b>МУҚАДДИМА.....</b>	<b>14</b>
<b>/ боб. АХБОРОТ ХАВФСИЗЛИГИГА ТАҲДИДЛАР</b>	
1.1. Ахборот урушилар ва киберхужумлар .....	17
1.2. Ахборот-коммуникацион тизимлар ва тармокларда таҳдидлар ва заифликлар .....	22
1.3. Компьютер жиноятчилигининг таҳлили .....	25
1.4. Тармокдаги ахборотга бўладиган намунавий хужумлар ..	28
1.5. Ахборот хавфсизлигини бузувчининг модели .....	32
1.6. Internet – хизматлар ва электрон бизнес тизимларида хавфсизлик-муаммолари .....	36
<b>II боб. АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ АСОСИЙ ЙЎЛЛАРИ</b>	
2.1. Ахборотни химоялаш концепцияси .....	43
2.2. Ахборот химоясининг стратегияси ва архитектураси .....	46
2.3. Ахборот хавфсизлигининг сиёсати .....	48
2.4. Ахборот-коммуникацион тизимлар ва тармоклар хавфсизлигига кўйиладиган талаблар .....	53
<b>III боб. АХБОРОТ ХАВФСИЗЛИГИНИНГ ҲУҚУКИЙ ВА ТАШКИЛИЙ ТАЪМИНОТИ</b>	
3.1. Ахборот хавфсизлиги соҳасида ҳуқукий бошқариш .....	59
3.2. Ахборот хавфсизлигининг ташкилий-маъмурӣ таъминоти .....	61
3.3. Ахборот хавфсизлиги бўйича стандартлар ва спецификациялар .....	65
<b>IV боб. АХБОРОТНИ ХИМОЯЛАШНИНГ КРИПТОГРАФИК УСУЛЛАРИ</b>	
4.1. Криптографиянинг асосий қоидалари 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 ракамли имзо .....	102
4.7. Криптографик калитларни бошқариш .....	107
<b>V боб. ИНДЕНТИФИКАЦИЯ ВА АУТЕНТИФИКАЦИЯ</b>	
5.1. Асосий тушунчалар ва туркумланиши .....	115
5.2. Пароллар асосида аутентификациялаш .....	120
5.3. Сертификатлар асосида аутентификациялаш .....	125
5.4. Катъий аутентификациялаш .....	128

5.5. Фойдаланувчиларни биометрик идентификациялаш ва аутентификациялаш .....	147
<b>VI боб. ТАРМОҚЛАРАРО ЭКРАН ТЕХНОЛОГИЯСИ</b>	
6.1. Тармоқлараро экранларнинг ишлаш хусусиятлари .....	153
6.2. Тармоқлараро экранларнинг асосий компонентлари .....	163
6.3. Тармоқлараро экранлар асосидаги тармоқ химоясининг схемалари .....	174
<b>VII боб. ХИМОЯЛАНГАН ВИРТУАЛ ХУСУСИЙ ТАРМОҚЛАР</b>	
7.1. Химояланган виртуал хусусий тармоқларни куриш концепцияси .....	185
7.2. Химояланган виртуал хусусий тармоқларнинг туркумланиши .....	193
7.3. Химояланган корпоратив тармоқларни куриш учун VPN ечимлар .....	203
7.4. Канал ва сеанс сатхларда химояланган виртуал каналларни куриш .....	220
7.5. IPSec протоколлар стекини химояланган виртуал хусусий тармоқлар куришда ишлатилиши .....	245
<b>VIII боб. ОЧИҚ КАЛИТЛАРНИ БОШҚАРИШ ИНФРАТУЗИЛМАСИ РКИ</b>	
8.1. РКІнинг ишлаш принципи .....	255
8.2. Очік қалитларни бошқариш инфратузилмасининг мантикий түзилмаси ва компонентлари .....	265
<b>IX боб. АХБОРОТ-КОММУНИКАЦИОН ТИЗИМЛАРДА СҮКИЛИБ КИРИШЛАРНИ АНИҚЛАШ</b>	
9.1. Хавфсизликни адаптив бошқариш концепцияси .....	271
9.2. Химояланишни таҳлиллаш .....	275
9.3. Ҳужумларни аниклаш .....	279
9.4. Компьютер вируслари ва вирусдан химояланиш мұаммолари .....	288
9.5. Вирусга қарши дастурлар .....	297
9.6. Вирусга қарши ҳимоя тизимини куриш .....	305
<b>X боб. МАЪЛУМОТЛАРНИ УЗАТИШ ТАРМОҒИДА АХБОРОТНИ ҲИМОЯЛАШ</b>	
10.1. Маълумотларни узатиш тармоқларида ахборот ҳимоясини таъминлаш .....	309
10.2. Алока каналларида маълумотларни ҳимоялаш усууллари .....	312

# **ХІ боб. СИМСИЗ АЛОҚА ТИЗИМЛАРИДА АҲБОРОТ ХИМОЯСИ**

11.1. Симсиз тармок 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

## **ХІІ боб. ХАВФСИЗЛИКНИ БОШҚАРИШ ВА ХИМОЯ ТИЗИМИНИ ҚУРИШ**

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

# ОГЛАВЛЕНИЕ

<b>ПРЕДИСЛОВИЕ .....</b>	14
<b>I глава. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b>	
1.1. Информационные войны и кибератаки .....	17
1.2. Угрозы и уязвимости в информационно-коммуникационных 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
<b>II глава. ОСНОВНЫЕ ПУТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b>	
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
<b>III глава. ПРАВОВОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ</b>	
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
<b>IV глава. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ</b>	
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
<b>V глава. ИНДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ</b>	
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
<b><i>VI глава. ТЕХНОЛОГИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ</i></b>	
6.1. Особенности функционирования межсетевых экранов	153
6.2. Основные компоненты межсетевых экранов .....	163
6.3. Схема защиты сети на базе межсетевых экранов .....	174
<b><i>VII глава. ЗАЩИЩЕННЫЕ ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ</i></b>	
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
<b><i>VIII глава. ИНФРАСТРУКТУРА УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ РКИ</i></b>	
8.1. Принцип функционирования РКИ.....	255
8.2. Логическая структура и компоненты инфраструктуры управления открытыми ключами.....	265
<b><i>IX глава. ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ</i></b>	
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
<b><i>X глава. ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ</i></b>	
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 ПОСТРОНИЕ 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
<b>ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА .....</b>	375
<b>СПИСОК СОКРАЩЕНИЙ .....</b>	378

# CONTENTS

<b>INTRODUCTION .....</b>	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 AUTENTIFICATION</i>	
5.1. The basic concepts and classification.....	115
5.2. Authentification on the basis of passwords.....	120
5.3. Authentification on the basis of certificates.....	125
5.4. Strong authentification .....	128
5.5. Biometric identification and authentification users.....	147

<b><i>VI chapter. TECHNOLOGY OF GATEWAY SCREENS</i></b>	
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
<b><i>VII chapter. PROTECTED VIRTUAL PRIVATE NETWORKS</i></b>	
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
<b><i>VIII chapter. INFRASTRUCTURE OF MANAGEMENT OF THE PUBLIC KEYS PKI</i></b>	
8.1. Principle of functioning PKI .....	255
8.2. Logic structure and components of an infrastructure of management of the public keys.....	265
<b><i>IX chapter. DETECTION OF INTRUSIONS IN INFORMATION-COMMUNICATION SYSTEMS</i></b>	
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
<b><i>X chapter. PROTECTION OF THE INFORMATION IN NETWORKS OF DATA TRANSMISSION</i></b>	
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
<b><i>XI chapter. PROTECTION OF THE INFORMATION IN SYSTEMS OF WIRELESS COMMUNICATION</i></b>	
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
<b>THE USED LITERATURE .....</b>	<b>375</b>
<b>THE LIST OF REDUCTIONS .....</b>	<b>378</b>

## МУҚАДДИМА

Илдам кадамлар билан ривожланаётган компьютер ахборот технологиялари хаётимизда сезиларли ўзгаришларга сабаб бўлмоқда. «Ахборот» тушунчаси сотиб олиш, сотиш, бирор нарсага алмashiш ва х. мумкин бўлган маҳсус 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 харакатлардан химоялаш заруриятининг пайдо бўлиши табиийдир.

Ахборотни химоялаш муаммоси компьютер тизимлари ва тармоклари 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 ўкув адабиётларда етарлича ўз аксини топмаган.

Ўкувчи эътиборига ҳавола этилаётган китоб ахборот-коммуникацион тизимлар ҳавфсизлигига бағишлиган ва 12 та бобдан иборат.

Китобнинг I бобида ахборот ҳавфсизлигининг хозирги ҳолатига баҳо берилади. Компьютер жиноятчилиги таҳлил этилиб, тармок ахборотига бўладиган намунавий хужум усуллари келтириллади ҳамда ахборот ҳавфсизлигини бузувчининг модели тавсифланади. Шунингдек, бу бобда Internet – хизматлари ва электрон бизнес тизимларида ҳавфсизлик муаммолари кўрилган.

Ахборот ҳавфсизлигининг асосий тушунчалари, ҳавфсизликни таъминлашнинг амалда текширилган принциплари ҳамда ҳавфсизлик сиёсатини яратиш жараёни тавсифи китобнинг II бобида келтирилган. Шу билан бирга ахборот-коммуникацион тизимлар ва тармоклар ҳавфсизлигига кўйиладиган талаблар ва ахборот ҳавфсизлигини таъминловчи чоралар хусусида сўз юритилган.

Ахборот ҳавфсизлигининг ҳукукий ва ташкилий таъминоти, ҳавфсизликнинг ҳалқаро ва миллий ҳукукий месъёрлари китобнинг III бобида баён этилган.

Китобнинг IV боби ахборотни химояланганинг криптографик усууларига бағищланган бўлиб, маълумотларни шифрлашнинг блокли симметрик алгоритмлари, жумладан, АҚШнинг янги стандарти AES таҳлил этилган ва миллий стандартимиз ёритиб ўтилган. Замонавий асимметрик криптотизимлар мухокама этилиб, хэшлаш функцияларининг асосий хусусиятлари ва ишлатилиш соҳалари аниқланган. Рақамли имзони генерациялаш ва текшириш муолажалари кўрилган. Калитларни бошкариш – калитларни тақсимлаш жараёнига алоҳида эътибор килинган.

Тизимнинг фойдаланувчилар билан ўзаро алокасидаги асосий жараёнлар – фойдаланувчи ҳаракатини аутентификациялаш, авторизациялаш ва маъмурлаш, кўп ва бир маротабали пароллар хамда ракамли сертификатлар асосидаги аутентификациялаш хусусиятларининг таҳлили китобнинг V бобида ёритилган. Фойдаланувчини идентификациялаш ва аутентификациялашнинг намунавий схемалари кўрилган. Симметрик ва асимметрик криptoалгоритмларга асосланган катъий аутентификациялашга алоҳида эътибор берилган. Аугентификациялашнинг Kerberos протоколи мухокама этилган. Биометрик идентификациялаш ва аутентификациялаш восита-лари тавсифланган.

Тармоқларо экранларнинг функциялари таҳлили, уларнинг OSI моделининг турли сатҳларида ишлаши хусусиятлари мухокамаси, тармоқларо экранлар асосида тармоқни химоялаш схемалари, щахсий ва тақсимланган тармоқ экранларининг ишлатилиши VI бобда кўрилган.

Химояланган виртуал хусусий тармоқларни куриш концепцияси ва уларнинг асосий хусусияти – туннеллаш, виртуал химояланган каналларни куриш вариантлари таҳлили, химояланган виртуал хусусий тармоқларнинг катор аломатлари бўйича туркумланиши, VPN технологиянинг корпоратив ахборот тизимлари ва тармоқларида кўлланилишининг техник ва иктисадий афзалликлари, OSI очик тизимлар ўзаро алоқа эталон моделининг канал ва сеанс сатҳларида химояланган виртуал каналлар курилишининг муаммолари мухокамаси, IPSec протоколлар стекининг архитектураси, уларнинг химояланган хусусий тармоқлар куришда ишлатилиши масалалари китобнинг VII бобидан ўрин олган.

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

Ахборот хавфсизлигини адаптив бошқаришнинг долзарб муаммолари, корпоратив тармок хавфсизлигини адаптив бошқариш концепцияси тавсифи, химояланишни таҳлиллашнинг технологиялари ва воситалари батафсил мухокама этилиб, тармок ахборотини таҳлиллаш усууллари, хужумларни аниқлаш тизимларининг компонентлари ва архитектураси китобнинг IX бобида ўз аксини топган. Шу билан бир каторда компьютер вирусларидан химояланишнинг долзарб муаммолари хам ушбу бобдан ўрин олган. Компьютер вирусларининг туркумланиши келтирилган, вирус хаёт цикли боскичлари таҳлилланган, вируслар ва бошка заар келтирувчи дастурларнинг асосий тарқалиш каналлари кўрилган. Вирусга карши дастурларнинг асосийлари мухокама этилиб, вирусга қарши химоя тизимини куриш масаласи ёритилган.

Маълумотларни узатиш тармоғида ахборотни химоялаш муаммоси, маълумотларни узатиш тармоғи компонентларига ва архитектурасига реал таъсир этувчи функционал, архитектуравий ва бошқариш (маъмурий) талаблари хамда алока каналларида маълумотларни химоялаш усуулларининг мухокамаси X бобда ёритиб ўтилган.

Симсиз алока тизимларида ахборот химоясининг долзарб масалаларига бағищланган муаммолар XI бобда келтирилган бўлиб, унда симсиз тармок концепцияси ва тузилмаси кўрилган. Симсиз тармок хавфсизлигига таҳдидлар батафсил таҳлил этилиб, симсиз тармок хавфсизлиги протоколлари мухокама этилган. Симсиз курилмалар хавфсизлиги муаммолари хам ушбу бобдан ўрин олган.

Китобнинг XII боби тармок хавфсизлиги воситаларини бошқариш усуулларига бағищланган. Ахборот тизимларини бошқаришнинг кенг таркалган методологияси ITIL тавсифланган. Корхона микёсида ахборотни химоялаш тизимини бошқариш масаласи таърифланган. Хавфсизликни марказлаштирилган бошқаришнинг глобал ва локал хавфсизлик сиёсатига асосланган истиқболли архитектурасига алоҳида эътибор берилган. Ахборот тизимлари хавфсизлигининг аудити ва мониторинги кўрилган. Хавфхатарларни таҳлиллаш ва бошқариш муаммоси хамда тармок хавфсизлик тизимини куриш методологияси тавсифланган.

Кўлланмани тайёрлашда якиндан ёрдам берган (VII ва XI боблар) техника фанлари номзоди А.А. Фаниевга, такризчиларга хамда ўкув кўлланма ҳакидаги барча фикр мулоҳазалари учун хурматли китобхонларга муаллифлар ўз миннатдорчиликларини изхор этадилар.

## МУАЛЛИФЛАР

## 1.1. Ахборот урушлар ва киберхужумлар

Хавфсизлик – хар куни биз тўқнашадиган ҳаётимизнинг жихати: эшикни қулфлаймиз, кимматбаҳо нарсаларни бегона кўзлардан беркитамиз ва ҳамённи дуч келган жойда қолдирмаймиз. Бу «ракамли дунёга» ҳам расм бўлиши шарт, чунки хар бир фойдаланувчининг компютери карокчи хужуми объекти бўлиши мумкин.

Тижорат ташкилотлари хавфсизликни таъминлаш ўзининг биринчи галдаги вазифаси эмас, балки уни таъминлашга сарф этиладиган ҳаражатларни муқаррар боло деб ҳисоблаб келгандар. Қандайдир даражада бу «оқилона иш»: нихоят, усиз ҳам иш бажаришда тўсиклар тўлиб-тошиб ётибдику?! Аммо фирманинг барча корпоратив биноларига кеча-кундуз киришга рухсат беришга журъят этувчи акли жойида «саноат капитанлари»ни кўрганмисиз? Албатта, йўқ! Ҳатто кичкина компания биносининг кириш йўлида сизни коровул ёки киришни чегараловчи ва назоратловчи тизими карши олади. Ахборотни химоялаш эса ҳали кўнгилдагидек эмас. Ахборотни қандай йўқотиш мумкинлигини ва бу қандай оқибатларга олиб келишини барча ҳам тушунавермайди.

Йирик ўйинчилар яхшигина сабок олдилар: хакерлар Yahoo.com, Amazon.com каби компанияларга ва ҳатто космик тадқиқот агентилиги NASAга катта зарар етказдилар. Хавфсизлик хизмати бозорининг энг йирик номоёндаларидан бири RSA Security, хар қандай таҳдидга карши чора борлиги хусусидаги ўйламасдан килган баёнотидан бир неча кундан кейин, хужумга дучор бўлди [33].

Одатда, одамлардан ёки предметлардан чиқадиган ва зарар етказдиган таҳдидлар куйидаги синфларга бўлинади: ички ёки ташки ва тузилмаланган (маълум объектга карши) ёки тузилмаланмаган («кимга Худо беради» кабилида манзилланувчи). Масалан, компютер вируслари «ташки тузилмаланмаган таҳдидлар» сифатида туркумланади ва тамомила оддий ҳисобланади. Қизиги

шундаки, фойдаланувчилар ўзининг компьютерини муайян нишон деб хисобламайдилар, улар ўзларини яхшигина химоялангандек сезадилар. Керакли химоя даражаси аксарият ҳолларда ишингизнинг холатига боғлик. Агар ташкилотингиз ёки компаниянгиз кандайдир тазик нишони бўлса, агар сиз миллий энергетик ресурсларни тақсимловчи ёки миллий алоқа тармокларига хизмат килувчи давлат инфратузилмаси таркибида бўлсангиз, оддий терористлар бомбаларини ва пистолетларини четга кўйиб, 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 преискурантлардан фойдаланиш максадида кирувчи ракиблар, Web-сайтингизни таъмагирлик максадида бузувчилар ва шунга ўхшашлар тўғрисида қайгуришингизга тўғри келади.

Аммо, вахимага 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 бокувчингиз-шахсий компьютер хавфсизлигини таъминлашга озгина вакт сарф қилмайсиз? Бу нафақат аппарат воситаларига, балки маълумотларга ҳам таалукли. Маълумотларни ўғирлатиш ёки йўқотиш катта, баъзида, тузатиб бўлмайдиган зарар келтиради.

Маълумки, тизим маъмурлари барча маҳфий материаллардан фойдаланиш имконига эга ва, одатда, компания фойдасидан ўз улушларига эга эмаслар. Шу сабабли худди улар ташкилот хавфсизлигига таҳдид сола олувчилар ичida энг каттаси хисобланадилар. Таъкидлаш лозимки, компания ишга кирувчиларни синчиклаб текширади. Худди шундай, хавфсизлик хизматини таъминловчиларга, айникса, маслаҳат бериш. режалаштириш ва мұмурлашни тавсия этувчиларга диккат билан караш лозим.

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

миз, холос. Жамоятимизнинг ахборотлашиши ягона дунё ахборот маконининг яратилишига олиб келадики, бу макон доирасида ахборотни йигиш, 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 айникса, ишлаб чиқаришда ва бошқаришда янги технологияларнинг қўлланилиши сўзсиз фойдалидир. Аммо, саноатнинг тезликда рифожланиши Ер экологиясига таҳдид сола бошлади, ядро физикаси соҳасидаги ютуклар 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 кандай фандагидек урушда ўзининг тарихи, ўзининг коидаси, машхур намоёндалари, ўзининг методологияси пайдо бўлди.

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

Турли мамлакатларнинг ҳарбий доктриналарида электрон курол ривожи режалари ва маҳсус вазифаларга мўлжалланган дастурий таъминот тўғрисида эслатишлар кўзга ташланмокда. Турли разведка манбаларидан келаётган ахборотнинг тахлили натижасида хулоса қилиш мумкинки, баъзи бир давлатларнинг раҳбарлари ҳужумкор кибер-дастурларни яратишни молияламоқдалар.

Ахборот урушига оддий воситалар ёрдамида ҳарбий харакатлар самара бермайдиган ҳолларга нисбатан стратегик альтернатива сифатида қаралмокда.

Ҳарбийлар томонидан киритилган *ахборот уруши* атамаси реал, кирғинли ва емирувчи ҳарбий харакатлар билан боғлик шафқатсиз ва хавфли фаолиятни англатади. Бу урушнинг алоҳида кирралари-штаб уруши, электрон уруши, психологик амаллар ва х.

Ҳар кандай уруш, ахборот уруши шу жумладан, замонавий курол ёрдамида олиб борилади. Ахборот куроли ёрдамида, уруш олиб борилувчи барча куроллардан фарқли ўлароқ, зълон килинмаган ва кўпинча дунёга кўринмайдиган урушларни олиб бориш мумкин (олиб борилмокда ҳам). Бу куролнинг таъсир объектлари – иқтисодий, сиёсий, ижтимоий ва х. каби жамият ва дав-

лат институтлари. Маълумотларни узатиш тармокларининг кела-жак жанглар майдонига айланиши аллақачон эътироф этилган.

Ахборот қуроли ҳужумда ва мудофаада «электрон тезлик» билан ишлатилиши мумкин. У энг илғор технологияларга асосланган бўлиб, ҳарбий низоларни дастлабки боскичида ҳал этилишини таъминлайди ҳамда умуммақсад кучларнинг кўлланилишини истисно қиласди. Ахборот қуроли қўлланишининг стратегияси ҳужумкор характерга эга. Аммо хусусий заифлик нуткаи назари мавжуд, айникса фуқаролик секторида. Шу сабабли бундай қуролдан ва ахборот терроризмидан химояланиш муаммоси ҳозирда биринчи ўринга чиккан. Фойдаланувчиларига дунё тармокларида ишлашни таъминловчи мамлакатларнинг миллий ахборот ресурсларининг заифлиги – ҳар икки томонга ҳавфли нарса.

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

Ҳозирда ҳужумкор ахборот қуроли сифатида қўйидагиларни кўрсатиш мумкин:

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

- *мантиқий бомбалар* – сигнал бўйича ёки ўрнатилган вактда ҳаракатга келтириш мақсадида ҳарбий ёки фуқаро инфратузилмаларига ўрнатилувчи дастурланган қурилмалар;

- *телекоммуникация тармоқларида ахборот алмашинувини бостириш воситалари*, давлат ва ҳарбий бошқарув каналларида ахборотни соҳталашибтириш;

- *тестли дастурларни бетарафлашибтириш воситалари*;
- объект дастурий таъминотига айғоқчилар томонидан атайн киритилувчи турли хил ҳатоликлар.

Универсаллик. маҳфийлик, дастурий-аппарат амалга оширилишининг ҳар хиллиги, таъсирининг кескинлиги, кўлланилишининг вакти ва жойини танлаш имконияти, нихоят, фойдалилиги ахборот қуролини ҳаддан ташқари ҳавфли қиласди. Бу қуролни, масалан, интеллектуал мулкни химоялаш воситасига ўхшатиб никоблаш мумкин. Ундан ташқари, у ҳатто уруш эълон килмасдан

хужум харакатларини автоном тарзда олиб бориш имконини беради.

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

Ахборот куроли кўлланилишини олдини олиш ёки кўлланиши оқибатларини бартараф килиш учун қўйидаги 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 килинишидан химоялаш;
- ахборот сифатини саклаш (ўз вактидалиги, аниқлиги, тўлалиги ва фойдаланувчанлиги).

Давлатнинг дунё очик тармоғига уланишининг иқтисодий ва илмий-техник сиёсатини ахборот хавфсизлиги орқали кўриш лозим. Бу очик, фукароларнинг ахборотга ва интеллектуал мулкга эга бўлиш конуний хукукини саклашга мўлжалланган сиёsat мамлакат худудида тармок асбоб-ускуналарини унга ахборот куроли элементларининг киришидан саклашни кўзда тутиш лозим. Бу муаммо хозирда, 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 хисоблаш ресурсларидан оператив фойдаланиши давлатчиликни, фукаролик жамияти институтларини мустаҳкамлаш, ижтимоий инфратузилмаларининг ривожланиш шартлари сифатида талкин этиш мумкин.

Аммо мамлакатнинг ҳалқаро телекоммуникация тизимида ва ахборот алмашинувида иштирокининг ахборот хавфсизлиги муаммосини комплекс ҳал килмасдан мумкин эмаслигини аниқ тасаввур этиш лозим. Айнисса, хусусий ахборот ресурсларини химоялаш муаммоси ахборот ва телекоммуникация технологиялар соҳасида ривожланган мамлакатлардан технологик оркада колаётган мамлакатлар учун жиддий хисобланади.

Ахборот қуролини ишлаб чикишни ва уни ишлатишни кимёвий ва бактериологик қурол каби тақиқлаш эҳтимолдан узок. Ҳудди 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 тармокларда таҳдидлар ва заифликлар**

Тармок технологиялари ривожининг бошланғич босқичида вируслар ва компьютер ҳужумларининг бошка турлари таъсиридаги зарар кам эди. чунки у даврда дунё иктисадининг ахборот технологияларига боғликлиги катта эмас эди. Ҳозирда, ҳужумлар сонининг доимо ўсиши ҳамда бизнеснинг ахборотдан фойдаланиш ва алмашибининг электрон воситаларига боғликлиги шароитида машина вактининг йўқолишига олиб келувчи ҳатто озгина ҳужумдан келган зарар жуда катта ракамлар оркали ҳисобланади. Мисол тариқасида ксептириш мумкинки, факат 2003 йилнинг биринчи чорагида дунё микёсидаги йўқотишлар 2002 йилдаги барча йўқотишлар йигиндининг 50 %ини ташкил этган ёки бўлмаса 2006 йилнинг ўзида Россия Федерациясида 14 мингдан ортиқ компьютер жиноятчилиги ҳолатлари кайд этилган [24, 34, 35]. Корпоратив тармокларда ишланадиган ахборот, айникса, заиф бўлади. Ҳозирда рухсатсиз фойдаланишга ёки ахборотни модификациялашга, ёлғон ахборотнинг муомалага кириши имконининг жиддий ошишига кўйидагилар сабаб бўлади:

- компьютерда ишланадиган, узатиладиган ва сакланадиган ахборот хажмининг ошиши;
- маълумотлар базасида мухимлик ва маҳфийлик даражаси турли бўлган ахборотларнинг тўпланиши;
- маълумотлар базасида сакланётган ахборотдан ва ҳисоблаш тармок ресурсларидан фойдаланувчилар доирасининг кенгайиши;
- масофадаги ишчи жойлар сонининг ошиши;

- фойдаланувчиларни боғлаш учун Internet глобал тармоғини ва алоқанинг турли каналларини кенг ишлатиши;
- фойдалувчилар компьютерлари ўртасида ахборот алмашинувининг автоматлаштирилиши.

Ахборот хавфсизлигига таҳдид деганда ахборотнинг бузилиши ёки йўкотилиши хавфига олиб келувчи химояланувчи обьектга карши килинган харакатлар тушунилади. Олдиндан шуни айтиш мумкинки, сўз барча ахборот хусусида эмас, балки унинг факат, мулк эгаси фикрича. тижорат кийматига эга бўлган кисми хусусида кетялти.

Замонавий корпоратив тармоклар ва тизимлар дучор бўладиган кенг тарқалган таҳдидларни таҳлиллаймиз. Хисобга олиш лозимки, хавфсизликка таҳдид манбалари корпоратив ахборот тизимининг ичидаги (ички манба) ва унинг ташкарисида (ташқи манба) бўлиши мумкин. Бундай ажратиш тўғри, чунки битта таҳдид учун (масалан, ўғирлаш) ташки ва ички манбаларга карши харакат усуллари турлича бўлади. Бўлиши мумкин бўлган таҳдидларни хамда корпоратив ахборот тизимининг заиф жойларини билиш хавфсизликни таъминловчи энг самарали воситаларни танлаш учун зарур хисобланади.

Тез-тез бўладиган ва хавфли (зарар ўлчами нуктаи назаридан) таҳдидларга фойдаланувчиларнинг, операторларнинг, маъмурларнинг ва корпоратив ахборот тизимларига хизмат кўрсатувчи бошка шахсларнинг атайн килмаган хатоликлари киради. Баъзида бундай хатоликлар (нотўғри киритилган 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 килади. Бунда зарар манбаси ташкилотнинг фойдаланувчиси ҳам, тармок фойдаланувчиси ҳам бўлиши мумкин, охиргиси айниқса хавфли.

Зарар ўлчами бўйича иккинчи ўринни ўғирлашлар ва соҳталаштиришлар эгаллайди. Текширилган ҳолатларнинг аксариятида ишлаш режимлари ва химоялаш чоралари билан аъло даражада таниш бўлган ташкилот штатидаги ҳодимлар айбдор бўлиб чиқдилар. Глобал тармоклар билан боғланган кувватли ахборот каналининг мавжудлигида, унинг ишлаши устидан етарлича назорат йўклиги бундай фаолиятга қўшимча имкон яратади.

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

Хозирда ташки коммуникация оркали рухсатсиз фойдаланишга атайин килинган 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 сукилиб кириш уринишларига дучор бўлар экан. Хавф-хатарлар тахлил килинганида ташкилот корпоратив ёки локал тармоғи компьютерларининг хужумларга карши туриши ёки бўлмаганида ахборот хавфсизлиги бузилиши фактларини кайд этиш учун етарлича химоялан-маганлигини хисобга олиш зарур. Масалан, ахборот тизимларини химоялаш Агентлигининг (АҚШ) тестлари кўрсатадики, 88 % компьютерлар ахборот хавфсизлиги нуктаи назаридан нозик жойларга язаки, улар рухсатсиз фойда таниш учун фаол ишлатишлари мумкин. Ташкилот ахборот тузилмасидан масофадан фойдаланиш ҳоллари алоҳида кўрилиши лозим.

Ҳимоя сиёсатини тузишдан аввал ташкилотда компьютер мухити дучор бўладиган хавф-хатар баҳоланиши ва зарур чоралар кўрилиши зарур. Равшанки, ҳимояга таҳдидни назоратлаш ва зарур чораларни кўриш учун ташкилотнинг сарф-харажати ташкилотда активлар ва ресурсларни химоялаш бўйича хеч кандай чоралар кўрилмаганида кутиладиган йўкотишлардан ошиб кетмаслиги шарт.

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

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

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

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



1.1-расм. Хавфсизликнинг бузилиш манбалари.

1.1.-расмда келтирилган статистик маълумотлар ташкилот маъмуриятига ва ходимларига корпоратив тармок ва тизими хавфсизлигига таҳдидларни самарали камайтириш учун харакатларни 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 каторда корпоратив тармок ва тизимга ҳам ташқаридан, ҳам ичкаридан бўладиган хужумларни олдини олиш бўйича тармок хавфсизлиги масаласини счишга жиддий ўтиборни қаратиш зарур.

### 1.3. Компьютер жиноятчилигининг таҳлили

Компьютер жиноятчилиги статистикаси таҳлил этилса қайғули манзараага эга бўламиз. Компьютер жиноятчилиги етказган зарарни наркотик моддалар ва қуролларнинг ноконуний айланишидан олинган фойдага киёслаш мумкин. Факат АҚШда «Электрон жиноятчилар» етказган ҳар йилги зарар қарийб 100 млд. долларни ташкил этар экан.

Яқин келажақда жиной фаолиятнинг бу тури даромадлилiği, пул маблағларининг айланиши ва унда иштирок этувчи одамлар сони бүйича яқин вактларгача ноконуний фаолият орасида даромадлиги билан биринчи ўринни эгаллаган ноконуний бизнеснинг уч туридан ўзид кетиш әхтимоллиги катта. Бу ноконуний бизнеслар-наркотик моддалар, курол ва кам учрайдиган ёввойи хайвонлар билан савдо қилиш.

Давлат ва хусусий компаниялар фаолиятининг социологик тадқики маълумотларига қараганда XXI асрнинг биринчи ийлларида иктисодий соҳадаги жиноятчилик банк ва бошка тизимларнинг ахборот-коммуникацион комплексларига бўлиши мумкин бўлган ғаразли иктисодий ҳаракатларга қаратилган бўлади.

Кредит-молия соҳасидаги компьютер жиноятчилигининг сони муттасил ўсиб бормоқда. Масалан, онлайн магазинларида 25 %гача қаллоблик тўлов амаллари кайд этилган. Шунга қарамасдан Farb давлатларида электрон тижоратнинг юкори даромадли замонавий бизнеснинг фаол ривожланиши кўзга ташланмокда. Маълумки, бу соҳа ривожланиши билан параллел равишда «виртуал» қаллобларнинг хам даромади ошади. Қаллоблар энди якка ҳолда ҳаракат килмайдилар. улар пухталиқ билан тайёланган, яхши техник ва дастурий куролланган жиной гурухлар билан, банк хизматчиларининг ўзлари иштирокида ишлайдилар.

Хавфсизлик соҳасидаги мутахассисларнинг кўрсатишича бундай жиноятчиларнинг улуши 70 %ни ташкил этади. «Виртуал» ўтри ўзининг ҳамкасби-оддий босқинчига нисбатан кўп топади. Ундан ташқари, «виртуал» жиноятчилар уйидан чиқмасдан ҳаракат киладилар. Фойдаланишнинг электрон воситаларини ишлатиб килинган ўғрилик зарарининг ўртacha қўрсаткичи факат АҚШда банкни куролли босқинчиликдан келган зарарнинг ўртacha 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 ўсајапти, аслида юкорида келтирилган маълумотлардан бир тартибга ошиши мумкин. Чунки кўп йўқотишлар аникланмайди ёки эълон килинмайди. ўзига хос «индамаслик сиёсати»ни тизим маъмурларининг ўзининг тармоғидан рухсатсиз фойдаланганлик тафсилоти-

ни, бу нохуш ходисанинг тақрорланишидан кўркиб ва ўзининг химоя усулини ошкор этмаслик важида мухокама этишини хоҳламасликлари билан тушуниш мумкин.

Компьютер ишлатиладиган инсон фаолиятининг бошқа соҳаларидаги ҳам вазият яхши эмас. Йилдан-йилга ҳукукни муҳофаза килувчи органларига компьютер жиноятчилиги хусусидаги мурожаатлар ошиб бормоқда.

Барча мутахассислар вирусларнинг тарқалиши билан бир каторда ташки ҳужумларнинг кескин ошганлигини эътироф этмоқдалар. Кўриниб турибдики, компьютер жиноятчилиги натижасида зарап катъий ортмоқда. Аммо компьютер жиноятчилиги кўпинчя «виртуал» қаллоблар томонидан амалга оширилади дейиш хақиқатга тўғри келмайди. Ҳозирча компьютер тармоқларига сукилиб кириш хавфи ҳар бири ўзининг усулига эга бўлган хакерлар, кракерлар ва компьютер кароқчилари томонидан келмоқда.

*Хакерлар*, бошқа компьютер кароқчиларидан фарқли ҳолда, баъзида, олдиндан, мақтаниш мақсадида компьютер эгаларига уларнинг тизимиға кириш ниятлари борлигини билдириб кўядилар. Муваффакиятлари хусусида Internet сайтларида хабар берадилар. Бунда хакер мусобакалашув ниятида кирган компьютерларига зарар етказмайди.

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

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

Баъзи «мутахассислар» жиддий гурӯх ташкил киладилар, чунки бундай криминал бизнес ўта даромадлидир. Бу эса тез орада, «виртуал» жиноятнинг зарари жиноят бизнесининг анъанавий хилидаги зарапдан бир тартибга (агар кўп бўлмаса) ошишига сабаб бўлади. Ҳозирча бундай таҳдидни бетарафлаштиришнинг самарали усувлари 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, ҳакикатан, тармок хавфсизлигини таъминлайди.

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

- тармок трафигини таҳлиллаш;
- тармоқнинг ёлғон объектини киритиш;
- ёлғон маршрутни киритиш;
- хизмат килишдан воз кечишга ундаидиган ҳужумлар.

**Тармок 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 пароли ва идентификатори тармок орқали очик, шифрланмаган кўринишда узатилади. Демак, Internet хостларидан фойдаланиш учун фойдаланувчининг исми ва паролини билиш кифоя.

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

FTP ва TELNET протоколларининг таҳлили кўрсатадики, TELNET паролни символларга ажратади ва паролнинг ҳар бир символини мос пакетга жойлаштириб битталаб узатади, FTP эса, аксинча, паролни бугунлайича битта пакетда узатади. Пароллар шифрланмаганлиги сабабли пакетларнинг маҳсус сканер-дастурлари ёрдамида фойдаланувчининг исми ва пароли бўлган пакетни ажратиб олиш мумкин. Худди шу сабабли, хозирда оммавий тус олган ICQ дастури ҳам ишончли эмас. ICQнинг протоколлари ва ахборотларни саклаш, узатиш форматлари маълум ва демак, унинг трафиги ушлаб колиниши ва очилиши мумкин.

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

**Тармоқнинг ёлғон объектини киритиш.** Ҳар қандай тақсимланган тармоқда кидириш ва манзиллаш каби «нозик жойлари» мавжуд. Ушбу жараёнлар кечишида тармоқнинг 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 чиқкани каби тасаввур этиш мумкин. Бу холда нияти бузук одам унчалик кийналмасдан электрон хат-хабарингизни эгаллаши, мумкин, сиз эса ҳатто ундан шубҳаланмасдан ўзингиз барча электрон почтангизни жўнаттган бўлар эдингиз.

Қандайдир хостга мурожаат этилганида манзилларни маҳсус ўзгартишлар амалга оширилади (IP-манзилдан тармоқ адаптери ёки маршрутизаторининг физик манзили аникланади). Internetда бу муаммони ечишда ARP(Address Resolution Protocol) проколидан фойдаланилади. Бу куйидагича амалга оширилади: тармоқ ресурсларига биринчи мурожаат этилганида хост кенг кўламли ARP-сўровни жўнатади. Бу сўровни тармоқнинг берилган сегментидаги барча станциялар қабул килади. Сўровни қабул килиб, хост сўров юборган хост хусусидаги ахборотни ўзининг ARP-жадвалига киритади, сўнгра унга ўзининг Ethernet-манзили бўлган ARP-жавобни жўнатади. Агар бу сегментда бундай хост бўлмаса, тармоқнинг бошка сегментларига мурожаатга имкон берувчи маршрутизаторга мурожаат килинади. Агар фойдаланувчи ва нияти бузук одам бир сегментда бўлса, ARP-сўровни ушлаб колиш ва ёлғон ARP-жавобни йўллаш мумкин бўлади. Бу усулнинг таъсири факат битта

сегмент билан чегараланғанлығы тасалы сифатида хизмат килиши мүмкін.

ARP билан бўлган холга ўхшаб DNS-сўровни ушлаб колиш йўли билан Internet тармоғига ёлғон DNS-серверни киритиш мүмкін.

Бу куйидаги алгоритм бўйича амалга оширилади:

1. DNS-сўровни кутиш.

2. Олингандан сўровдан керакли маълумотни чикариб олиш ва тармок бўйича сўров юборган хостга ёлғон DNS-жавобни ҳакиқий 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 ҳакиқий хисоблайди).

**Ёлғон маршрутни киритиш.** Маълумки, замонавий глобал тармоклари бир-бири билан *тармоқ узеллари* ёрдамида уланган тармок сегментларининг мажмуудир. Бунда *маршрут* деганда маълумотларни манбадан қабул қилувчига узатишга хизмат қилувчи тармок узелларининг кетма-кетлиги тушунилади. Маршрутлар хусусидаги ахборотни алмашишни унификациялаш учун маршрутларни бошқарувчи маҳсус 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 хужум қилувчи ёлғон хостни киритишдан бўлак нарса эмас. Ҳатто, охири объект ҳакиқий бўлса, ҳам маршрутни ахборот барibir ёлғон хостдан ўтадиган килиб қуриш мүмкін.

Маршрутни ўзгартириш учун хужум қилувчи тармокка тармокни бошқарувчи қурилмалар (масалан, маршрутизаторлар) номидан берилган тармокни бошқарувчи протоколлар оркали аниқланган маҳсус хизматчи хабарларни жўнатиши лозим. Маршрутни муваффакиятли ўзгартириш натижасида хужум қилувчи таксимланган тармоқдаги иккита объект алмашадиган ахборот оқими устидан тўла назоратга эга бўлади, сўнгра ахборотни ушлаб колиши, таҳлиллаши, модификациялаши ёки оддийгина йўқотиши мүмкін. Бошқача айтганда таҳдидларнинг барчá турларини амалга ошириш имконияти туғилади.

**Хизмат килишдан воз кечишига ундейдиган тақсимланган хужумлар** – DDoS (Distributed Denial of Service) компьютер жиноятчилигининг нисбатан янги хили бўлсада, кўркинчли тезлик билан таркалоюда. Бу хужумларниг ўзи анчагина ёкимсиз бўлгани етмаганидек, улар бир вактнинг ўзида масофадан бошқариувчи юзлаб хужум килувчи 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 ёкимсиз сифатларини ўйғуллаштирган яна биттаси stacheldraht («тикон симлар») пайдо бўлди.

1.2-расмда хизмат килишдан воз кечишига ундейдиган хужум воситаларининг характеристикалари келтирилган.

Хизмат килишдан воз кечишига ундейдиган оддий тармоқ 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 аниклаш жуда кийин.

Хизмат кўрсатишдан воз кечиши хужумлари учун воситалар			
ХУЖУМ ҚИЛУВЧИ СЕРВЕРЛАР			
trinoo	TFN	TFN2K	stacheldraht
пакетларни жўнатувчининг адресини бузмайди	пакетларни жўнатувчининг адресини бузади	пакетларни жўнатувчининг адресини бузади	- пакетларни жўнатувчининг адресини бузади
- парол ўрнатилга нидан сўнг атакани ўтказади	- турли протоколли атакалар хилини мададлайди	- тармоқ интерфейси ни таҳлиллайди	- хабарларни тестлашдан ўтказади
		- шифрлашнинг ишончили даражасига эга	- ТСРнинг шифрланган пакетларини ишлатади

1.2-расм. Хизмат килишдан воз кечишига ундейдиган хужум воситаларининг характеристикалари.

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

## 1.5. Ахборот хавфсизлигини бузувчининг модели

Бўлиши мумкин бўлган таҳдидларни олдини олиш учун нафакат операцион тизимларни, дастурий таъминотни химоялаш ва фойдаланишни назорат килиш, балки бузувчилар туркумини ва улар фойдаланадиган усуулларни аниклаш лозим.

Сабаблар, мақсадлар ва усуулларга боғлик ҳолда ахборот хавфсизлигини бузувчиларни тўртта категорияга ажратиш мумкин:

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

*Саргузашт қидирудувчи*, одатда, ёш, кўпинча талаба ёки юкори синф ўкувчиси ва унда ўйлаб килинган хужум режаси камдан-кам бўлади. У нишонини тасодифан танлайди, кийинчиликларга дуч келса чекинади. Хавфсизлик тизимида нуксонли жойни топиб, у маҳфий ахборотни йигишга тиришади, аммо ҳеч қачон уни яширинча ўзгартиришга уринмайди. Бундай саргузашт қидирудувчи муваффакиятларини факат якин дўстлари-касбдошлари билан ўртоқлашади.

*Ғояли хакер* – бу ҳам саргузашт қидирудувчи, аммо мохиррок. У ўзининг эътиқоди асосида муайян нишонларни (хостлар ва ресурсларни) танлайди. Унинг яхши кўрган хужум тури Web-сервернинг ахборотини ўзгартириши ёки жуда кам ҳолларда, хужум кили-нувчи ресурслар ишини блокировка килиш. Саргузашт қиди-рувчиларга нисбатан ғояли хакерлар муваффакиятларини кенгроқ аудиторияда, одатда, ахборотни хакер Web-узелда ёки Usenet анжуманида жойлаштирилган ҳолда эълон киладилар.

*Хакер-проффесионал* харакатларнинг аник режасига эга ва маълум ресурсларни мўлжаллайди. Унинг хужумлари яхши ўйланган ва одатла, бир неча боскичда амалга оширилади. Аввал у

дастлабки ахборотни йигади (операцион тизим тури, тақдим этиладиган сервислар ва қўлланиладиган ҳимоя чоралари). Сўнгра у йиғилган маълумотларни хисобга олган ҳолда ҳужум режасини тузади ва мос инструментларни танлайди (ёки ҳатто ишлаб чиқади). Кейин, ҳужумни амалга ошириб, маҳфий ахборотни олади ва ниҳоят ҳаракатларининг барча изларини йўқ килади. Бундай ҳужум килувчи профессионал, одатда, яхши молияланади ва якка ёки профессионаллар командасида ишлаши мумкин.

*Ишончсиз ходим* ўзининг ҳаракатлари билан саноат жосуси етказадиган муаммога тенг (ундан ҳам қўп бўлиши мумкин) муаммони туғдиради. Бунинг устига унинг борлигини аниклаш мураккаброқ. Ундан ташкари, унга тармокнинг ташки ҳимоясини эмас, балки фақат, одатда, унчалик қатъий бўлмаган тармокнинг ички ҳимоясини бартараф килишига тўғри келади. Аммо, бу ҳолда унинг корпоратив маълумотлардан рухсатсиз фойдаланиши хавфи бошка ҳар кандай нияти бузук одамнидан юкори бўлади.

Юкорида келтирилган ахборот хавфсизлигини бузувчилар категорияларини уларни малакалари бўйича гурухлаш мумкин: хаваскор (саргузашт кидиравчи), мутахассис (ғояли хакер, ишончсиз ходим), профессионал (хакер-профессионал). Агар бу гурухлар билан хавфсизликнинг бузилиши сабаблари ва ҳар бир гурухнинг техник куролланганлиги таккосланса, ахборот хавфсизлигини бузувчининг умумлаштирилган моделини олиш мумкин (1.3-расм).

Ахборот хавфсизлигини бузувчи, одатда, маълум малакали мутахассис бўлган ҳолда компьютер тизимлари ва тармоклари хусусан, уларни ҳимоялаш воситалари хусусида барча нарсаларни билишига уринади. Шу сабабли бузувчи модели қуйидагиларни аниклади:

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



1.3-рас.и. Ахборот хавфсизлигини бузувчининг модели.

Тизимдан рухсатсиз фойдаланишга мажбур этиш сабабларининг диапазони етарлича кенг: компьютер билан ўйнаганидаги хаяжон күттаринкилигидан то жирканч менеджер устидан хокимлик хиссиятигача. Бу билан нафакат күнгил очишни хохловчи хаваскорлар, балки профессионал дастурчилар ҳам шуғулланади. Улар паролни танлаш, фараз килиш натижасида ёки бошқа хакерлар билан алмашиш йўли оркали қўлга киритадилар. Уларнинг бир кисми нафакат файлларни кўриб чиқади, балки файлларнинг мазмунни билан қизика бошлайди. Бу жиддий таҳдид хисобланади, чунки бу ҳолда беозор шўхликни ёмон ният билан килинган харакатдан ажратиш қийин бўлади.

Якин вактгача раҳбарлардан норози хизматчиларнинг ўз мавқеларини суиистеммол килган ҳолда тизимни бузишлари, ундан бегоналарнинг фойдаланишларига йўл қўйишлари ёки тизимни иш холатида қаровсиз қолдиришлари ташвишлантиради. Бундай харакатларга мажбур этиш сабаблари куйидагилар:

- хайфсанга ёки раҳбар томонидан танбехга реакция;
- иш вактидан ташкари бажарилган ишга фирма ҳак тўламаганидан норозилик;

– фирмани қандайдир янги тузилаётган фирмага ракиб сифатида заифлаштириш максадида касос олиш каби ёмон ният.

Рахбардан норози ходим жамоа фойдаланувчи хисоблаш тизимларига энг катта таҳдидлардан бирини тұғдиради. Шунинг учун хам хакерлар билан курашиш агентлиги индивидуал компьютер сохибларига жон деб хизмат күрсатадилар.

Профессионал хакерлар-хисоблаш төхникасини ва алоқа тизимини жуда яхши биладиган компьютер фанатлари (мутаассиблари) хисобланади. Тизимга кириш учун профессионаллар омадга ва фарзга таянмайдилар ва қандайдир тартибни ва тажрибани ишлата дилар. Уларнинг максади-химояни аниклаш хамда йўқотиш, хисоблаш қурилмасининг имкониятларини ўрганиш ва максадига эришиш мумкинлиги тўғрисида карорга келиш.

Бундай профессионал хакерлар категориясига қуйидаги шахслар киради:

- сиёсий максадни кўзловчи жиной гурухларга кирувчилар;
- саноат жосуслик максадларида ахборотни олишга уринувчилар;
- текин даромадга интилувчи хакерлар гурухи.

Умуман профессионал хакерлар хавф-хатарни минималлаштиришга уринадилар. Бунинг учун улар бирга ишлашга фирманда ишлайдиган ёки фирмадан якинда ишдан бўшатилган ходимларни жалб этадилар, чунки бегона учун банк тизимиға киришда ошкор бўлиш хавфи жуда катта. Ҳакикатан, банк хисоблаш тизимларининг мураккаблиги ва юқори тезкорлиги, хужжатларни юргизиш ва текшириш усуllibарининг мунтазам такомиллаштирилиши бегона шахс учун хабарларни ушлаб колиш ёки маълумотларни ўғирлаш максадида тизимга ўрнашишига имкон бермайди. Профессионал хакерлар учун яна бир кўшимча хавотир-тизимдаги бир компонентнинг ўзгариши бошқа бир компонентнинг бузилишига олиб келиши ва хатардан дарак берувчи сигналга сабаб бўлиши мумкин.

Хакерлар хавф-хатарни камайтириш максадида одатда, молиявий ва оиласи муммиларга эга бўлган ходимлар билан алоқага кирадилар. Кўпгина одамлар хаётида хакерлар билан тўқнаш масликлари мумкин, аммо алкаголга ёки қиморга ружу қўйган ходимлар билмасдан жиной гурух билан боғланган қандайдир бир букмекердан қарздор бўлиб қолишли мумкин. Бундай ходим қандайдир ўйин-кулги кечасида сухбатдошининг профессионал

агент эканлигига шубха килмаган холда ортиқча гапириб юбориши мумкин.

## **1.6. Internet – хизматлар ва электрон бизнес тизимларида хавфсизлик муаммолари**

Хозирда Internet-хизматининг қуидаги тижорат шаклари кенг тарқалган:

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

*Internet-банкинг.* Замонавий Internet-технологиялар банкларга хизматларининг бир кисмини янги савияга ўтказишга ва шу орқали янги мижозларни жалб этишга ва уларга хизмат қилиш харажатларини пасайтиришга имкон яратади. Анъанавий банкларнинг аксарияти ўз мижозларига электрон хизмат қилиш ва счёт тўловининг кўшимча шакларини тавсия этади. Факат Internetда иш юритувчи банклар нисбатан якинда пайдо бўлди. Улар Web-банклар деб аталади. Энг йирик Web-банклар сирасига First Internet Bank, Net-Bank, CompuBank ва катор бошка банклар тааллукли.

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

Хозирда Internet-банкинг хизмати ҳар бири Internet орқали амалга оширилувчи қуидаги имкониятларга эга:

- нақд пулсиз хисоб-китобларни бажариш;
- коммунал хизматлар учун тўлови;
- Internetдан фойдаланиш учун тўлови;
- уяли ва пейджинг алоқа операторлари счёtlарини тўлаш;
- ички ва банклараро хужжат асосидаги тўловларни бажариш;
- ўз счёtlари бўйича маблағларни ўтказиш;
- исталган вакт оралиғи учун ўз счёtlари бўйича барча банк амалларини кузатиш.

*Internet-банкинг тизимидаш фойдаланиш мижозларга катор имтиёзлар беради:*

- фоизли ставкалари нисбатан юқори;
- шахсан банкка бориш зарурияти йўклиги хисобидан 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 аскотади-карта хисобидан маблағни чиқариш тизимлар томонидан тайёрланган хисоблар бўйича кўчирмада дархол акслантирилади. Бу мижозга ўз амалларини назоратлашда кулайлик туғдиради.

*Internet-трейдинг.* Internet-технологиялар фонд бозори учун жуда истиқболли. Internet-технологиялар туфайли, дунёда бўш капитални кўйишнинг энг яхши усули сифатида тан олинган кимматбахо коғозларни сотиб олиш, хозирда барча хоҳловчилар учун осон. Internet-трейдинг инвесторларни битимларни тузишнинг содалиги ва онлайн-брокерларнинг хизматига таърифларнинг пастлиги билан ўзига жалб қиласи.

*Internetнинг замонавий имкониятлари* кўчмас мулк билан бўладиган амалларни (сотиб олиш, сотиш, алмаштириш, мерос бўйича бериш, ижарага бериш ва х.) анъанавий шаклларига нисбатан айтарлича енгиллаштириш ва тезлаштиришга имкон беради. Мижоз уйидан 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-сугурта.* Суѓурталаш деганда суѓурталанувчи-мижоз (суѓурта хизматларини сотиб олувчи) билан суѓурталовчи (бундай хизматларни тақдим этувчи) ўртасида шартнома муносабатларини ўрнатиш ва мададлаш тушунилади. Суѓурталовчи суѓурта дастурини ишлаб чиқади ва аниклайди, мижозга таклиф этади, агар суѓурталанувчи рози бўлса иккала томон шартнома тузади. Мижоз бирданига ва мунтазам тўловларни амалга оширади, суѓурталовчи, ўз навбатида, суѓурта холат келиши билан суѓурталанувчига суѓурта шартномаси шартлари бўйича компенсация пулини тўлашга мажбурият олади.

Битимга келишиш жараёнида сугурта полиси деб аталаувчи хужжат шакллантирилади. Бу хужжат сугурталовчи ва сугурта компанияси учун юридик хужжат ҳисобланади. Унда сугурта объекти (мол-мулк, одам, масъулият), сугурталанувчи ҳолат, сугурта муддатининг бошланиши ва ниҳояси, сугурта суммаси, сугурта мукофоти каби мухим томонлари олдиндан айтиб ўтилади.

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

*ASP иловаларини ижарага бериш бўйича хизмат кўрсатиши.* Янги иктисадиёт ривожининг истикболли йўналишларидан бири ASP (Applications Service Providing) иловаларини ижарага бериш бўйича хизмат кўрсатишдир. Internet ёки хусусий тармок оркали фойдаланувчидан узокдаги серверда жойлашган иловалардан фойдаланишини ASP иловалари амалга оширади.

ASP иловаларининг провайдери ўзининг серверларига иловаларнинг дастурий таъминотини ўрнатади ва улардан мижозларнинг фойдаланишини таъминлайди. Мижоз компьютерига бундай дастурий таъминотни ўрнатиши, уни янгилаши, захира нусхалаши ва х.шарт эмас. Барча ишларни ASP провайдери бажаради. Мижоз провайдерга иловалардан фойдалангани учун ижара ҳакини тўлайди.

Компанияларнинг ASP хизматларидан фойдаланишининг сабаби қўйидагилар:

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

Яқин йилларда ASP бозорининг тез ўсиши кутилмоқда. Бу эса, ўз навбатида, барча компанияларга исталган бизнес-иловалардан бир хилда фойдаланишини тақдим этиш оркали, бизнес ривожида баркарорликни 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, мухокама килиш, ўзгартириш, товарларни ва хизматларни сотиш усулларини ҳамда тўловни амалга ошириш жараёниларини ўзгартириш учун янги технологиялардан фойдаланади. Ҳозирда электрон тижорат ва бизнеснинг аксарият муаммолари ахборот хавфсизлиги билан боғлик, яъни хавфсизлик

муаммолари электрон тижорат ва бизнес ривожидаги жиддий түсик хисобланади.

Хар кандай тижорат компаниясининг бошқа компаниялар билан ёки ушбу компаниянинг бўлимлари орасида алока ўрнатилиши зарур. Хозирда глобал Internet тармоғи ўзининг узеллари ўртасида ишончли ва арzon ахборот алмашинувини таъминлайди. Очиқ 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 лаёкатлигини бузувчи ва ёки ахборот тизими маълумотларини бузувчи маҳсус дастур – «тробян отларининг» киришига олиб келиши мумкин. Бу хил дастурларнинг ичida вируслар кенг тарқалган. Ўзига хос малакали мутахассислар корпоратив ахборот тармокларига билинмасдан кириш учун кўпинча умуммаксад тармоклардан фойдаланадилар.

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

Internet конфиденциал ахборотни дунёнинг исталган нуктасига юбориши мумкин, аммо у етарлича химояланмаган бўлса, ушлаб колиниши, нусхалаштирилиши, ўзгартирилиши хамда ҳар кандай четдаги фойдаланувчилар – нияти бузук одамлар, ракиблар ва оддий кизикувчилар томонидан ўқилиши мумкин. Масалан, етарлича химояланмаган тўлов топшириғи ёки кредит карточка номерини жўнатаётгандан эсда тутиш лозимки, жўнатиш хусусий/шахсий тармок орқали амалга оширилмаяпти ва четдаги фойдаланувчилар хабарингизни манипуляция килиш имкониятига эга. Ундан ташкари хабарингиз алмаштирилиб кўйилиши мумкин: хабарларни худди *B* фойдаланувчидан юборилганидек *A* фойдаланувчидан юбориш усувлари мавжуд. Internet тармоғи маҳсус пакет, тамомила конуний пакетлар, сонининг ҳаддан ташкари кўплиги узатишдаги

бузилишлар, тармок компонентларининг носозлиги туфайли ишга лаёкат бўйласлиги мумкин. Бундай ҳоллар «хизмат килишдан воз кечиши» деб аталади ва электрон тижорат учун энг жиддий таҳдид хисобланади. 2.2-жадвалда ахборот хавфсизлиги бузилишининг статистикаси келтирилган [24].

## 2.2-жадвал

Ахборот хавфсизлиги бузилишининг турлари	Қайд этилганлиги %	Йўқотишлар %
Корпоратив тармоқдан рухсатсиз четдан фойдаланиш	44	25
Хизмат килишдан 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 хисобланади ва усувлар ва воситаларнинг бутун бир тўплами ёрдамида таъминланиши шарт. Электрон тижорат соҳасидаги савдо кўлами Internet хавфсизлиги масалаларидан ташвишланган харидорлар, сотувчилар ва молия институтларининг бошидан кечиравчи қўркувлари билан чегараланди. Бу қўркувлар, хусусан, куйидагиларга асосланади:

- конфиденциалликка кафолатнинг йўқлиги-кимдир маълумотларингизни узатилаётганида ушлаб колиши ва кийматли ахборотни (масалан, кредит карточкангизнинг рақамларини, товар етказиб бериш санаси ва манзил) топишга уриниши мумкин;
- амалда иштирок этувчиларни текшириш даражасининг етарили эмаслиги – транзакция катнашчилари текширилмаганида томонларнинг бири «маскарад» уюштириши мумкинки, унинг оқибати йккинчи томонга анча қимматга тушади. Масалан, харидор сайтга кириб ундаги компаниянинг хакиқийлигига шубха килади, шундай

хол ҳам рўй бериши мумкинки, харидор кредит карточкасининг ракамларини етарлича ваколатга эга бўлмаган шахсга беради;

– сотувчидаги буюртма берган харидор кредит карточкасининг қонуний ғасири эканлигинининг текшириш имкони йўқ;

– кредит карточкасининг банк-эмитенти тўловни бажаришга талаб кўйган сотувчини текширишни истаб колиши мумкин;

– маълумотлар яхлигига кафолат йўқ – ҳатто маълумотларни жўнатувчи индентификацияланган бўлсада, учинчи томон маълумотларни, улар узатилиши вактида, ўзгартириш имкониятига эга.

Ахборот хавфсизлигини таъминлаш нуқтаи назаридан электрон тижоратнинг намунавий қўлланилишини – Internet оркали маҳсулотга ва хизматларга эга бўлишни кўрайлик. Ушбу жараён куйидаги боскичлар оркали ифодаланиши мумкин.

1. Буюртмачи Web-сервер оркали 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 оркали текширилади.

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

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

6. Мижоз онлайн режимида буюртма хақини тўлайди.

7. Товар буюртмачига стказилади.

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

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

боскичда буюртмачи кредит карточкасининг ракамини киритганда кучаяди;

• ёлғон буюртмалар бериш ва электрон магазин ходимлари томонидан фирибгарлик килиш. Ҳозирда ички/ташки таҳдидлар муносабати 60/40 %ни ташкил этади;

- электрон тижорат тизимида узатиладиган маълумотларни ушлаб колиш. Буюртмачининг кредит картаси хусусидаги ахборотни ушлаб колиш 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 пройдери – мижозлар ишончини йўқотади, моддий зарар кўради. Баъзи холларда бу компанияларга кредит карточка раками фош килингани учун даъво қўзғатилиши мумкин. «Хизмат қилишдан воз кечиш» ҳужуми натижасида электрон магазиннинг ишлаши бузилиши мумкин, унинг ишга лаёқатлиигини тиклашга инсон, вакт 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 фарқланади (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 кулагилиги ва техник мутахассисларга қўйиладиган талаблар ўртасида муросага етишиш ташкил этади.

Компьютер тизимиға икки нұктай назардан караш мумкин: унда факат ишчи станциялардан фойдаланувчиларни кўриш мумкин, ёки факат тармоқ операцион тизимининг ишлашини хисобга 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. Мос холда ҳар бир сатҳ учун ҳимоялаш усули турлича бўлади. Тизимнинг ишончли ҳимояланиши ҳимояланган сатҳлар сони билан белгиланади.

Биринчи, кўриниб турган ва амалда энг кийин йўл-ходимларни тармоқ ҳужумларини кийинлаштирувчи хатти-харакатга ўргатиш. Бу бир карашда осондай тувлсада, аммо мушкул иш. Internet дан фойдаланишни чегаралаш лозим. Аксарият фойдаланувчилар чегараланишлар сабабини билмайдилар. Шунинг учун такиклар аниқ ифодаланиши лозим.

Тармоқда ахборотни ҳимоялашнинг зарурий даражасини ишлаб чикишда ходимлар ва раҳбариятнинг ўзаро жавобгарлиги, шахс

ва ташкилот манфаатларига риоя килиш, хукукни муҳофаза килувчи органлар билан ўзаро алоқа ҳисобга олинади. Ракобатли шароитда хизматларнинг катта сонини тақдим этиш ва хизмат килиш вактини қисқартириш орқали етакчи ўринни саклаб қолиш ва янги мижозларни жалб этиш мумкин. Бунга факат барча амалларни автоматлаштиришнинг зарурый даражасини гаъминлаш эвазига эришиш мумкин. Айни замонда ҳисоблаш техникасининг ишлатилиши билан нафакат пайдо бўлган муаммолар ҳал этилади, балки ахборотни бузилиши ва йўқотилиши, тасодифан ва атайин модификацияланиши ҳамда ахборотни бегоналар тарафидан рухсатсиз олиниши билан боғлик янги ноанъанавий таҳдидлар пайдо бўлади.

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

Мавжуд ҳолатнинг таҳлили кўрсатадики, ахборотни химоялаш учун килинадиган тадбирлар даражаси, одатда, автоматлаштириш даражасидан паст. Бундай оркада колиш жiddий оқибатларга олиб келиши мумкин.

Автоматлаштирилган комплексларда ахборотнинг заифлигига ҳисоблаш ресурсларининг концентрацияланиши, уларнинг ҳудудий таксимланганлиги, магнит элтувчиларида маълумотларнинг катта ҳажмини узок вакт сакланиши, кўпгина фойдаланувчиларнинг ресурслардан бир вактда фойдаланиши сабаб бўлади.

Бундай шароитда химоялаш чораларини кўриш заруриятига шубха килмаса бўлади. Аммо куйидаги кийинчиликлар мавжуд:

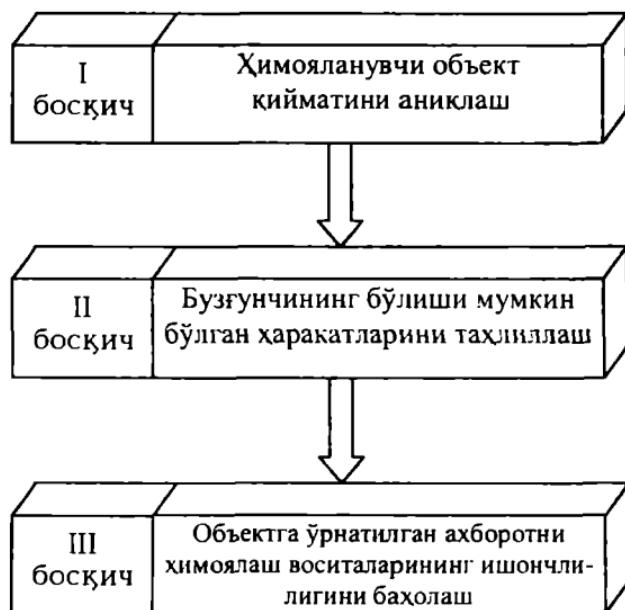
- ҳозирги кунда химояланган тизимларнинг ягона назарияси йўқ;
- химоя воситаларини ишлаб чикарувчилар хусусий масалаларни ечиш учун асосан алоҳида компонентларни тавсия этадилар, химоялаш тизимини шакллантириш ва бу воситаларнинг бирга ишлатилиши масалалари эса истеъмолчи ихтиёрига колдирилади;
- ишончли химояни таъминлаш учун техник ва ташкилий муаммолари комплексини ҳал этиш ва мос ҳужжатларни ишлаб чикиш зарур.

Юкорида санаб ўтилган кийинчиликларни бартараф килиш учун нафакат алоҳида корхона, балки давлат даражасидаги ахборот жараёнларида иштирок этувчилари характеристининг координацияси

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

Концепция – ахборот хавфсизлиги муаммосига расмий кабул килинган карашлар тизими ва уни замонавий тенденцияларни хисобга олган ҳолда ечиш йўллари. Концепцияда ифодаланган максадлар, масалалар ва уларни бўлиши мумкин бўлган ечиш йўллари асосида ахборот хавфсизлигини таъминлашнинг муайян режалари шакллантирилади.

Концепцияни ишлаб чикишни уч боскичда амалга ошириш тавсия этилади (2.1-расм).



2 1-расм. Ахборот химояси концепциясини ишлаб чикиш боскичлари.

Биринчи босқичда химоянинг максадли кўрсатмаси, яъни кандай реал бойликлар, ишлаб чикариш жараёнлари, дастурлар, маълумотлар базаси химояланиши зарурлиги аникланиши шарт. Ушбу босқичда химояланувчи алоҳида обьектларни аҳамияти бўйича табақалаштириш максадга мувофик хисобланади.

Иккинчи босқичда химояланувчи обьектга нисбатан бўлиши мумкин бўлган жиноий харакатлар таҳлилланиши лозим. Иктиносий жосуслик, тероризм, саботаж, бузиш орқали ўғирлаш каби кенг тарқалган жиноятчиликларнинг реал хавф-хатарлик даражасини аниклаш муҳим хисобланади. Сўнгра, нияти бузук одамларнинг химояга мухтож асосий обьектларга нисбатан харакатларининг эҳтимоллигини таҳлиллаш лозим.

Учинчи босқичнинг бош масаласи—вазиятни, 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 архитектураси (2.2-расм) ахборот хавфсизлиги концепцияси асосида ишлаб чиқилади.

Ахборот хавфсизлиги бўйича тадбирлар комплексининг асосини ахборот химоясининг стратегияси ташкил этиши лозим. Унда ишончли химоя тизимини куриш учун зарурй максадлар, мезонлар, принциплар ва муолажалар аникланади. Яхши ишлаб чиқилган стратегияда нафакат химоя даражаси, раҳналарни кидириш, брандмауэрлар ёки роҳу-серверлар ўрнатиладиган жой ва х. ўз аксини топиши лозим, балки ишончли химояни кафолатлаш учун уларни ишлатиш муолажалари ва усуллари хам аникланиши лозим.

Ахборот химояси умумий стратегиясининг муҳим хусусияти хавфсизлик тизимини тақиқлашдир. Иккита асосий йўналишни ажратиш мумкин:

- химоя воситаларининг таҳлили;
- хужум бўлганини аниклаш.



2.2-расм. Ахборот хавфсизлигини таъминлаш иерархияси.

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

## 2.3. Ахборот хавфсизлигининг сиёсати

Ахборот хавфсизлигининг сиёсатини ишлаб чикишда, аввало, химоя килинувчи объект ва унинг вазифалари аникланади. Сўнгра душманинг бу объектга кизикиши даражаси, хужумнинг эҳтимолли турлари ва кўриладиган зарар баҳоланади. Нихоят, мавжуд карши таъсир воситалари етарли химояни таъминламайдиган объектнинг заиф жойлари аникланади.

Самарали химоя учун ҳар бир объект мумкин бўлган таҳдидлар ва хужум турлари, маҳсус инструментлар, куроллар ва портловчи моддаларнинг ишлатилиши эҳтимоллиги нуктаи назаридан баҳоланиши зарур. Таъкидлаш лозимки, нияти бузук одам учун энг кимматли объект унинг ёътиборини тортади ва эҳтимолли нишон бўлиб хизмат килади ва унга қарши асосий кучлар ишлатилади. Бунда хавфсизлик сиёсатининг ишлаб чикилишида ечими берилган объектнинг реал химоясини таъминловчи масалалар ҳисобга олинниши лозим.

Қарши таъсир воситалари химоянинг тўйик ва эшелонланган концепциясига мос келиши шарт. Бу дегани, карши таъсир воситаларини марказида химояланувчи объект бўлган концентрик доираларда жойлаштириш лозим. Бу ҳолда душманинг исталған объектга йўли химоянинг эшелонланган тизимини кесиб ўтади. Мудофаанинг ҳар бир чегараси шундай гашкы қилинади, кўриклаш ходимининг жавоб чораларини кўришига старлича вақт мобайнида хужумчини ушлаб туриш имкони бўлсин.

Сўнгги боскичда карши таъсир воситалари қабул қилинган химоя концепциясига биноан бирлаштирилади. Бутун тизим хаёти циклининг бошлангич ва қутилувчи умумий нархини дастлабки баҳолаш амалга оширилади.

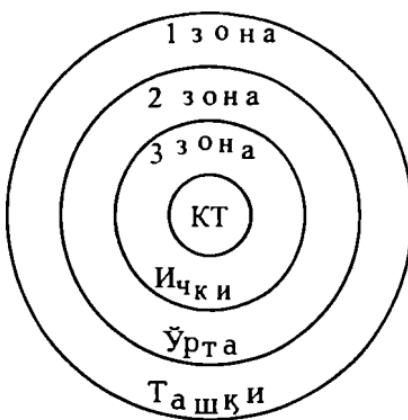
Агар бир бинонинг ичидаги турли химоялаш талабларига эга бўлган обьектлар жойлашган бўлса, бино отсек (бўлма)ларга бўлинади. Шу тарика умумий назоратланувчи макон ичидаги ички периметрлар ажратилади ва рухсатсиз фойдаланишдан ички химоя воситалари яратилади. Периметр, одатда, физик тўсиклар оркали аникланиб, бу тўсиклардан ўтиш электрон усул ёки кўриклаш ходимлари томонидан бажарилувчи маҳсус муолажалар ёрдамида назоратланади.

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

ниш жойи хам хисобга олиниши зарур. Кўп сонли бинолари бўлган ер участкалари хавфсизликни таъминлаш бўйича умумий ёки кисман 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 факат хужум килиниши эҳтимоли кўпроқ бўлган муҳим обьектларга ўрнатиш мумкин. Худди шу тарика участкадаги ҳар бир иморат ёки обьект хужумчини ушлаб колиш имконияти нуктаи назаридан баҳоланади.

Юқоридаги келтирилган талаблар таҳлили кўрсатадики, уларнинг барчаси ахборотни ишлаш ва узагиши курилмаларидан хукуксиз фойдаланиш, ахборот элтувчиларини ўғирлаш ва саботаж имкониятини йўл кўймасликка олиб келади.

Бинолар, иморатлар ва ахборот воситаларининг хавфсизлик тизимини назорат пунктларини бир зонадан иккинчи зонага ўтиш йўлида жойлаштирган ҳолда концентрик ҳалка кўринишида ташкил этиш максадига мувофик хисобланади (2.3-расм).



1-зона. Компьютер тармоғи (КТ) хавфсизлигининг ташки 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;
- бўйм бўш зоналарни чиқариб ташлаш;

3-зона. КТ хавфсизлигининг ички зонаси.

Таъминлаш:

- шахсий компьютерга фойдаланиш факат 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 яккалаш. Бино ва хоналарга киришни назоратловчи автоматик ва ноавтоматик тизимлар ишлатилади. Назорат тизими кундузи ва кечаси кузатиш воситалари билан тўлдирилиши мумкин.

Хавфсизликнинг физик воситаларини танлаш химояланувчи объектнинг муҳимлигини, воситаларга кетадиган харажатни ва назорат тизими ишончлилиги даражасини, ижтимоий жихатларни ва инсон нафси бузуклигини олдиндан ўрганишга асосланади. Бармоқ, кафтлар, кўз тўр пардаси, қон томирлари излари ёки нутқи аниклаш каби биометрик индентификациялаш ишлатилиши мумкин. Шартнома асосида техник воситаларга хизмат кўрсатувчи ходимларни объектга киритишнинг маҳсус режими кўзда тутилган. Бу шахслар идентификацияланганларидан сўнг объектга кузатувчи ҳамроҳлигида киритилади. Ундан ташқари, уларга аник келиш режими, маконий чегараланиш, келиб-кетиш вакти, бажарадиган иш характеристи ўрнатилади.

Нихоят, бино периметри бўйича бостириб киришни аникловчи турли датчиклар ёрдамида комплекс кузатиш ўрнатилади. Бу датчиклар объектни қўриклишнинг марказий пости билан боғланган ва бўлиши мумкин бўлган бостириб кириш нукталарини, айникса ишланмайдиган вактларда, назорат килади.

Вакти-вакти билан эшиклар, ромлар, том, вентиляция туйнуклари ва бошқа чикиш йўлларининг физик химояланиш ишончлилигини текшириб туриш лозим.

Ҳар бир хонага ичидаги нарсанинг муҳимлилигига боғлик фойдаланиш тизимиға эга бўлган зона сифатида каралади. Кириш-чикиш ҳуқуки тизими шахс ёки объект муҳимлигига боғлик ҳолда селекцияли ва даражалари бўйича рутбалangan бўлиши шарт. Кириш-чикиш ҳуқуки тизими марказлашган бўлиши мумкин (руҳсатларни бошқариш, жадвал ва календар режаларининг тузилиши, кириш-чикиш ҳуқукининг ёзма намуналари ва х.).

Назорат тизимини вакти-вакти билан текшириб туриш ва уни доимо ишга лаёкатли ҳолда саклаш лозим. Буни ихтисослашган бўлинмалар ва назорат органлари таъминлайди.

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

Юкорида келтирилганларга хulosса килиб, компьютер тармокларини химоялашда ахборот хавфсизлиги сиёсати қандай аникланиши хусусида сўз юритамиз. Одатда, кўп сонли фойдаланувчиларга эга бўлган корпоратив компьютер тармоклари учун маҳсус «хавфсизлик сиёсати» деб аталувчи, тармоқда ишлашни маълум тартиб ва коидаларга бўйсундирувчи (регламентловчи) хужоат тузилади.

Сиёсат одатда, икки кисмдан иборат бўлади: умумий принциплар ва ишлашнинг муайян коидалари. Умумий принциплар Internetда хавфсизликка ёндашишни аникласа, коидалар нима рухсат этилишини ва нима рухсат этилмаслигини белгилайди. Коидалар муайян муолажалар ва турли қўлланмалар билан тўлдирилиши мумкин.

Одатда, хавфсизлик сиёсати тармок асосий сервисларидан (электрон почта, WWW ва х.) фойдаланишни регламентлайди ҳамда тармокдан фойдаланувчиларни улар қандай фойдаланиш хукукига эга эканликлари билан таништиради. Бу эса ўз навбатида фойдаланувчиларни аутентификациялаш муолажасини аниклайди.

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

Автоматлаштирилган комплекс ҳимояланган хисобланади, қачонки барча амаллар обьектлар, ресурслар ва муолажаларни бевосита химоясини таъминловчи катъий аникланган коидалар бўйича бажарилса (2.4-расм).

## Хавфсизлик

қоидалари



2.4-расм. Ахборот хавфсизлиги сиёсатини тъминлашнинг асосий қоидалари.

Химояга кўйиладиган талабларнинг асосини таҳдидлар рўйхати ташкил этади. Бундай талаблар ўз навбатида химоянинг зарурӣ вазифалари ва химоя воситаларини аниклайди.

Демак, компьютер тармоғида ахборотни самарали химоясини тъминлаш учун химоя тизимини лойиҳалаш ва амалга ошириш уч боскичда амалга оширилиши керак.

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

Биринчи боскичда компьютер тармоғининг заиф элементлари таҳлилланади, таҳдидлар аникланади ва баҳоланади, химоянинг оптималь воситалари танланади. Хавф-хатарни таҳлиллаш хавфсизлик сиёсатини қабул килиш билан тугалланади.

Иккинчи боскич – хавфсизлик сиёсатини амалга оширишдаги молиявий харажатларни хисоблаш ва бу масалаларни ечиш учун мос воситаларни танлаш билан бошланади. Бунда танланган воситалар ишланинг ихтилоғли эмаслиги, воситаларни етказиб бе-рувчиларнинг обрўси, химоя механизмлари ва бериладиган кафолатлар хусусидаги тўла ахборот олиш имконияти каби омиллар хисобга олиниши зарур. Ундан ташкири, ахборот хавфсизлиги бўйича асосий қоидалар акс эттирилган принциплар хисобга олиниши керак.

Учинчи боскич – хавфсизлик сиёсатини мададлаш боскичи энг муҳим хисобланади. Бу боскичда ўтказиладиган тадбирлар нияти бузук одамларнинг тармокка бостириб кишини доимо назорат килиб туришни, ахборот обьектини химоялаш тизимидағи «рахна»ларни аниклашни, конфиденциал маълумотлардан рухсатсиз фойдаланиш холларини хисобга олишни талаб этади. Тармок хавфсизлиги сиёсатини мададлашда асосий жавобгарлик тизим маъмури бўйнида бўлади. У хавфсизликнинг муайян тизими бузилишининг барча холларига оператив муносабат билдириши, уларни таҳлиллаши ва молиявий воситаларнинг максимал тежалишини хисобга олган ҳолда химоянинг 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 химоялаш соҳасига таалтуқли ҳужжатлар хусусида сўз юритилади. Ҳужжатларда қўйилган талаблар давлат секторида ёки таркибида давлат сири бўлган ахборотни ишловчи тижорат ташкилотларида бажарилиши шарт. Бошқа гижорат тузилмалар учун ҳужжатлар тавсия характерига эга.

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

Бу ҳужжатда хавфсизликнинг исталган даражасига эришиш бўйича асосланган чораларни ишлаб чиқиш ва қўллаш мақсадида автоматлаштирилган тизимларнинг ахборотни химоялаш нуктаи назаридан ишлаши шароитлари бўйича туркумланиши келтирилган. Ҳар бир химоялаш бўйича маълум минимал талаблар мажмуи орқали характерланувчи химояланишнинг тўккизта 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
<b>Фойдаланиши башқариш қисм тизимиға</b>									
<i>Идентификациялаш, ҳақиқийлигин текшириш ва субъектлар фойдаланишининг назорати</i>									
– тизимга	x	x	x	x	x	x	x	x	x
– терминалларга, ЭҲМга, ЭҲМ тармоғи узелларига, алоқа каналларига, ЭҲМни ташки курилмаларига	–	–	–	x	–	x	x	x	x
– дастурларга	–	–	–	x	–	x	x	x	x
– жилдларга, каталогларга, файлларга, қайдларга	–	–	–	x	–	x	x	x	x
Ахборот оқимларини башқариш	–	–	–	x	–	–	x	x	x
<b>Рўйхатга ва ҳисобга олиш қисм тизимиға</b>									
Рўйхатга ва ҳисобга олиш									
– субъектларнинг тизимга(дан) киришини (чиқишини)	x	x	x	x	x	x	x	x	x
– босма (график) хужжатларни беришни	–	x	–	x	–	x	x	x	x
– дастурни ва жараёнларни (топшириқлар, масалалар) ишга туширишни (тугаллашни)	–	x	–	x	–	x	x	x	x
– субъект дастурларидан фойдаланиши (химояланувчи файллардан фойдаланиш, уларни яратиш ва йўкотиш, алоқа линиялари ва каналлари оркали узатишни)	–	–	–	x	–	x	x	x	x

- субъект дастурларидан-фойдаланишни (терминалардан, ЭХМдан, ЭХМ тармоғи узелларидан, алоқа каналларидан, ЭХМ ташки қурилмаларидан, дастурли жилдлардан, катлоглардан, файллардан, кайдлар ҳошияларидан фойдаланишни)	-	-	-	x	-	x	x	x	x
- фойдаланувчи субъектлар ваколатларини ўзгартиришларни	-	-	-	-	-	-	x	x	x
- химояланувчи фойдаланиш объектнинг яратилишини	-	-	-	x	-	-	x	x	x
Ахборот элтувчиларини ҳисобга олиш	x	x	x	x	x	x	x	x	x
Оператив хотира ва ташки тўплагичларни тозалаш	-	x	-	x	-	x	x	x	x
Химояни бузишга уринишни сигнализацияси	-	-	-	-	-	x	x	x	x
<i>Криптографик қисм тизимиға</i>									
Конфиденциал ахборотни шифрлаш	-	-	-	-	-	-	x	x	x
Фойдаланишни турли субъектларига (субъектлар грухига) тегишли ахборотни турли калитларда шифрлаш	-	-	-	-	-	-	-	-	x
Аттестациядан ўтган (сертификацияланган) криптографик воситалардан фойдаланиш	-	-	-	-	-	-	-	x	x
<i>Яхлитликни таъминловчи қисм тизимиға</i>									
Дастурий воситалар ва ишланувчи ахборотнинг яхлитлигини таъминлаш	x	x	x	x	x	x	x	x	x
Ҳисоблаш техникаси воситалари ва ахборот элтувчиларини қўриклаш	x	x	x	x	x	x	x	x	x

Ахборот химояси маъмуратининг (хизматининг) мавжудлиги	-	-	-	x	-	-	x	x	x
Ахборот химояси тизими-ни вакти-вакти билан тестлаш	x	x	x	x	x	x	x	x	x
Ахборот химояси тизими-ни тиклаш воситаларининг мавжудлиги	x	x	x	x	x	x	x	x	x
Сертификацияланган химоя воситаларидан фойдаланиш	-	x	-	x	-	-	x	x	x

Синфлар ахборот ишланиши хусусиятлари билан бир-биридан фарқланувчи учта гурухга бўлинади. Ҳар бир гурух ичидаги ахборотнинг кийматлигига (конфиденциаллигига) боғлик холда химоя бўйича талаблар иерархияси ва демак, химояланиш синфлари сакланади. Ҳар бир гурух кўрсаткичларини, охиргисидан бошлаб кўриб чиқамиз.

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

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

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

Умумий холда химоялаш тадбирлари 4 та кисм тизимни ўз ичига олади:

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

Хисоблаш техникаси воситаларини рухсатсиз фойдаланишдан химояланиш кўрсаткичлари «Хисоблаш техникаси воситалари. Ахбортни рухсатсиз фойдаланишдан химоялаш. Химоялаш кўрсаткичлари» деб аталувчи хужжатда келтирилган. Унда ахбортдан рухсатсиз фойдаланишдан химояланишнинг 7-синфи аникланган. Энг пастки синф – еттинчи, энг юкори синф – биринчи. Ҳар бир синф химояланиш талабларини олдингисидан мерос килиб олади. Химоянинг амалга оширилган моделлари ва уларни текшириш ишончлилигига боғлиқ ҳолда синфлар тўртта гурухга ажратилади.

Биринчи гурухда факат еттинчи синф бўлади (минимал химояланиш).

Иккинчи гурух танланадиган химоя билан характерланиб олтинчи ва бешинчи синфларни ўз ичига олади. Танланувчи химоя номма-ном айтилган субъектларнинг тизимнинг номма-ном айтилган обьекларидан фойдаланишни кўзда тутади. Бунда ҳар бир «субъект-объект» жуфтлиги учун фойдаланишнинг рухсат этилган турлари аникланиши шарт. Фойдаланиш назорати ҳар бир обьектга ва ҳар бир субъектга кўлланилади.

Учинчи гурух муҳтор хукукли химоя билан характерланиб, тўртинчи, учинчи ва иккинчи синфларни ўз ичига олади. Муҳтор хукукли химоя тизимнинг ҳар бир субъект ва обьектига, унинг мос иерархиядаги ўрнини кўрсатувчи туркумлаш белгисини бериш тизимдан фойдаланувчи ёки маҳсус ажратилган субъект томонидан амалга оширилади. Ушбу хукукга кирувчи синфлардан талаб килинадиган нарса-фойдаланишнинг диспетчерини (reference monitor–хаволалар монитори) амалга оширилиши. Фойдаланиш назорати барча обьектларга нисбатан ҳар кандай субъект томонидан очик ва яширин фойдаланишда амалга оширилиши шарт. Фойдаланишга рухсат бериш факат танланадиган ва муҳтор хукукли коидаларнинг биргаликда рухсати бўлгандағина амалга оширилиши мумкин.

Тўртинчи гурух тасдиқланган химоя билан характерланиб факат биринчи синфи ўз ичига олади.

Тизим химояланиш синфини олиши учун қуидагиларга эга бўлиши лозим:

- тизим бўйича маъмур кўлланмаси;
- фойдаланувчи кўлланмаси;
- тестлаш ва конструкторлик хужжатлар.

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

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

- хукукий;
- ташкилий-маъмурӣ;
- инженер-техник.

Хукукий чораларга компьютер жиноятчилиги учун жавобгарликни белгиловчи меъёрларни ишлаб чикиш, дастурчиларнинг муаллифлик хукукини химоялаш, жиноий ва фукаролик конун-чилигини ҳамда суд жараёнини такомиллаштириш киради. Уларга яна компьютер тизимларини яратувчи устидан жамоатчилик назорати масалалари ҳамда, агар компьютер тизимларининг битимга келган мамлакатларнинг ҳарбий, иктисадий ва ижтимоий жиҳатларига таъсири бўлса, чеклашлар бўйича мос ҳалқаро шартномаларни кабул килиш киради. Факат охирги йилларда компьютер жиноятчиликларга қарши хукукий кураш муаммолари бўйича ишлар пайдо бўлди.

Ташкилий-маъмурӣ чораларга компьютер тизимларини кўриклаш, ходимларни танлаш, маҳсус мухим ишларни бир киши томонидан бажарилиш ҳолларига йўл кўймаслик, марказ ишдан чиққанида унинг ишга лаёқатлигини тиклаш режасининг мавжудлиги, барча фойдаланувчилардан (юкори раҳбарлар ҳам бунга киради) химояланиш воситаларининг универсаллиги, марказ хавф-сизлигини таъминлашга мутасадди шахсларга жавобгарликни юклаш, марказ жойланадиган жойни танлаш ва х. киради.

Инженер-техник чораларга компьютер тизимини рухсатсиз фойдаланишдан химоялаш, мухим компьютер тизимларини резервлаш, ўғирлаш ва диверсиядан химояланишни таъминлаш, резерв электр манбаи, хавфсизликнинг маҳсус дастурий ва ашпарат воситаларини ишлаб чикиш ва амалга ошириш ва х. киради.

## **III боб. АХБОРОТ ХАВФСИЗЛИГИНИНГ ҲУҚУҚИЙ ВА ТАШКИЛИЙ ТАЪМИНОТИ**

### **3.1. Ахборот хавфсизлиги соҳасида ҳуқукий бошқариш**

Ахборот хавфсизлигининг ҳуқукий таъминоти – ахборотни химоялаш тизимида бажарилиши шарт бўлган конунлаштирувчи далолатномалар мөъёрий-ҳуқукий хужжатлар, коидалар йўрикномалар, кўлланмалар мажмуи. Ҳозирда ахборот хавфсизлигининг ҳуқукий таъминоти масаласи ҳам амалий, ҳам конунчилик жихатидан фаол ўрганиб чиқилмоқда.

Компьютер жиноятчиликларини килиш инструментлари сифатида телекоммуникация ва ҳисоблаш техникаси воситалари, дастурий таъминот ва интеллектуал биљим ишлатилади. Компьютер жиноятчиликларини қилиш соҳаси сифатида нафакат компьютерлар, глобал ва корпоратив тармоқлар (Internet/Intranet), балки ахборот технологиясининг замонавий, юкори унумли воситалари ҳамда ахборотнинг катта ҳажми ишланадиган, масалан, статистик ва молия институтлари, танланади.

Шу сабабли, ҳар қандай ташкилот фаолиятини турли-туман ахборотни олиш учун кўлда ёки ҳисоблаш техникаси воситалари ёрдамида ишлаш, ахборотни таҳлиллаш натижасида қандайдир муайян счимларни олиш ва уларни алока каналлари орқали узатишсиз тасаввур этиб бўлмайди. Компьютерга ҳам тажовуз обьекти, ҳам тажовуз килувчи инструмент сифатида қараш мумкин. Агар компьютер факт тажовуз обьекти бўлса, конун бузилишини мавжуд ҳуқукий месъёрлар орқали баҳолаш мумкин. Агар компьютер факт инструмент бўлса «техник воситаларни кўллаш» аломати старли бўлади. Юкоридаги тушунчаларни бирлаштириш мумкин компьютер бир вактнинг ўзида ҳам инструмент ҳам обьект. Ҳусусан, бундай вазиятга машина ахборотининг ўғирланиши факти тааллукли.

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

лик. муаллифлик манбаатлари боғлиқ бўлса, жиной жавобгарлик Ўзбекистон Республикаси конунларида бевосига кўзда тутилган.

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



3.1-расм. Ахборот хавфсизлигини таъминлашнинг хуқукий меъёрлар.

Хуқукий бошқариш предметлари қуйидагилар.

ахборот химоясининг хуқукий режими;

- ахборотлаштириш жараёнларида конуний муносабат катнашчиларининг хуқукий мақоми;

субъектларнинг, уларнинг ахборот тузилмалари ва гизимлари ишлиши жараённинг турли боскич ва сатҳларидан хуқукий мақомини хисобга олган ҳолда, муносабатлари тартиби.

Ахборот хавфсизлиги бўйича конунларни Ўзбекистон Республикаси бутун конунлар тизимининг ажралмас кисми сифагида тасаввур килиш мумкин, хусусан:

- таркибида ахборотлаштириш масалаларига доир меъёрлар бўлганинг конституция конунлари:

- таркибида ахборотлаштириш масалаларига доир меъёрлар бўлган умумий асосий конунлар (мулк, ер ости бойликлари, ер, фуқоролар хукуки, фуқаролик, солик хусусида);

- хўжаликнинг алоҳида тузилмаларига, иктисадиётга, давлат органлари тизимиға тегишли бошқариши ва уларнинг макомини аниқлаш бўйича конунлар. Бу конунлар ахборот масалалари бўйича алоҳида меъёрларни ўз ичига олади;

- муносабатларнинг, хўжалик соҳаларининг, жараёнларнинг муайян мухитига бутунлай тегишли маҳсус конунлар. Буларга ахборотлаштириш бўйича конунлар тааллукли;

- ахборотлаштириш соҳасидаги конун талабларининг бажарилишини регламентловчи меъёрий хужжатлар;

- конунлар билан белгиланган ахборотлаштириш соҳасидаги меъёрий хужжатлар;

- таркибида ахборотлаштириш соҳасида конун бузилишига жавобгарлик меъёрлари бўлган Ўзбекистон Республикасининг хукукни муҳофаза килиш конунлари.

Компьютер тармоклари хавфсизлигини таъминловчи давлат хукукий механизмининг ривожланмаган шароитида корхонанинг давлат ва ходимлар жамоаси билан муносабатларни хукукий асосда ростловчи хужжатлари жиддий аҳамиятга эга бўлади. Бундай муҳим хужжатлар таркибига кўйидагиларни киритиш мумкин:

- корхона (фирма, банк) устави;

- жамоа шартномаси;

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

- ишчи ва хизматчиларнинг ички меҳнат тартиб коидалари;

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

### **3.2. Ахборот хавфсизлигининг ташкилий-маъмурий таъминоти**

Ахборотни ишончли химоя механизмини яратишда ташкилий тадбирлар муҳим рол ўйнайди, чунки конфиденциал ахборотлардан руҳсатсиз фойдаланиш асосан, техник жихатлар билан эмас, балки химоянинг элементар коидаларини ёътиборга олмайдиган фойдаланувчилар ва ходимларнинг жинояткорона ҳаракатлари, бепарволиги, совукконлиги ва масъулиятсизлиги билан боғлик.

Ташкилий таъминот конфиденциал ахборотдан фойдаланишга имкон бермайдиган ёки жиддий кийинчилик туғдирувчи ижро чилиарнинг ишлаб-чикариш ва ўзаро муносабатларини меъёрий-хукукий асосида регламентлашдир.

Ташкилий тадбирларга куйидагилар киради:

– хизматчи ва ишлаб чикариш бино ва хоналарни лойихалашда, куришда ва жиҳозлашда амалга ошириладиган тадбирлар. Бу тадбирларнинг асосий максади худудга ва хоналарга яширинча кириш имконини йўқотиш; одамларнинг ва транспортнинг юриши назоратининг кулайлигини таъминлаш; фойдаланишнинг алоҳида тизимиға эга бўлган ишлаб-чикариш зоналарини яратиш ва х.;

– ходимларни танлашда амалга ошириладиган тадбирлар. Бу тадбирларга ходимлар билан танишиш, конфиденциал ахборот билан ишлаш қоидалари билан ишлашни ўргатиш, ахборот химояси қоидасини бузганилиги учун жавобгарлик даражаси ва х. билан таништириш киради;

– ишончли пропуск режимини ва ташриф буюрувчиларнинг назоратини ташкил килиш;

– хона ва худудларни ишончли кўриклиш;

– хужжатлар ва конфиденциал ахборот элтувчиларини саклаш ва ишлатиш, шу жумладан, кайд этиш, бериш, бажариш ва кайтариш тартибларига риоя килиш;

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

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

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

– ишга қабул килишда сухбат. Сухбат натижасида номзоднинг мос бўш жойга қабул килиниши мақсадга мувофиқлиги аникланади;

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

корхона тижорат сирларини саклаши бўйича тилхат ва фирма сирларини ошкор килмасликка ваъда беради;

– ходимларни конфиденциал ахборот билан ишлаш қоидалари ва муолажаларига ўқитиш. Ходимларни ўқитишда нафақат ишлабчиқариш кўникумларига эга бўлиш ва уларни юкори даражада саклаш, балки уларни саноат (ишлаб чиқариш) маҳфийлиги ахборот хавфсизлиги, интеллектуал мулк ва тижорат сирлари химояси талабларини бажариш зарурлигига катъий ишонч руҳида тарбиялаш кўзда тутилади. Мунтазам ўқитиш раҳбарият ва ходимларнинг корхона тижорат манфаатларини химоя килиш масалалари бўйича билимдонлик даражасини ошишига имкон яратади;

– ишдан бўшаётганлар билан сұхбат. Сұхбат давомида ишдан бўшаётган ходимнинг фирма сирларини фош килмасликка катъий ваъда бериши лозимлиги таъкидланади ва бу ваъда, одатда, тилхат оркали расмийлаштиради.

Тадбирларнинг мухим йўналишларидан бири иш юритиш ва хужжат юритиш тизимини пухта ташкил этиш хисобланади. Бу эса ўз навбатида иш юритиш тартибини, хужжатларни кайдлаш, ишлаш, саклаш, йўкотиш ва мавжудлигини хамда тўғри бажарилишини назорат килишни таъминлайди. Тизимни амалга оширишда хужжатлар · хавфсизлигига ва ахборот конфиден-циаллигига алоҳида эътибор бериш лозим.

Ахборотни хужжатлаштириш катъий беътидан гиланган қоидалар ёрдамида амалга оширилади. Бу қоидаларнинг асосийлари ГОСТ 6.38-90 «Ташкилий-бошқарувчи хужжатлар тизими. Хужжатларни расмийлаштиришга талаблар», ГОСТ 6.10.4-84 «Унификацияланган хужжатлар тизими. Хисоблаш техника воситалари оркали яратилувчи машина элтувчиларидағи ва машинограммалардаги хужжатларга хукукий куч бериш» кабилар баён этилган. Бу ГОСТларда ахборотга хужжат хукукини берувчи 31 та реквизитлар кўзда тутилган, аммо бу реквизитларнинг барчасининг хужжатда мавжудлиги шарт эмас. Асосий реквизит – матн. Шу сабабли, ҳар қандай равон баён этилган матн хужжат хисобланади ва унга хукукий куч бериш учун сана ва имзо каби мухим реквизитларнинг мавжудлиги кифоя.

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

ловчи маҳсус маъмурий хизматни яратиш талаб килинади. Унинг штат тузилмаси, сони ва таркиби фирманинг реал эктиёлари, ахборотининг конфиденциаллик даражаси ва хавфсизлигининг умумий холати оркали аникланади.

- Маъмурый тадбирларга қўйидагилар киради:
  - операцион тизимнинг тўғри конфигурациясини мададлаш;
  - иш журналларининг назорати;
  - пароллар алмашишининг назорати;
  - химоя тизимида «раҳна»ларни аниклаш;
  - ахборотни химояловчи воситаларни тестлаш.
- Тармок операцион тизимининг тўғри конфигурациясини мададлаш масаласини, одатда, тизим маъмур хал этади. Маъмур операцион тизим (одамлар эмас) риоя қилиши лозим бўлган маълум коидаларни яратади. Тизимни маъмурлаш – конфигурация файлларини тўғри тузишдир. Бу файлларда (улар бир нечта бўлиши мумкин, масалан, тизимнинг ҳар бир кисмiga биттадан файл) тизим ишлаши коидаларининг тавсифи бўлади.

Хавфсизлик маъмурни компютер тармоғи холатини оператив тарзда (тармок компьютерлари химояланиши холатини кузатиш оркали) ва оператив бўлмаган тарзда (ахборот химояси тизимидаги воеаларни кайдловчи журналларни тахлиллаш оркали) назоратлаш лозим. Ишчи станциялар сонининг ошиши ва турли туман компонентлари бўлган дастурий воситаларнинг ишлатилиши ахборот химояси тизимидағи ходисаларни қайдлаш журналлар ҳажмини жиддий ошишига олиб келади. Журналлардаги маълумотлар ҳажми шунчалик ошишиб кетиши мумкинки, маъмур улар таркибини жоиз вакт мобайнида тахлиллай олмайди.

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

Ундан ташқари, бундай коидаларга асосланган тизим-статик, котиб колган тизим. У фактат қатъий маълум хужумларга қарши кўра ошиши мумкин. Олдиндан кўзда тутилмаган қандайдир янги таҳдиднинг пайдо бўлишида тармок хужуми нафакат муваффакиятли, балки тизим учун кўринмайдиган бўлиши мумкин. Шу-

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

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

### **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, тасдикланган юкори сифатли ечимлар ва методологиялар кайд этилган. Иккинчидан, стандартлар ва спецификациялар аппарат-

дастурий тизимлар ва уларнинг компонентларининг ўзаро қўшила олишигини таъминловчи асосий восита хисобланади. (Internet-уюшмада бу восита ҳакиқатдан самарали ишламоқда).

Стандартлар ва спецификацияларнинг бир-биридан жиддий фарқланувчи иккита гурухини ажратиш мумкин:

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

- химоя воситалари ва усуулларини амалга ошириш ва улардан фойдаланишинг турли жихатларини регламентловчи спецификациялар.

Бу гурухлар маълумки, ихтилофга бормайдилар, балки бир-бирини тўлдирадилар. Баҳолаш стандартлари ташкилий ва архитектуравий спецификациялар вазифасини ўтаган холда ахборот тизимларининг ахборот хавфсизлиги нуқтаи назаридан муҳим бўлган тушунчалари ва жихатларини тавсифлайди. Спецификациялар эса архитектура белгилаган ахборот тизимини қандай қуриш 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. Муболагасиз тасдиқлаш мумкинки, «Тўқ сарик китоб»и ахборот хавфсизлигининг тушунчалар негизини ифодалайди. Ундаги тушунчаларнинг санаб ўтишининг ўзи етарли: *хавфсиз ва ишончли тизимлар, хавфсизлик сиёсати, кафолатлик даражаси, ҳисобкитоблилиги, ишончли ҳисоблаш асоси, мурожсаатлар 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 хисобланади. Бу ҳужжат икки кисмдан иборат. Биринчи кисм изоҳнинг ўзига бағишлиланган бўлса, иккинчи кисмида ўзига хос ёки тармоқ конфигурациялари учун айниқса, муҳим бўлган *хавфсизлик сервислари тавсифланади*. Биринчи кисмга киритилган энг муҳим тушунчалардан бири – тармоқдаги ишончли ҳисоблаш асоси. Муҳим жихат-

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

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

Бахолаш стандартларидан яна бири «*Европа мамлакатларининг уйгулаштирилган мезонлари*»да ахборот тизими ишлаши лозим бўлган шароитларга априор шартлар йўқ. Фараз қилинади, аввал баҳолаш максади ифодаланади, сўнгра сертификациялаш органи бу максадга қанчалик тўлиқ эришилишини, яъни, муайян вазиятда хавфсизликнинг архитектураси ва амалга оширилиши механизмларининг қанчалик корректлигини ва самаралилигини аниклайди. Баҳолаш максадини ифодалашни енгиллаштириш ниятида стандартда ҳукumat ва тижорат тизимларига хос функционалликнинг ўнта тахминий синфлари тавсифланган.

Ушбу стандартда ахборот технологиялар тизимлари ва маҳсулотлари ўртасидаги фарқ таъкидланади, аммо таалабларини унификациялаш ниятида ягона – баҳолаш обьекти тушунчаси киритилиди. Стандартда хавфсизлик функциялари (сервислари) ва уларни амалга оширувчи механизмлар орасида фарқнинг кўрсатилиши ҳамда кафолатланишнинг икки жиҳати – хавфсизлик воситаларининг *самарадорлиги* ва *корректлигининг* ажратилиши мухим хисобланади. Баҳолаш стандартлари гурухига ахборот хавфсизликнинг муайян, аммо мухим ва мураккаб жиҳатини регламентловчи АҚШнинг «*Криптографик модуллар учун хавфсизлик таалаблари*» Федерал стандарти ҳамда «*Ахборот технологиялар хавфсизлигини баҳоловчи мезонлар*» халқаро стандарти таалукли.

Техник спецификациялар орасида биринчи ўринга, сўзсиз, X800 «Очик тизимлар ўзаро харакати учун хавфсизлик архитектураси» хужжатини кўйиш лозим. Бу хужжатда хавфсизликнинг энг мухим тармок сервислари ажратилган: *аутентификация, фойдаланишини бошқариш, маълумотларни конфиденциаллиги ва ёки яхлитлигини таъминлаш ҳамда килинган харакатдан танишининг мумкин эмаслиги*. Сервисларни амалга ошириш учун хавфсизликнинг

куйидаги тармок механизмлари ва уларнинг комбинациялари кўзда тутилган: *шифрлаш*, *электрон рақамли имзо*, фойдаланишини бошкариш, маълумотлар яхлитлигининг назорати, аутентификация, *трафикни тўлдириш*, *маршрутлашни бошқариш*, *нотаризация*. Хавфсизликнинг сервислари ва механизмлари амалга оширилувчи етти сатҳли этalon моделининг сатҳлари танланган. Нихоят, таксимланган конфигурациялар учун хавфсизлик воситаларининг маъмурлаш масалалари батафсил кўриб чиқилган.

Internet – ўюшманинг RFC 1510 «Аутентификациянинг тармоқ сервери Kerberos (VS)» спецификацияси хусусий, аммо мухим ва долзарб муаммога турли таксимланган мухитда тармокка ягона кириш концепциясини мададлаган холда аутентификациялашга тегишли.

Kerberos аутентификациялаш сервери ишончли учинчи гараф бўлиб, хизмат қўрсатилувчи субъектларнинг маҳфий калитларига эга ва уларга хакикийликнинг жуфтлашиб текширишда ёрлам беради. Kerberosнинг мижоз компонентларининг аксарият замонавий операцион тизимларда мавжудлиги унинг канчалик мухим жанлигилан далолат беради.

IPsec техник спецификацияси тармоқ сатҳида конфиденциаллик ва яхлитлик воситаларининг гўлиқ тўпламини тавсифлаган холда, муболағасиз фундаментал аҳамиятга эга. IPsec асосида юкорирок сатҳ (татбикӣ сатҳга кадар) протоколларини химоялаш механизми ҳамда хавфсизликнинг тугалланган воситалари, хусусан виртуал хусусий тармоклар курилади. Албатта, IPsec криптографик механизмларига ва калит инфратузилмаларига таянади.

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

Юкорида эслатиб ўтилган инфратузилма нуктаи 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 атрибулар каркаслари» (The Directory: Public-key and attribute certificate frameworks) тавсиялари жуда мухим хисобланади. X.509 тавсияларида очик калитлар ва атрибулар яъни очик калитлар инфратузилмаси ва имтиёзларни

бошқаришнинг базавий элементлари сертификатларининг формати тавсифланган.

Маълумки, ахборот хавфсизлигини таъминлаш комплекс муаммо бўлиб, конуний, маъмурӣ, муолажавий ва дастурий-техник сатҳларда чораларни келишилган холда кўришни талаб этади. Маъмурӣ сатҳнинг базавий ҳужжати ташкилот *хавфсизлиги сиёсатини* ишлаб чиқишида ва амалга оширишда Internet – уюшманнинг «Ташкилот ахборот хавфсизлиги бўйича қўлланма»си (Site Security Handbook) наъмунали кўмакчи вазифасини ўташи мумкин. Унда хавфсизлик сиёсати муолажаларини шаклланти-рилишининг амалий жиҳатлари ёритилади, маъмурӣ ва муолажа-вий сатҳларнинг асосий тушунчалари изоҳланади, тавсия этувчи харакатларнинг сабаблари кўрсатилган, хавф-хатарлар тахлили, ахборот хавфсизлигининг бузилишига муносабат ва бузилиш бартараф этилганидан кейинги харакат мавзуларига тўхтаб ўтилган.

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

Корпоратив ахборот тизимини ривожлантиришда ва қайта тузища «Internet-хизмат билан таъминловчуни қандай танлаш лозим» (Site Security Handbook Addendum for ISPs) тавсияси сўзсиз фойдалидир. Биринчи галда унинг коидаларига ташкилий ва архитектуравий химоялашни шакллантириш жараённида риоя килиш лозим.

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

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

заси. Маълумотларни шифрлаш алгоритми», О‘з DSt 1106:2006 «Ахборот технологияси. Маълумотларни криптографик муҳофазаси. Хешлаш функцияси» ва О‘з DSt 1108:2006 «Ахборот технологияси. Очик тизимлар ўзаро боғликлиги. Электрон ракамли имзо очик қалити сертификати ва атрибут сертификатининг тузилмаси» стандартларини ва РН 45-187:2006 «Хавфсизлик талаблари» бошқарув хуҷоатини кўрсатиб ўтиш мумкин. Ушбу марказ томонидан ишлаб чиқилган стандартлар №05-11 12.04.2006 йилда ўзбекистон стандартлаштириш, метрология ва сертификациялаш агентлиги томонидан тасдикланган.

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

# IV боб. АХБОРОТНИ ХИМОЯЛАШНИНГ КРИПТОГРАФИК УСУЛЛАРИ

## 4.1. Криптографиянинг асосий қондалари ва таърифлари

Ахборотни химоялашнинг аксарият механизмлари асосини шифрлаш ташкил этади. *Ахборотни шифрлаш* деганда очик ахборотни (дастлабки матнни) шифрланган ахборотга ўзгартириш (шифрлаш) ва аксинча (расшифровка килиш) жараёни тушунилади. Шифрлаш криптотизимининг умумлаштирилган схемаси 4.1-расмда келтирилган.



4.1-расм. Шифрлаш криптотизимининг умумлаштирилган схемаси.

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

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

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

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

мумкин. Муайян калит ёрдамида шифрланган ахборот фактат ушбу калит эгаси (ёки эгалари) томонидан расшифровка килиниши мумкин.

Ахборотни тескари ўзгартириш күйидаги күринишига эга:

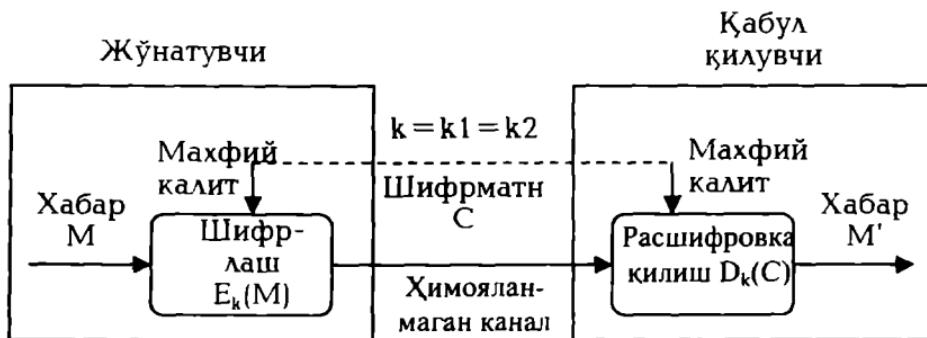
$$M' = D_{k_2}(C)$$

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

Криптотизимларнинг иккита синфи фарқланади:

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

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



4.2-расм. Симметрик шифрлаш криптотизимнинг схемаси.

Электрон хужжатларни узатишининг конфиденциаллигини симметрик криптотизим 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 сакланади. Шахсий калит элтувчиси эгасидан бошқа одамларнинг фойдаланишига карши чоралар кўрилиши шарт.

Симметрик шифрлаш ахборотни «ўзи учун», масалан, эгаси йўклигига ундан рухсатсиз фойдаланишни олдини олиш максадида, шифрлашда жуда кулагай хисобланади. Бу танланган файлларни архивли шифрлаш ва бутун бир мантикий ёки физик дискларни шаффофф (автоматик) шифрлаш бўлиши мумкин.

Симметрик шифрлашнинг ноқулайлиги – ахборот алмашинуви бошланмасдан олдин барча манзилатлар билан маҳфий калитлар билан айирбошлаш заруриятидир. Симметрик криптотизимда маҳфий калитни алоканинг умумфойдаланувчи каналлари орқали узатиш мумкин эмас. Маҳфий калит жўнатувчига ва қабул килувчига калитлар таркатилувчи 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 ножоиздир. Хакикатан, калит обрўсизлантирилганда (йўкотилганида, ўғирлатилганда) барча абонентларнинг хужжат алмасиши хавф остида колади. Бу холда калитларнинг матрицаси (4.3-расм) ишлатилиши мумкин.

	1	2	3	...	n	
1	$k_{11}$	$k_{12}$	$k_{13}$		$k_{1n}$	1-абонент учун калитлар түплами
2	$k_{21}$	$k_{22}$	$k_{23}$	...	$k_{2n}$	2-абонент учун калитлар түплами
3	$k_{31}$	$k_{32}$	$k_{33}$		$k_{3n}$	3-абонент учун калитлар түплами
	...	...	...	...	...	...
n	$k_{n1}$	$k_{n2}$	$k_{n3}$	...	$k_{nn}$	n-абонент учун калитлар түплами

4.3-расм. Калитлар матрицаси.

*Калитлар матрицаси* абонентларнинг жуфт-жуфт боғланишили жадвалидан иборат. Жадвалнинг ҳар бир элементи  $i$  ва  $j$  абонентларни боғлашга мўлжалланган ва ундан факат ушбу абонентлар фойдалана оладилар. Мос ҳолда, калитлар матрицаси элементлари учун қуидаги тенглик ўринли.

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

Матрицанинг ҳар бир  $i$ - катори муайян  $i$  абонентнинг колган  $N-1$  абонентлар билан боғланишини таъминловчи калитлар түпламидан иборат. Калитлар түплами (тармок түпламлари) криптографик тармокнинг барча абонентлари ўртасида таксимланади. Таксимлаш алоқанинг ҳимояланган каналлари оркали ёки кўлдан-кўлга тарзда амалга оширилади.

Асимметрик криптотизимларда ахборотни шифрлашда ва расшифровка килишда турли калитлардан фойдаланилади:

- очик калит  $K$  ахборотни шифрлашда ишлатилади, маҳфий калит  $k$  дан хисоблаб чиқарилади;

- маҳфий калит  $k$ , унинг жуфти бўлган очик калит ёрдамида шифрланган ахборотни расшифровка килишда ишлатилади.

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

борот алмашнадиган криптографик тармоқ абонентларининг харбирида бўлиши шарт.

Асимметрик шифрлашнинг умумлаштирилган схемаси 4.4-расмда келтирилган.



4.4-расм. Асимметрик шифрлашнинг умумлаштирилган схемаси.

Асимметрик криптотизимда шифрланган ахборотни узатиш қуидагича амалга оширилади:

1. Тайёргарлик боскичи:

абонент *B* жуфт қалитни генерациялади: маҳфий қалит  $k_B$  ва очик қалит  $K_B$ ;

- очик қалит  $K_B$  абонент *A* га ва қолган абонентларга жўналилади.

2. *A* ва *B* абонентлар ўртасида ахборот алмашиш:

- абонент *A* абонент *B*нинг очик қалити  $K_B$  ёрдамида ахборотни шифрлайди ва шифрматни абонент *B*га жўнатади;

- абонент *B* ўзининг маҳфий қалити  $k_B$  ёрдамида ахборотни расшифровка киласди. Ҳеч ким (шу жумладан, абонент *A* хам) ушбу ахборотни расшифровка килаолмайди, чунки абонент *B*нинг маҳфий қалити унда йўқ.

Асимметрик криптотизимда ахборотни химоялаш ахборот қабул килувчи қалити  $k_B$ нинг маҳфийлигига асосланган.

Асимметрик криптотизимларнинг асосий хусусиятлари қуидагилар:

1. Очик калитни ва шифр матнни химояланган канал оркали жүннатиш мумкин, яъни нияти бузук одамға улар маълум бўлиши мумкин.

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

## 4.2. Симметрик шифрлаш тизими

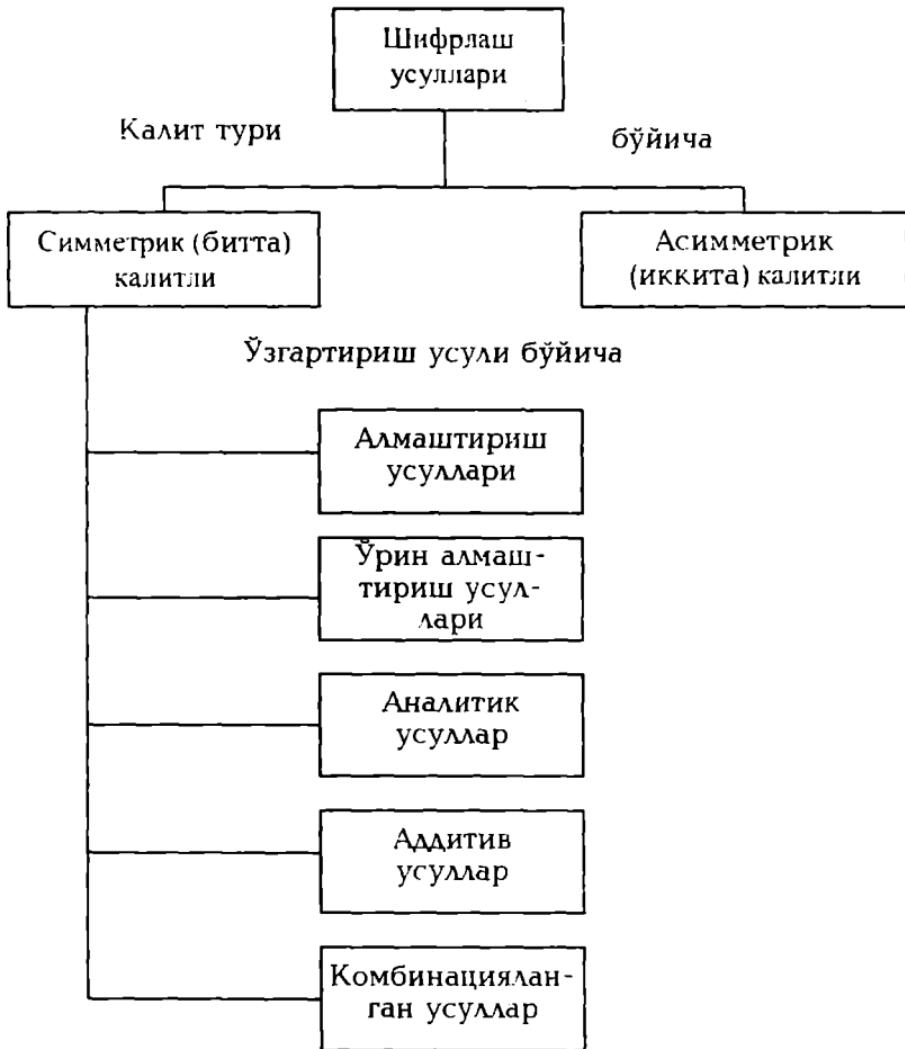
Шифрлаш усуллари турли аломатлари бўйича туркумланиши мумкин. Туркумланиш вариантиларидан бири 4.5-расмда келтирилган.

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

Иккала алфавитдаги символлар ўртасидаги мослик маълум алгоритм бўйича К символлар узунлигига эга бўлган дастребки матн  $T_0$  символларининг ракамли эквивалентларини ўзgartариш оркали амалга оширилади.

**Моноалфавитли алмаштириш алгоритми** куйидаги қадамлар кетма-кетлиги кўринишда ифодаланиши мумкин

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



4.5-расм. Шифрлаш усулларининг туркумланиши.

**2-қадам.**  $L_{oh}$  кетма-кетлигининг ҳар бир сонини  $h_{ii} = (k_1 x h_{oi}(s_{oi}) + k_2)(mod R)$  формула оркали хисобланувчи  $L_{ih}$  кетма-кетлигининг мос сони  $h_{ii}$  га алмаштириш йўли билан  $L_{ih}$  сон кетма-кетлигини шакулантириш, бу ерда,  $k_1$ -ўнлик коэффициент;  $k_2$ -сиљжитиш коэффици-санти. Танланган  $k_1$ ,  $k_2$  коэффициентлар  $h_{ob}$ ,  $h_{ii}$  сонларнинг бир маъноли мослигини таъминлаши лозим,  $h_{ii}=0$  олинганида эса  $h_{ii}=R$  алмашинуви бажарилиши керак.

**3-қадам.**  $L_{th}$  кетма-кетликнинг ҳар бир сони  $h_{ti}(s_{ti})$ ни  $[1 \times R]$  ўлчамли шифрлаш алфавитнинг мос  $s_{ti} \in T_i (i=1, K)$  символи билан алмаштириш йўли билан  $T_i$  шифрматнни хосил килиш.

**4-қадам.** Олинган шифрматн ўзгармас  $b$  узунлиқдаги блокларга ажратилади. Агар охирги блок тўлик бўлмаса блок оркасига маҳсус символ-тўлдирувчилар жойлаштирилади (масалан, \*). **Мисол.** Шифрлаш учун дастлабки маълумотлар қуидагилар:

$T_0 = <\text{ХИМОЯ ХИЗМАТИ}>$

$A_0 = <\text{АБВГДЕЁЖЗИЙКЛМНОРСТУФХЦЧШЪЭЮЯЎКFX}>$

$A_1 = <\text{ОРЁЯТЭ-ЖМЧХАВДИФҚҚСЕЗПИЦГХЛЬШБЮ КГН}>$

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

Алгоритмнинг қадамба-қадам бажарилиши қуидаги натижаларни олинишига олиб келади.

**1-қадам.**  $L_{oh} = <35, 10, 14, 16, 31, 36, 23, 10, 9, 14, 1, 20, 10>$

**2-қадам.**  $L_{th} = <12, 9, 21, 17, 36, 14, 12, 9, 6, 21, 18, 3, 9>$

**3-қадам.**  $T_1 = <\text{ХЖЕФНВХЖТЕКЁЖ}>$

**4-қадам.**  $T_2 = <\text{ХЖЕФ НВХЖ ТЕКЁ Ж***}>$

Расшифровка килишда блоклар бирлаштирилиб  $K$  символли шифрматн  $T_i$  хосил килинади. Расшифровка килиш учун қуидаги бугун сонли тенгламани ечиш лозим:

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

$k_1, k_2, h_{ti}$  ва  $R$  бутун сонлар маълум бўлганда  $h_{ti}$  катталиги п ни саралаш оркали хисобланади. Бу муолажани шифрматнинг барча символларига татбик килиш унинг расшифровка килинишига олиб келади.

Алмаштириш усулининг камчилиги сифатида дастлабки ва берилган матнлар статистик характеристкаларининг бир хиллигидир. Дастлабки матн кайси тилда ёзилганлигини билган криптоаналитик ушлаб колинган ахборотларни статистик ишлаб, икката алфавитдаги символлар ўртасидаги мувофиқликни аниқлаши мумкин.

**Полиалфавитли алмаштириши усуллари** айтарлича юкори криптобардошликка эга. Бу усуллар дастлабки матн символларини алмаштириш учун бир неча алфавитдан фойдаланишга асосланган. Расман полиалфавитли алмаштиришини қуидагича тасаввур этиш мумкин.  $N$ -алфавитли алмаштиришда дастлабки  $A_0$  алфавитдаги  $s_{0i}$  символи  $A_1$  алфавитдаги  $s_{1i}$  символи билан алмаштирилади ва  $x$ .  $s_{0i}$ ни  $A_1$  символ билан алмаштирилганидан сўнг  $S_{0iA_{1i}}$ , символнинг ўринини  $A_1$  алфавитдаги  $S_{1iA_{1i}}$  символ олади ва  $x$ .

Полиалфавитли алмаштириш алгоритмлари ичида **Вижинер жадвали (матрикаси)**  $T_h$  ни ишлагувчи алгоритм энг кенг таркалган. Вижинер жадвали  $[RxR]$  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. Сикиб чикарилган символлар ўнг тарафдаги бўшаган ўринни гўлиради (циклик силжитиш). Агар ўзбек алфавити ишлатилса, Вижинер матрикаси  $[36 \times 36]$  ўлчамга эга бўлади (4.6-расм).

АБВГД.....	.....ЎКГХ
БВГДЕ.....	.....ҚФҲА
ВГДЕЖ.....	.....ҒҲАБ
АБВГ.....	.....ЯЎҚFX

4.6-расм. Вижинер матрикаси.

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

Агар калит сифатида  $\langle F\bar{U}ZA \rangle$  сўзи танланган бўлса, шифрлаш матрикаси бешта катордан иборат бўлади (4.7-расм).

$T_{sh}$	АБВДЕЁЖЗИЙКЛМНОРСТУФҲЦЧШЬЭЮЯЎҚFX_
	FX_АБВДЕЁЖЗИЙКЛМНОРСТУФҲЦЧШЬЭЮЯЎҚ
	ЎҚFX_АБВДЕЁЖЗИЙКЛМНОРСТУФҲЦЧШЬЭЮЯ
	ЗИЙКЛМНОРСТУФҲЦЧШЬЭЮЯЎҚFX_АБВДЕЁЖ
	АБВДЕЁЖЗИЙКЛМНОРСТУФҲЦЧШЬЭЮЯЎҚFX_

4.7-расм. «Fўза» калити учун шифрлаш матрикаси.

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

**1-қадам.** Узунлиги  $M$  символли калит  $K$  ни танлаш.

**2-қадам.** Танланган калит  $K$  учун  $[(M+1), R]$  ўлчамли шифрлаш матрикаси  $T_{sh} = (b_{ij})$  ни қуриш.

**3- қадам.** Дастребки матннинг ҳар бир символи  $s_{or}$  тагига калит символи  $k_m$  жойлаштирилади. Калит кераклича тақорланади.

**4-қадам.** Дастребки матн символлари шифрлаш матрицаси  $T_m$ дан қуидаги коида бўйича танланган символлар билан кетма-кет алмаштирилади.

1)  $K$  калитнинг алмаштирилувчи  $s_{or}$  символга мос  $k_m$  символи аникланади;

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

3)  $s_{or} = b_{ii}$  шарт бажарилувчи  $j$  устун аникланади.

4)  $s_{or}$  символи  $b_{ij}$  символи билан алмаштирилади.

**5-қадам.** Шифрланган кетма-кетлик маълум узунликдаги (масалан 4 символли) блокларга ажратилади. Охирги блокнинг бўш жойлари маҳсус символ-тўлдирувчилар билан тўлдирилади.

Расшифровка килиш қуидаги кетма-кетликда амалга оширилади.

**1-қадам.** Шифрлаш алгоритмининг 3-қадамидагидек шифрматн 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 каноатлантирувчи  $i$  категор аникланади.  $i$ -каторда  $b_{ij} = s_{ir}$  элемент аникланади. Расшифровка килинган матнда  $r$  – ўрнига  $b_{ij}$  символи жойлаштирилади.

**3-қадам.** Расшифровка килинган матн ажратилмасдан ёзилади. Хизматчи символлар олиб ташланади.

**Мисол.** К=<ҒЎЗА> калити ёрдамида Т=<ПАХТА ФАРАМИ> дастребки матнни шифрлаш ва расшифровка килиш талаб этилсан. Шифрлаш ва расшифровка килиш механизми 4.8-расмда келтирилган.

Полиалфавитги алмаштириш усууларининг криптобардоцилиги оддий алмаштириш усууларига караганда айтгарлича юкори. чунки уларда дастребки кетма-кетликнинг бир хил символлари турли символлар билан алмаштирилиши мумкин. Аммо шифрнинг статистик усууларига бардошлилиги калит узунлигига боғлиқ.

Дастребки матн ПАХТА ФАРАМИ

Калит ҒЎЗА ҒЎЗА ҒЎЗА

Алмаштирилган

сўнгти матн МЎЮТИЯЕАНЎУИ

Шифрматн	МҮЮТ ФЯЕАНҮҮИ
Калит	ФҮЗА ФҮЗА ФҮЗА
Расшифровка	
килинган матн	ПАХТ А ГА РАМИ
Дастлабки матн	ПАХТА ФАРАМИ

4.8-расм. Вижинер матрицаси ёрдамида шифрлаш мисоли.

**Үрин алмаштириши усуллари.** Үрин 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 блокини матрицага катор бўйича ёзишни, ўкишни эса устун бўйича амалга оширишни кўрсатиш мумкин. Матрица каторларини тўлдириш ва шифрланган ахборогни устун бўйича ўкиш кетма-кетлиги калит ёрдамида берилиши мумкин. Усулнинг криптобардошлиги блок узунлигига (матрица улчамига) боғлик. Масалан, узунлиги 64 символга teng бўлган блок (матрица ўлчами 8x8) учун калитнинг  $1,6 \cdot 10^9$  комбинацияси бўлиши мумкин. Узунлиги 256 сим-волга teng бўлган блок (матрица ўлчами 16x16) калитнинг мумкин бўлган комбинацияси  $1,4 \cdot 10^{26}$  га етиши мумкин. Бу холда калитни саралаш масаласи замонавий ЭҲМлар учун ҳам мураккаб хисобланади.

*Гамильтон марирутларига* асосланган усулда ҳам ўрин алмаштиришлардан фойдаланилади. Ушбу усул куйидаги қадамларни бажариш оркали амалга оширилади.

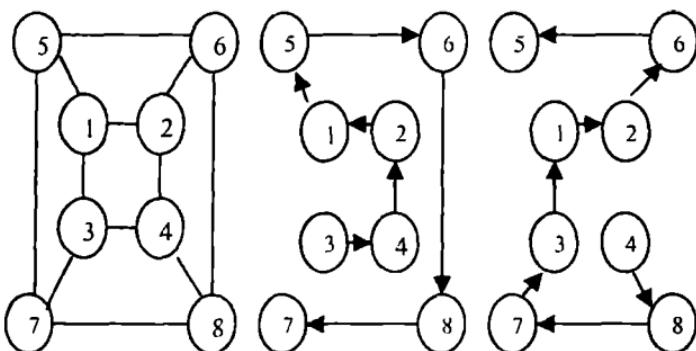
**1-қадам.** Дастлабки ахборот блокларга ажратиласди. Агар шифрланувчи ахборот узунлиги блок узунлигига каррали бўлмаса, охирги блокдаги бўш ўринларга маҳсус хизматчи символлар тўлдирувчилар жойлаштириласди (масалан, \*).

**2-қадам.** Блок символлари ёрдамида жадвал тўлдириласди ва бу жадвалда символнинг тартиб раками учун маълум жой ажратиласди (4.9-расм).

**3-қадам.** Жадваидаги символларни ўкиш маршрутларнинг бири бўйича амалга ошириласди. Маршрутлар сонининг ошиши шифр криптобардошлигини оширади. Маршрутлар кетма-кет танланади ёки уларнинг навбатланиши калит ёрдамида бериласди.

**4-қадам.** Символларнинг шифрланган кетма-кетлиги белгиланган  $L$  узунликдаги блокларга ажратилади.  $L$  катталик 1-қадамда дастлабки ахборот бўлинадиган блоклар узунлигидан фарқланиши мумкин.

Расшифровка килиш тескари тартибда амалга оширилади. Калитга мос ҳолда маршрут танланади ва бу маршрутга биноан жадвал тўлдирилади.



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

Жадвалдан символлар элемент ракамлари келиши тартибida ўқилади.

**Мисол.** Дастлабки матн  $T_0$  «ЎРИН АЛМАШТИРИШ УСУЛИ»ни шифрлаш талаб этилсин. Калит ва шифрланган блоклар узунлиги мос ҳолда куйидагиларга тенг:  $K=<2,1,1>$ ,  $L=4$ . 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.  $B1=<\text{ЎРИН\_АЛМ}>$ ,  $B2=<\text{АШТИРИШ}>$ ,  $B3=<\text{УСУЛИ}**>$ ;

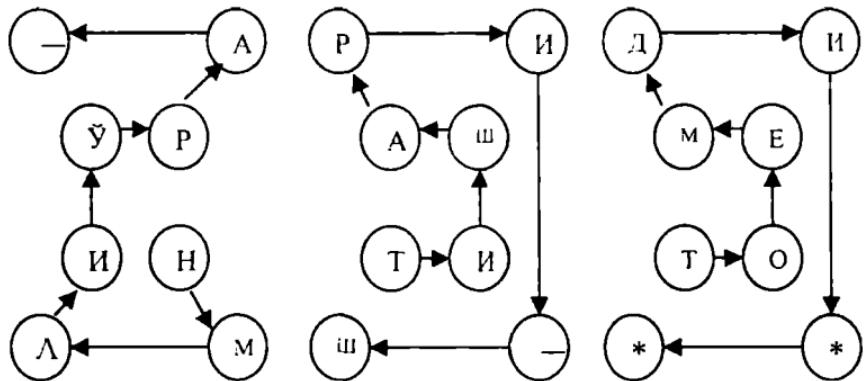
**2-қадам.** 2,1,1 маршрутли учта матрица тўлдирилади;

**3-қадам.** Маршрутларга биноан символларни жой-жойига кўйиш оркали шифрматнни хосил килиш.

$T_1=<\text{НМЛИЎРА\_ТИШАРИ\_ШТОЕМДИ}**>$

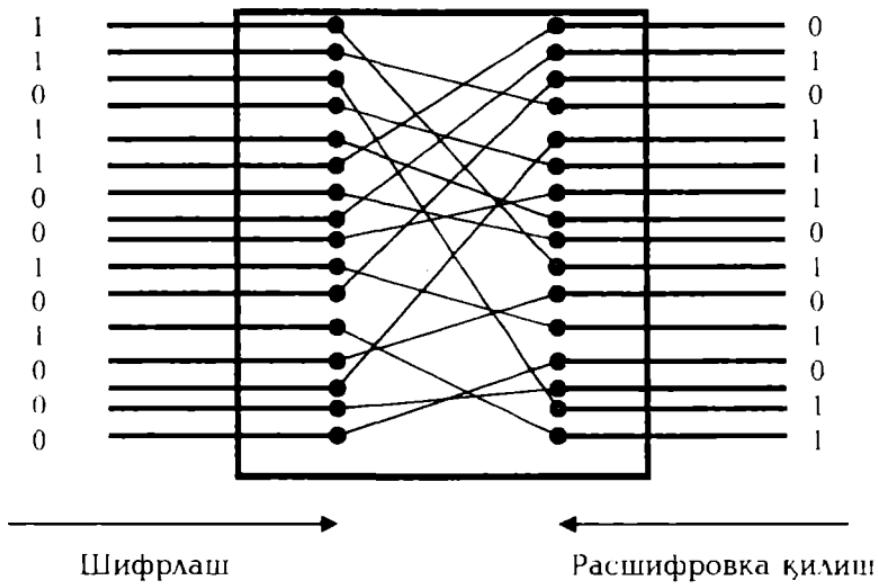
**4-қадам.** Шифрматнни блокларга ажратиш.

$T_1=<\text{НМЛИ ЎРА ТИША РИ ШТОЕМ ДИ}**>$



4.10-расм. Гамильтон маршрути ёрдамида шифрлаш мисоли.

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



4.11-расм. Ўрин алмаштириш схемаси.

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

килиш учун эса схеманинг кириш ва чикиш йўллари ўзаро алмаштирилади.

Ўрин алмаштириш усулларининг амалга оширилиши содда бўлсада, улар иккита жиддий камчиликларга эга. Биринчидан, бу усулларни статистик ишлаш орқали фош килиш 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 хосил килинади. Бу векторнинг элементлари  $c_i = \sum_j a_{ij} b_j$  ифодаси орқали аникланади.

Ахборотни расшифровка килиш  $C_k$  векторларини  $A$  матрицага тескари бўлган  $A^{-1}$  матрицага кетма-кет кўпайтириш орқали аникланади.

**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 килиш талаб этилсин.

Дастлабки сўзни шифрлаш учун куйидаги кадамларни бажариш лозим.

**1-қадам.** Дастлабки сўзни алфавитдаги ҳарфлар тартиб раками кетма-кетлигига мос сон эквивалентини аниклаш.

$$T_0 = \langle 1, 10, 12, 1, 14, 1 \rangle$$

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

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

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 14 \\ 1 \end{vmatrix} = \begin{vmatrix} 65 \\ 103 \\ 137 \end{vmatrix}$$

**3-қадам.** Шифрланган сүзни көтмә-кет сонлар күринишида ёзиш.

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

Шифрланган сүзни расшифровка қилиш қуйидагича амалга оширилады:

**1-қадам.**  $A$  матрицаның аникловчиси хисобланади:

$$|A| = -115.$$

**2-қадам.** Ҳар бир элементи  $A$  матрицадаги  $a_{ij}$  элементтің алгебраик түлдірувчысы бўлган бириктирилган матрица  $A^*$  аникланади.

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}$$

**3-қадам.** Транспонирланган матрица  $A^T$  аникланади.

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

**4-қадам.** Қуйидаги формула бўйича тескари матрица  $A^{-1}$  хисобланади:

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

Хисоблаш натижасида қуйидагини оламиз.

$$A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}$$

**5-қадам.**  $B_1$  ва  $B_2$  векторлар аникланади:

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

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

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

**6-қадам.** Расшифровка килинган сўзнинг сон эквиваленти  $T_2 = \langle 1, 10, 12, 1, 14, 1 \rangle$  символлар билан алмаштирилади. Натижада, дастлабки сўз  $T_0 = \langle \text{АЙЛАНА} \rangle$  хосил бўлади.

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

Ушбу усуулар учун калит сифатида гамма ишлатилади. Аддитив усуулнинг криптобардошлиги калит узунлигига ва унинг статис-тик характеристкаларининг текислигига боғлик. Агар калит шифрланувчи символлар кетма-кетлигидан киска бўлса, шифрматн криптоаналитик томонидан статистик усуулар ёрдамида расшифровка килиниши мумкин. Калит ва дастлабки ахборот узунликлари канчалик фарқланса, шифр-матнга мувваффакиятли хужум эҳтимоллиги шунчалик ортади. Агар калит узунлиги шифрланувчи ахборот узунлигидан катта бўлган тасодифий сонларнинг даврий бўлмаган кетма-кетлигидан ибораг бўлса, калитни билмасдан туриб шифрматнни расшифровка килиш амалий жихатдан мумкин эмас. Алмаштириш усууларидагидек гаммалашда калит сифатида ракамларнинг такрорланмайдиган кетма-кетлиги ишлатилиши мумкин.

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

чекиз кетма-кетлигини шакллантиришда нисбатан киска узунлик-дай дастьлабки ахборотдан фойдаланади.

Псевдотасодифий сонлар кетма-кетлигини шакллантиришда коңгруэнт генераторлардан хам фойдаланилади. Бу синф генераторлари сонларнинг шундай псевдотасодифий кетма-кетликларини шакллантиради, улар учун генераторларнинг даврийлиги ва чикиш 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 қўйидаги 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 дастьлабки катталилар.

Бундай датчикнинг тақорланиш даври  $A$  ва  $C$  катталиклари-га боғлиқ.  $m$  киймати одатда  $2^8$  га тенг қилиб олинади. Бу сурʼа.  $\lambda$ -ЭҲМдаги сўзининг битлардаги узунлиги. Шакллантирувчи сон кетма-кетликларининг тақорланиш даври  $c$ -тоқ сон ва  $A \pmod{4} = 1$  бўлгандагина максималь бўлади. Бундай генераторларни аппарат ёки программ воситалари орқали осонгина яратиш мумкин.

**Шифрлашнинг комбинацияланган усулилари.** Кудратли компьютерлар, гармок технологиялари ва нейронли хисоблашларнинг пайдо бўлиши хозиргача умуман фош килинмайди деб хисобланган криптографик тизимларни обрўсизлантирилишига сабаб бўлди. Бу эса ўз навбатида юкори бардошликка эга криптографик тизимларни яратиш устида ишлашни такозо этди. Бундай криптографик тизимларни яратиш усулиларидан бири шифрлаш усулиларини комбинациялашдир. Куйида энг кам вакт сарфида криптобардошликни жиддий ошишини гаъминловчи шифрлашнинг комбинацияланган усули устида сўз боради. Шифрлашнинг ушбу комбинацияланган усулига биноан маълумотларни шифрлаш икки боскичда амалга оширилади. Биринчи боскичда маълумотлар стандарт усул (масалан, DES усул) ёрдамида шифрланса, иккинчи боскичда шифрланган маълумотлар маҳсус усул бўйича кайта шифрланади. Маҳсус усул сифатида маълумотлар векторини элементлари нолдан фарқли бўлган сон матрицасига кўпайтиришдан фойдаланиш мумкин.

Гаммалашни кўллашда агар шифр гаммаси сифатида ракамларнинг тақрорланмайдиган кетма-кетлиги ишлатилса шифрланган матнни фош килиш жуда кийин. Одатда, шифр гаммаси хар бир шифрланувчи сўз учун тасодифий ўзгариши лозим. Агар шифр гаммаси шифрланган сўз узунлигидан катта бўлса ва дастлабки матннинг хеч кандай кисми маълум бўлмаса, шифрни факат тўғридан-тўғри саралаш оркали фош этиш мумкин. Бунда крипто-бардошлиқ қалит ўлчами оркали аникланади. 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 килиш жараёни-қалит маълум бўлганида шифр гаммасини қайта генерациялаш ва уни шифрланган маълумотларга сингдиришдан иборат.

Шифрланган маълумотлар векторини матрицага кўпайтириши кўллашда шифрланган матн бир байт узунликдаги  $f_i$  векторларга ажратилади ва хар бир вектор квадрат матрица  $|M_{ij}|$  га кўпайтирилади ва шифрланган векторлар шакллантирилади:

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

Бу усулнинг асосий афзалиги сифатида унинг маълумотлар ишланишининг турли жабхаларидаги мосланувчанлигини кўрсатиш мумкин. Хар бир всектор алоҳида шифрланганлиги сабабли маълумотлар блокини узагиш ва дастурланган маълумотлардан ихтиёрий фойдаланиш имконияти туғилади. Ушбу усулни аппарат ёки дастурий усулда амалга ошириш мумкин.

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

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

Комбинацияланган усулларнинг юкори самарадорлигига унинг иккала боскичини аппарат усулда амалга ошириш оркали эришиш мумкин. Аммо бу ускуна харажатларининг жиддий ошишига олиб келади. Дастурий усулда амалга оширилишида эса маълумотларни шифрлаш ва расшифровка килиш вакти ошиб кетади. Шу сабабли комбинацияланган усулларни аппарат-дастурий усулда, яъни усулнинг бир боскичи аппарат усулда, иккинчи боскичи дастурий усулда амалга оширилиши максадга мувофик хисобланади.

#### 4.3. Асимметрик шифрлаш тизимлари

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

Очик калитли тизимларини кўллаш асосида кайтарилмас ёки бир томонли функциялардан фойдаланиш ётади. Бундай функциялар қуйидаги хусусиятларга эга. Маълумки  $X$  маълум бўлса  $y=f(x)$  функцияни аниклаш осон. Аммо унинг маълум киймати бўйича  $x$  ни аниклаш амалий жихатдан 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 аниклаш мумкин.  $E_z$  алгоритми ёрдамида аниклик соҳасидаги барча  $x$  учун  $f_Z(x)$  функцияни осонгина олиш мумкин. Худди шу тарика  $D_z$  алгоритми ёрдамида жоиз кийматлар соҳасидаги барча  $y$  учун тескари функция  $x=f_z^{-1}(y)$  хам осонгина аникланади. Айни вактда жоиз кийматлар соҳасидаги барча  $z$  ва деярли барча,  $y$  учун хатто  $E_z$  маълум бўлганида хам  $f_z^1(y)$ ни хисоблашлар ёрдамида топиб бўлмайди. Очик калит сифатида  $y$  ишлатилса, махфий калит сифатида  $x$  ишлатилади.

Очик калитни ишлатиб шифрлаш амалга оширилганда ўзаро мулоқотда бўлган субъектлар ўргасида махфий калитни алмашиб заруриятни йўколади. Бу эса ўз навбатида узатилувчи ахборотнинг криптоҳимоясини соддалаштиради.

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

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

**1-қадам.** Иккита 200дан катта бўлган туб сон р ва q танланади.

**2-қадам.** Калитнинг очик ташкил ғувчиси п хосил килинади

$$n=p^*q.$$

**3-қадам.** Күйидаги формула бўйича Эйлер функцияси хисобланади:

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

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

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

**5-қадам.** Күйидаги шартни қаноатлантирувчи е сони аникланади:

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

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

**6-қадам.** Дастребаки ахборот унинг физик табиатидан қатъий назар раками иккили қўринишда ифодаланади. Битлар кетма-кетлиги  $L$  бит узунликдаги блокларга ажратилади, бу ерда,  $L-L \geq \log_2(n+1)$  шартини қаноатлантирувчи энг кичик бугун сон каби қўрилади. Шундай килиб, дастребаки ахборот  $X(i)$ ,  $i=1, I$  сонларнинг кетма-кетлиги оркали ифодаланади.  $i$  нинг киймати шифрланувчи кетма-кетликнинг узунлиги оркали аникланади.

**7-қадам.** Шифрланган ахборот кўйидаги формула бўйича аникланувчи  $Y(i)$  сонларнинг кетма-кетлиги қўринишида олинади:

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

Ахборотни расшифровка килишда кўйидаги муносабатдан фойдаланилади:

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

**Мисол:** <ГАЗ> сўзини шифрлаш ва расшифровка килиш талаб этгисин. Дастребаки сўзни шифрлаш учун кўйидаги қадамларни бажариш лозим.

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

**2-қадам.**  $n = 3 \cdot 11 = 33$  хисобланади.

**3-қадам.** Эйлер функцияси аникланади.

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

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

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

6-қадам. Дастрекки сўзнинг алфавитдаги ҳарфлар гартиб рақами кетма-кетлигига мос сон эквиваленти аникланади. 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. Дастрекки ахборот иккили кодда кўйидаги кўринишга эга бўлади:

000100 000001 001001.

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

Демак, дастрекки матн  $X(i) \leq <4,1,9>$  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  $Y(i)=<16,1,15>$

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

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

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

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

Дастрекки сон кетма-кетлиги расшифровка қилинган  $X(i)=<4,1,9>$  кўринишида дастрекки матн  $<\Gamma A Z>$  билан алмашгирилади.

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

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

мумкин. Бу ўз навбатида айтарлича хисоблаш ресурсларини талаб килади.

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

Барча очик калитли шифрлаш усувлари учун *NP*-тўлик масалани (тўлик саралаш масаласи) ечишга асосланган криптотахлил усулидан бошка усувларининг йўклиги катъий исботланмаган. Агар бундай масалаларни ечувчи самарали усувлар пайдо бўлса, бундай хилдаги криптотизим обрўсизлантирилади.

Юкорида кўрилган шифрлаш усувларининг криптобардошлиги калит узунлигига боғлик бўлиб, бу узунлик замонавий гизимлар учун, тоақал, 90 битдан катта бўлиши шарт.

Айрим мухим қўлланишларда нафақат калит, балки шифрлаш алгоритми ҳам маҳфий 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 хисоблаш машиналари, комплекслари ва тармоқларида ахборотни криптографик ўзгартириш алгоритмларига давлат стандарти (ГОСТ 2814-89) жорий этилган. Бу алгоритмлар маҳфийлик даражаси ихтиёрий бўлган ахборотни ҳеч қандай чекловсиз шифрлаш имконини беради. Алгоритмлар аппарат ва дастурий усувларда амалга оширилиши мумкин.

Стандартда ахборотни криптографик ўзгартиришнинг куйидаги алгоритмлари мавжуд:

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

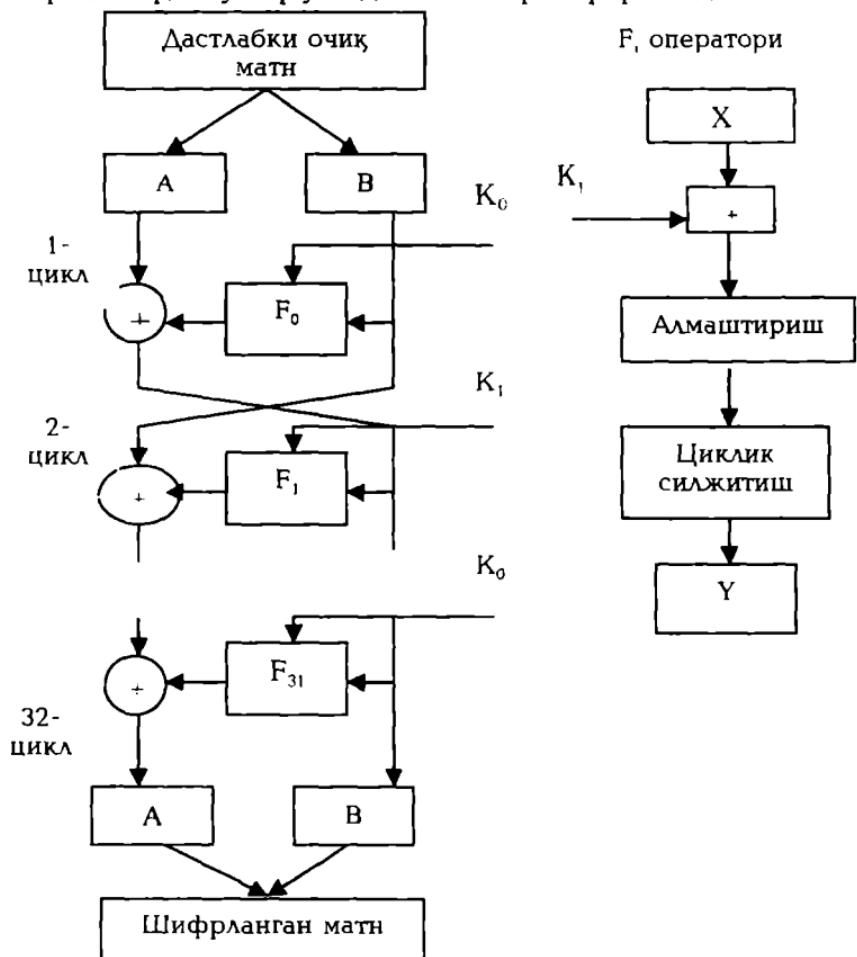
Бу алгоритмлар учун 8 ва 32 хонали иккили сўзларга ажратилиган 256 бит ўлчамли калитнинг ишлатилиши ҳамда дастлабки шифрланувчи иккили кетма-кетликнинг 64 битли блокларга ажратилиши умумий хисобланади.

**Оддий алмаштириши** алгоритмининг моҳияти куйидагича (4.12-расм).

Дастлабки кетма-кетликнинг 64 битли блоки иккита 32 хонали А ва В иккили сўзларга ажратилади. А сўзлар блокининг кичик хо-

наларини В сўзлар эса катта хоналарини ташкил этади. Бу сўзларга сони  $i=32$  бўлган циклик итерация оператори  $F_i$  қўлланилиди. Блокнинг кичик битларидағи сўз (биринчи итерациядаги А сўзи) калитининг 32 хонали сўзи билан mod2<sup>32</sup> бўйича жамланади; ҳар бири 4 битдан иборат кисмларга (4 хонали кириш йўли векторлари) ажратилиди; махсус алмаштириш узеллари ёрдамида ҳар бир вектор бошқаси билан алмаштирилди; олинган векторлар 32 хонали сўзга бирлаштирилиб, чап тарафга циклик равишда силжитилиди ва 64 хонали блокдаги бошқа 32 хонали сўз (биринчи итерациядаги В сўзи) билан mod 2 бўйича жамланади.

Биринчи итерация тугаганидан сўнг кичик битлар ўрнида В сўз жойланади, чап тарафда эса А сўз жойланади. Кейинги итерацияларда сўзлар устидаги амаллар тақорланади.



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

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

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

Демак, шифрлашда калитнинг танланиш тартиби қуйидаги кўринишда бўлади:

$$\begin{aligned} K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, \\ K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0. \end{aligned}$$

Расшифровка қилишда калитлар тескари тартибда ишлатилади.

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

*Гаммалаш* алгоритмida дастлабки битларнинг кетма-кетлиги гамманинг битлари кетма-кетлиги билан mod2 бўйича жамланади. Гамма оддий алмаштириш алгоритмiga биноан хосил килинади. Гаммани шакллантиришда иккита маҳсус доимийлардан ҳамда 64-хонали иккили кетма-кетлиик синхропосилкадан фойдаланилади. Ахборотни факат синхропосилка борлигига расшифровка қилиш мумкин.

Синхропосилка маҳфий бўлмайди ва очик ҳолда ҳисоблаш машинаси хотирасида сакланиши ёки алоқа канали оркали узатилиши мумкин.

*Тескари боғланишили гаммалаш* алгоритми гаммалаш алгоритмидан факат шифрлаш жараёнининг биринчи қадамидаги харакатлар билан фарқланади.

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

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

Имитоставкани шакллантириш алгоритми күйидаги харакатлар кетма-кетлигидан иборат. Очик ахбортот 64 битли  $T(i)$  ( $i=1,2,3,\dots,m$ ) блокларга ажратилади, бу ерда  $m$ -шифрланувчи ахбортот ҳажми орқали аникланади. Биринчи блок  $T(1)$  оддий алмаштириш алгоритмининг биринчи 16 итерацияларига биноан ўзгартирилади. Калит сифатида дастлабки ахбортот шифрланишда ишлатиладиган калит олинади. Олинган 64 битли иккили сўз иккинчи блок  $T(2)$  билан mod2 бўйича жамланади.  $T(1)$  блок устида кандай итерация ўзгартиришлари бажарилган бўлса жамлаш натижаси устида ҳам шундай ўзгартиришлар амалга оширилади ва охирида  $T(3)$  блок билан mod2 бўйича жамланади. Бундай харакатлар дастлабки ахбортотнинг  $m-1$  блоки бўйича тақорорланади. Агар охирги  $T(m)$  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 к бит узунликдаги сўз ажратиб олинади ва бу сўз имитовставка хисобланади.

Имитовставка шифрланган ахбортотнинг охирига жойлаштирилади. Бу ахбортот олингандан сўнг, у расшифровка килинади. Расшифровка килинган ахбортот бўйича имитовставка аникланади ва олингани билан солишибтирилади. Агар имитовставкалар мос келмаса, расшифровка килинган ахбортот нотўғри деб хисобланади.

**АҚШнинг ахбортотни шифрлаш стандарти.** АҚШда давлат стандарти сифатида DES(Data Encryption Standard) 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 макомини олган. DES стандартидан нафакат федерал департаментлар, балки нодавлат ташкилотлар, нафакат АҚШда, балки бутун дунёда фойдаланиб келинган.

DES стандартида дастлабки ахбортот 64 битли блокларга ажратилади ва 56 ёки 64 битли калит ёрдамида криптоографик ўзгартирилади.

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

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

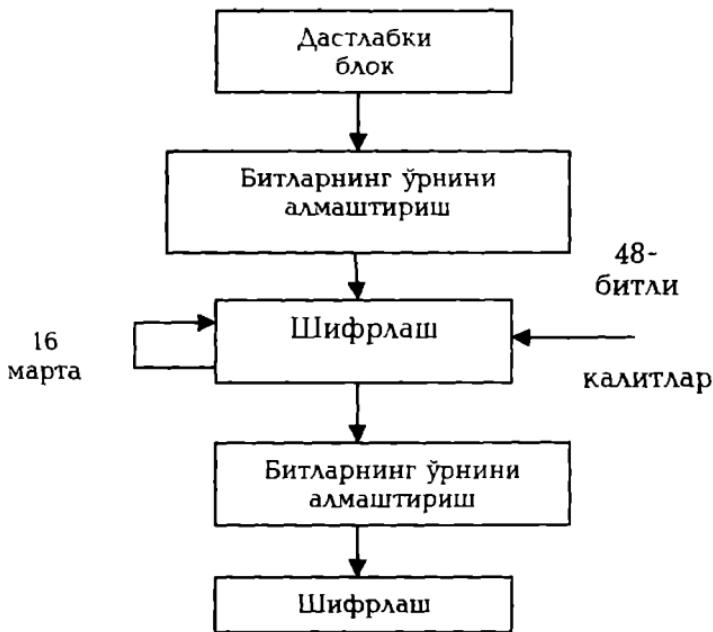
DES алгоритмидаги шифрлаш жараёнининг блок-схемаси 4.13-расмда келтирилган.

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

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

- калитнинг узунлиги 56 битни ташкил этади, бу ЭХМларнинг замонавий ривожи учун жуда кам;

- алгоритм яратилаётганида унинг аппарат усулда амалга оширилиши кўзда тутилган эди, яъни алгоритмда микропроцессорларда бажарилишида кўп вакт талаб қилувчи амаллар бор эди (масалан, машина сўзида маълум схема бўйича битларнинг ўрнини алмаштириш каби).



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

Бу сабаблар АКШ стандартлаш институтининг 1997 йилда симметрик алгоритмнинг янги стандартига танлов эълон килишига олиб келди. Танлов шартларига биноан алгоритмга қуидаги галаблар қўйилган эди:

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

Ундан ташкири танловда иштирок этувчилар учун қуидаги 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 мустакил тарзда криптотахлил килиб, унда кандайдир хужжатсиз имкониятлар йўклигига ишонч хосил килишлари учун зарур хисобланади.

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

Хозирда AES (Advanced Encryption Standard) деб аталувчи ушбу алгоритм Дж.Деймен (J. Daemen) ва В. Райджмен (V.Rijmen) томонидан яратилган. Бу алгоритм ноанъанавий блокли шифр бўлиб, кодланувчи маълумотларнинг ҳар бир блоки кабул килинган блок узунлигига караб  $4 \times 4$ ,  $4 \times 6$  ёки  $4 \times 8$  ўлчамдаги байтларнинг икки ўлчамли массивлари кўринишига эга.

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

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

да»ги ва «Электрон хужожат 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 тармокларида, телекоммуникацияда, алоҳида ҳисоблаш комплекслари ва ЭХМда ахборотни ишлаш тизимлари учун ахборотни шифрлашнинг умумий алгоритмини ва маълумотларни шифрлаш коидасини белгилайди.

Шифрлаш алгоритми дастурий ва аппарат усулларда амалга оширилиши мумкин.

Симметрик шифрлашнинг барча тизимлари қўйидаги камчиликларга эга:

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

- калитларни яратиш ва таксимлаш хизматига қўйиладиган талабларнинг юкорилиги. Сабаби, ўзаро алоканинг «хар ким – хар ким билан» схемасида  $n$  та абонент учун  $n(n-1)/2$  та калит талаб этилади, яъни калитлар сонининг абонентлар сонига боғликлиги квадратли. Масалан,  $n=1000$  абонент учун талаб килинадиган калитлар сони  $n(n-1)/2=499500$ . Шу сабабли, фойдаланувчилари юз миллиондан ошиб кетган «Internet» тармоғида симметрик шифрлаш тизимини қўшимча усул ва восита ўарсиз қўллашнинг иложи йўқ.

Асимметрик шифрлашнинг биринчи ва кенг тарқалган криптоалгоритми RSA (4.3 га карапсан) 1993 йилда стандарт сифатида кабул килинди. Ушбу криптоалгоритм хар гарафлама тасдикланган ва калитнинг етарли узунлигига бардошлиги зътироф этилган. Хозирда 512 битли калит бардошлини таъминлашда етарли хисобланмайди ва 1024 битли калитдан фойдаланилади. Баъзи муаллифларнинг фикрича процессор кувватининг ошиши RSA криптоалгоритмининг тўлик саралаш хужумларга бардошлигининг йўколишига олиб келади. Аммо, процессор кувватининг ошиши янада узун калитлардан фойдаланишга, ва демак, RSA бардошлигини ошишига имкон яратали.

Асимметрик криптоалгоритмларда симметрик криптоалгоритмлардаги камчиликлар бартарф этилган:

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

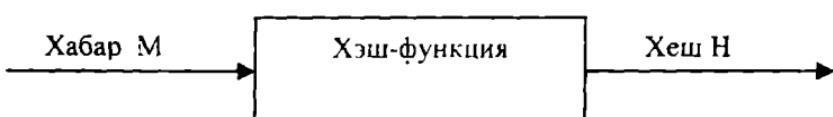
Аммо асимметрик криптотизимлар, хусусан, RSA криптотизими, камчиликлардан холи эмас:

- хозиргача асимметрик алгоритмларда ишлатилувчи функцияларнинг қайтарилимаслигининг математик исботи йўқ;
- асимметрик шифрлаш симметрик шифрлашга нисбаган секин амалга оширилади, чунки шифрлашда ва расшифровка килишда 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 кўйилишидан химоялаш зарур. Фараз килайлик « $A$ » абонентнинг компьютерида « $B$ » абонентнинг очик калити « $K_B$ » сакланади. « $l$ » нияги бузук одам « $A$ » абонентда сакланаётган очик калитлардан фойдалана олади. У ўзининг жуфт (очик ва махфий) « $K_n$ » ва « $k_n$ » калитларини яратади ва « $A$ » абонентда сакланаётган « $B$ » 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 леб ўйлаган холда) шифрлайди. Натижада, бу хабарни « $B$ » абонент ўкий олмайди, « $l$ » абонент осонгина расшифровка қиласди ва ўкийди. 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 чикиш йўлида белгиланган узунликдаги қатор  $h(M)$  ҳосил бўлади. Бошкacha айтганда, хеш-функция  $h(\cdot)$  аргумент сифатида узунлиги

ихтиёрий хабар (хужжат)  $M$  ни қабул килади ва белгиланган узунликдаги хеш-кыймат (хеш)  $H=h(M)$ ни кайтаради (4.14-расм).



4.14-расм. Хэшни шакллантириш схемаси.

**Хэш-кыймат  $h(M)$  – 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  $h(M)$  кийматининг хужжат  $M$ га боғликлиги мураккаб ва хужжат  $M$ нинг ўзини тиклашга имкон бермайди.

Хэшлаш функцияси қўйидаги хусусиятларга эга бўлиши лозим:

1. Хэш-функция ихтиёрий ўлчамли аргументга қўлланиши мумкин.
2. Хэш-функция чикиш йўлининг киймати белгиланган ўлчамга эга.
3. Хэш-функция  $h(x)$  ни ихтиёрий  $x'$  учун етарлича осон хисобланади. Хэш-функцияни хисоблаш тезлиги шундай бўлиши керакки, хеш-функция ишлатилганида электрон рақамли имзони тузиш ва текшириш тезлиги хабарнинг ўзидан фойдаланилганига қараганда анчагина катта бўлсин.
4. Хэш-функция матн  $M$  даги орасига қўйишлар (вставки), чиқариб ташлашлар (выбросы), жойини ўзгартиришлар ва х. каби ўзгаришларга сезгир бўлиши лозим.
5. Хэш-функция кайтариласлик хусусиятига эга бўлиши лозим.
6. Иккита турли хужжатлар (уларнинг узунлигига боғлик бўлмаган холда) хэш-функциялари кийматларининг мос келиши эҳтимоллиги жуда кичкина бўлиши шарт, яъни хисоблаш нуктаи назаридан  $h(x')=h(x)$  бўладиган  $x' \neq x$  ни топиш мумкин эмас.

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

5-хусусият  $h(\cdot)$  бир томонлама эканлигини билдиrsa, 6 хусусият бир бир хил тугунчани бсрувчи иккита ахборотни топиш мумкин эмаслигини кафолатлади. Бу сохталаштиришни олдини олади.

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

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

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

MD2, MD4 ва MD5 – Р.Райвест томонидан ишлаб чиқилган ахборот дайджестини хисобловчи алгоритмлар. Уларнинг хар бири 128 битли ҳёш-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 ҳёш-кодни тузувчи ахборот дайджестини хисобловчи алгоритм. Бу алгоритм MD4 ва MD5 алгоритмларига нисбаган ишончлирок.

## 4.6. Электрон ракамли имзо

Электрон хужжатларни тармок орқали алмашишда уларни ишлаш ва саклаш харажатлари камаяди, кидириш тезлашади. Аммо, электрон хужжат муаллифини ва хужжатнинг ўзини аутентификациялаш, яъни муаллифнинг ҳақиқийлигини ва олинган электрон хужжатда ўзгаришларнинг йўклигини аниқлаш муаммоси пайдо бўлади.

Электрон хужжатларни аутентификациялашдан максад уларни мумкин бўлган жинояткорона харакатлардан химоялашдир. Бундай харакатларга қўйидагилар киради:

- *фаол ушлаб қолиш* – тармокка уланган бузғунчи хужжатларни (файлларни) ушлаб колади ва ўзгартиради;
- *маскарад* – абонент *C* хужжатларни абонент *B* га абонент *A* номидан юборади;
- *ренегатлик* – абонент *A* абонент *B* га хабар юборган бўлсада, юбормаганман дейди;
- *алмаштириш* – абонент *B* хужжатни ўзгартиради, ёки янгисини шакллантиради ва уни абонент *A* дан олганман дейди;
- *такрорлаш* – абонент *A* абонент *B* га юборган хужжатни абонент *C* такрорлайди.

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

Электрон ракамли имзо методологияси хабар яхлитлигини ва хабар муаллифининг ҳақиқийлигини текшириш муаммосини самарали хал этишга имкон беради.

Электрон ракамли имзо телекоммуникация каналлари орқали узатилувчи матнларни аутентификациялаш учун ишлатилади. Ракамли имзо ишлаши бўйича оддий кўлёзма имзога ўхшаш бўлиб, қўйидаги афзалликларга эга:

- имзо чекилган матн имзо қўйган шахсга тегишли эканлигини тасдиқлайди;
- бу шахсга имзо чекилган матнга боғлик мажбуриятларидан тониш имкониятини бермайди;
- имзо чекилган матн яхлитлигини кафолатлайди.

Электрон раками имзо-имзо чекилувчи матн билан бирга узатилувчи кўшимча раками хабарнинг нисбатан катта бўлмаган сонидир.

Электрон раками имзо асимметрик шифрларнинг кайтарувчанилигига ҳамда хабар таркиби, имзонинг ўзи ва қалитлар жуфтининг ўзаро боғликлигига асосланади. Бу элементларнинг ҳатто бирининг ўзгариши раками имzonинг ҳакикийлигини тасдиқлашга имкон бермайди. Электрон раками имзо шифрлашнинг асимметрик алгоритмлари ва хеш-функциялари ёрдамида амалга оширилади.

Электрон раками имзо тизимининг кўлланишида бир-бирига имзо чекилган электрон хужжатларни жўнатувчи абонент тармоғининг мавжудлиги фараз килинади. Ҳар бир абонент учун жуфт - маҳфий ва очик қалит генерацияланади. Маҳфий қалит абонентда сир сакланади ва ундан абонент электрон раками имзони шакллантирища фойдаланади.

Очик қалит бошка барча фойдаланувчиларга маълум бўлиб, ундан имзо чекилган электрон хужжатни кабул килувчи электрон раками имзони текширишда фойдаланади.

Электрон раками имзо тизими иккита асосий муолажани амалга оширади:

- раками имзони шакллантириш муолажаси;
- раками имзони текшириш муолажаси.

Имзони шакллантириш муолажасида хабар жўнатувчисининг маҳфий қалити ишлатилса, имзони текшириш муолажасида жўнатувчининг очик қалитидан фойдаланилади.

### **Раками имзони шакллантириш муолажаси.**

Ушбу муолажани тайёрлаш боскичида хабар жўнатувчи абонент  $A$  иккита қалитни генерациялади: маҳфий қалит  $k_A$ , ва очик қалит  $K_A$ . Очик қалит  $K_A$  унинг жуфти бўлган маҳфий қалит  $k_A$  дан хисоблаш орқали олинади. Очик қалит  $K_A$  тармокнинг бошка абонентларига имзони текширишда фойдаланиши учун тарқатилади.

Рақамли имзони шакллантириш учун жүнатувчи  $A$  аввалинде имзо чекилүвчи матн  $M$  нинг хэш функцияси  $L(M)$  кийматини хисоблади (4.15-расм).

Хэш-функция имзо чекилүвчи дастлабки матн  $M$  ни дайджесть  $m$  га зичлаширишга хизмат килади. Дайджесть  $M$ -бутун матн  $M$  ни характерловчи битларнинг белгиланган катта бўлмаган сонидан иборат нисбатан киска сондир. Сўнгра жүнатувчи  $A$  ўзининг маҳфий калити  $k_A$  билан дайджесть  $m$  ни шифрлайди. Натижада, олингандан сонлар жуфти берилган  $M$  матн учун рақамли имзо хисобланади. Хабар  $M$  рақамли имзо билан биргаликда кабул килувчининг манзилига юборилади.

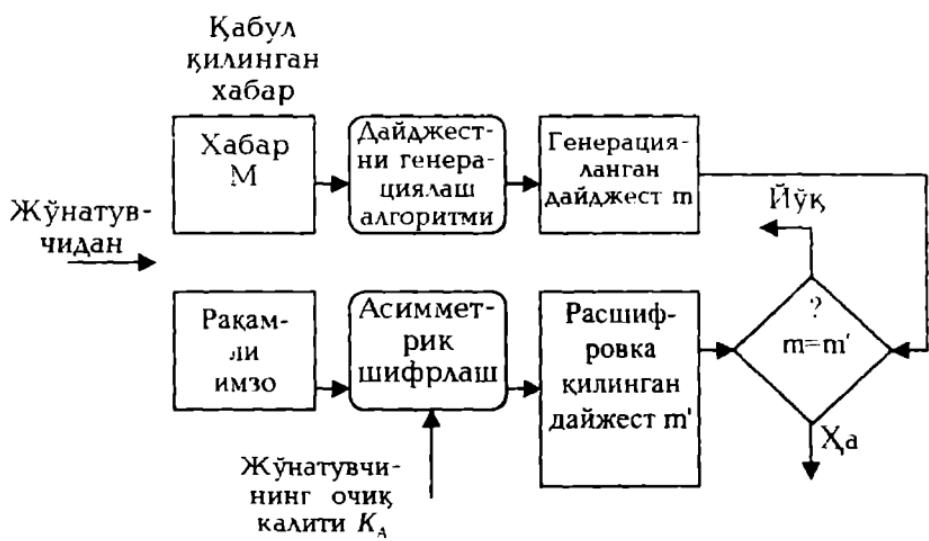


4.15-расм. Электрон рақамли имзони шакллантириш схемаси.

### Рақамли имзони текшириш муолажаси.

Тармок абонентлари олингандан хабар  $M$  нинг рақамли имзосини ушбу хабарни жүнатувчининг очик калити  $K_A$  ёрдамида текширишлари мумкин (4.16-расм).

Электрон рақамли имзони текширишда хабар  $M$  ни кабул килувчи  $B$  кабул килинган дайджестьни жүнатувчининг очик калити  $K_A$  ёрдамида расшифровка килади. Ундан ташкири, кабул килувчини ўзи хэш-функция  $h(M)$  ёрдамида кабул килинган хабар  $M$  нинг дайджести  $m$  ни хисоблади ва уни расшифровка килингани билан тақкослайди. Агар иккала дайджесть  $m$  ва  $m$  мос келса рақамли имзо ҳакикий хисобланади. Акс холда имзо қалбакилаштирилган ёки ахборот мазмуни ўзгартирилган бўлади.



4.16-расм. Электрон рақамли имзони текшириш схемаси.

Электрон рақамли имзо тизимининг принципиал жихати-фойдаланувчининг электрон рақамли имзосини унинг имзо чекишдаги маҳфий калитини билмасдан қалбакилаштиришнинг мумкин эмаслигидир. Шунинг учун имзо чекишдаги маҳфий калитни рухсагсиз фойдаланишдан химоялаш зарур. Электрон рақамли имзонинг маҳфий калитини, симметрик шифрлаш калитига ўхшаб, шахсий калит элитувчисида, химояланган ҳолда саклаш тавфсия этилади.

Электрон рақамли имзо-имзо чекилувчи хужжат ва маҳфий калит оркали аникланувчи ноёб сондир. Имзо чекилувчи хужжат сифатида хар қандай файл ишлатилиши мумкин. Имзо чекилган файл имзо чекилмаганига бир ёки бир нечта электрон имзо қўшилиши оркали яратилади.

Имзо чекилувчи файлга жойлаштирилувчи электрон рақамли имзо имзо чекилган хужжат муаллифини идентификацияловчи қўшимча ахборотга эга. Бу ахборот хужжатга электрон рақамли имзо хисобланмасидан олдин қўшилади. Ҳар бир имзо куйидаги ахборотни ўз ичига олади:

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

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

Асимметрик шифрлашга ўхшаш, электрон ракамли имзони текшириш учун ишлатиладиган очик калитнинг алмаштирилишига йўл кўймаслик лозим. Фараз килайлик, нияти бузук одам «*n*» абонент «*B*» компютерида сакланаётган очик калитлардан, хусусан, абонент *A* нинг очик калити  $K_A$  дан фойдалана олади. Унда у куйидаги харакатларини амалга ошириши мумкин:

- очик калит  $K_A$  сакланаётган файлдан абонент *A* хусусидаги индентификация ахборотини ўкиши;
- ичига абонент *A* хусусидаги индентификация ахборотини ёзган холда 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 хужжатларни ўзининг маҳфий калити  $k_n$  ёрдамида имзо чекиб жўнатиши мумкин. Бу хужжатлар имзосини текширишда абонент *B* абонент *A* имзо чеккан хужжатларни ва уларнинг электрон ракамли имзоларини тўғри ва ҳеч ким томонидан модификацияланмаган деб хисоблайди. Абонент *A* билан муносабатларини бевосита ойдинлаштирилишигача *B* абонентда олинган хужжатларнинг хаки-кийлигига шубха туғилмайди.

Электрон ракамли имзонинг катор алгоритмлари ишлаб чиқилган. 1977 йилда АҚШ да яратилган RSA тизими биринчи ва дунёда машҳур электрон ракамли имзо тизими хисобланади ва юкорида келтирилган принципларни амалга оширади. Аммо ракамли имзо алгоритми RSA жиддий камчиликка эга. У нияти бузук одамга маҳфий калитни билмасдан, хэшлаш натижасини имзо чекиб бўлинган хужжатларнинг хэшлаш натижаларини кўпайтириш оркали хисоблаш мумкин бўлган хужжатлар имзосини шакллантиришга имкон беради.

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

лар ва технологияларнинг Миллий университети томонидан ракамли имзонинг миллий стандартига асос каби қабул килинди.

#### 4.7. Криптографик қалитларни бошқариш

Хар кандай криптографик тизим криптографик қалитлардан фойдаланишга асосланган. Қалит ахбороти деганда ахборот тармоклари ва тизимларида ишлатилувчи барча қалитлар мажмуи тушунилади. Агар қалит ахборотларининг старлича ишончли бошқарилиши таъминланмаса, нияти бузук одам унга эга бўлиб олиб тармок ва тизимдаги барча ахборотдан хоҳлаганича фойдаланиши мумкин. Қалитларни бошқариш қалитларни генерациялаш, саклаш ва тақсимлаш каби вазифаларни бажаради. Қалитларни тақсимлаш қалигларни бошқариш жараёнидаги энг масъулиятли жараён ҳисобланади.

Симметрик криптотизимдан фойдаланилганда ахборот алмашинуvida иштирок этувчи иккала томон аввал маҳфий сессия қалити, яъни алмашинув жараёнида узатиладиган барча хабарларни шифрлаш қалити бўйича келишишлари лозим. Бу қалитни бошка барча билмаслиги ва уни вакти-вакти билан жўнатувчи ва қабул килувчida бир вактда алмаштириб туриш лозим. Сессия қалити бўйича келишиш жараёнини қалитларни алмаштириш ёки тақсимлаш деб ҳам юритилади.

Асимметрик криптотизимда иккита қалит-очик ва ёпик (маҳфий) қалит ишлатилади. Очик қалитни ошкор этиш мумкин, ёпик қалитни яшириш лозим. Хабар алмашинуvida факат очик қалитни унинг ҳакиқийлигини таъминлаган ҳолда жўнатиш лозим.

Қалитларни тақсимлашга қўйидаги талаблар қўйилади:

- тақсимлашнинг оперативлиги ва аниклиги;
- тақсимланувчи қалитларнинг конфиденциалитиги ва яхлитлиги.

Компьютер тармокларидан фойдаланувчилар ўргасида қалитларни тақсимлашнинг қўйидаги асосий усусларидан фойдаланилади.

1. Калитларни таксимловчи битта ёки бир нечта марказлардан фойдаланиш.

2. Тармок фойдаланувчилари ўртасида калитларни тўғридан-тўғри алмашиш.

Биринчи усулнинг муаммоси шундаки, калитларни таксимлаш марказига кимга, кайси калитлар таксимланганлиги маълум. Бу эса тармок бўйича узатилаётган барча хабарларни ўқишга имкон беради. Бўлиши мумкин бўлган суистеъмоллар тармок хавфсизлигининг жиддий бузилишига олиб келиши мумкин.

Иккинчи усулдаги муаммо – тармок субъектларининг ҳакикий эканлигига ишонч хосил килишдир.

Калитларни таксимлаш масаласи қўйидагиларни таъминловчи калитларни таксимлаш протоколини қуришга келтирилади:

- сеанс катнашчиларининг ҳакикийлигига иккала томоннинг тасдиги;
- сеанс ҳакикийлигининг тасдиги;
- калитлар алмашинувида хабарларнинг минимал сонидан фойдаланиш.

Биринчи усулга мисол тарикасида Kerberos деб аталувчи калитларни аутентификациялаш ва таксимлаш тизимини кўрсатиш мумкин.

Иккинчи усулга-тармок фойдаланувчилари ўртасида калитларни тўғридан-тўғри алмашишга батафсил тўхталашиб.

Симметрик калитли криптотизимдан фойдаланилганда криптографик химояланган ахборот алмашинувини истаган иккала фойдаланувчи умумий маҳфий 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 қўйидаги иккита асосий усул кўйланилади:

1. Симметрик криптотизимнинг маҳфий калитини химоялаш учун очик калитли асимметрик криптотизимдан фойдаланиш

2. Дифи-Хелманнинг калитларни очик таксимлаш гизимидан фойдаланиш.

Биринчи усул симметрик ва асимметрик калитли комбинацияланган криптотизим доирасида амалға оширилади. Бундай ёндашишда симметрик криптотизим дастлабки очик матнни цифрлаш ва узатышда ишлатылса, очик калитли асимметрик криптотизим факат симметрик криптотизимнинг маҳфий калигини шифрлаш, узатиш ва кейинги расшифровка килишда ишлатылади. Шифрлашнинг бундай комбинацияланган (гибрид) усули очик калитли асимметрик криптотизимнинг юкори маҳфийлиги билан маҳфий калитли симметрик криптотизимнинг юкори тезкорлигининг уйғун-лашишга олиб келади. Бундай ёндашиш баъзида электрон рақамили конверт схемаси деб юритилади.

Фараз килайлик, фойдаланувчи  $A$  хабар  $M$  ни фойдаланувчи  $B$  га ҳимояланган узатиш учун шифрлашнинг комбинацияланган усулидан фойдаланмокчи. Унда фойдаланувчиларнинг харакатлари куйидагича бўлади.

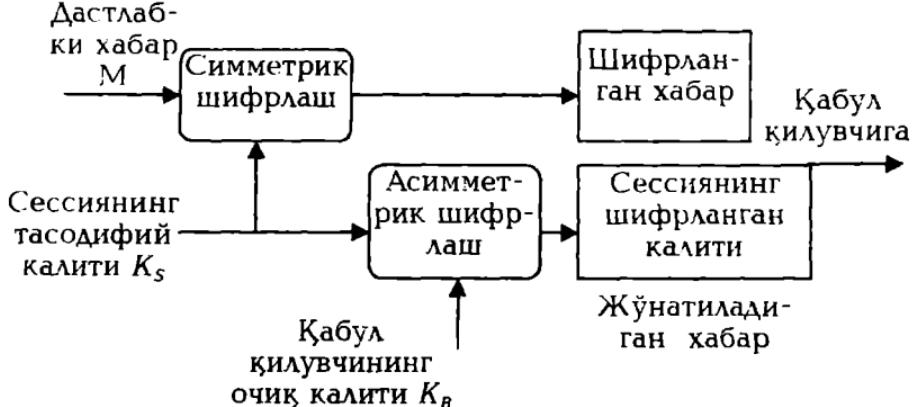
Фойдаланувчи  $A$  нинг харакатлари:

1. Симметрик сеанс маҳфий калит  $K_S$  ни яратади (масалан, тасодифий тарзда генерациялади).
2. Хабар  $M$  ни симметрик сеанс маҳфий калит  $K_S$  да шифрлайди.
3. Маҳфий сеанс калит  $K_S$  ни фойдаланувчи (хабар қабул килувчи)  $B$ нинг очик калити  $K_B$  да шифрлайди.
4. Фойдаланувчи  $B$  манзилига алоқанинг очик канали бўйича шифрланган хабар  $M$  ни шифрланган сеанс калити  $K_S$  билан биргаликда узатади.

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

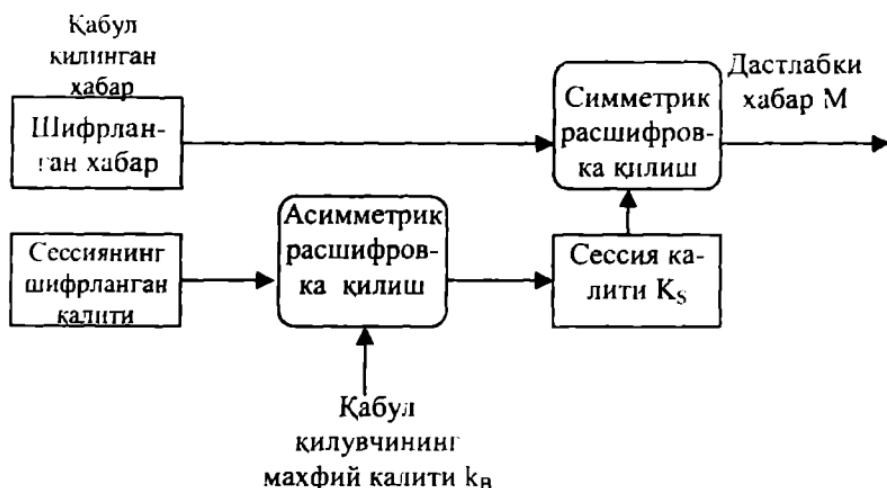
Фойдаланувчи  $B$  нинг харакатлари (электрон ракамили конвертни-шифрланган хабар  $M$  ни ва шифрланган сеанс калити  $K_S$  ни олганидан сўнгги) куйидагича:

1. Ўзининг маҳфий калити  $k_B$  бўйича сеанс калити  $K_S$  ни расшифровка киласди.
2. Олинган сеанс калити  $K_S$  бўйича олинган хабар  $M$  ни



4.17-расм. Комбинацияланган усул бүйича хабарни шифрлаш схемаси

Фойдланувчи *B* нинг харакатларини 4.18-расмда келтирилган хабарларни комбинацияланган усул бўйича расшифровка килиш схемаси орқали тушуниш мумкин.



#### 4.18-расм. Комбинацияланган усул бүйича хабарни расшифровка килиш схемаси

Олинган электрон ракамли конвертни фақат конуний кабул килувчи-фойдаланувчи  $B$  очиши чумкин. Фақат шахсий маҳфий қалит  $k_3$  эгаси бўлган фойдаланувчи  $B$  маҳфий сеанс қалити  $K_3$  ни

тўғри расшифровка килиш ва сўнгра бу калит ёрдамида олинган хабар  $M$  ни расшифровка килиши ва ўкиши мумкин.

Ракамли конверт усулида симметрик ва асимметрик криптоалгоритмларнинг камчиликлари куйидагича компенсацияланади:

- симметрик криптоалгоритм калитларини гаркатиш муаммоси бартараф килинади, чунки хабарни шифрловчи сеанс калити  $K_S$  очик канал бўйича шифрланган кўринишда узагилади, калит  $K_S$ ни расшифровка килиш учун асимметрик криптоалгоритмдан фойдаланилади;

- бу холда асимметрик шифрлаш тезкорлигининг секинлиги муаммоси пайдо бўлмайди, чунки асимметрик алгоритм бўйича факат киска калит  $K_S$  шифрланади, барча маълумотлар эса тезкор симметрик криптоалгоритм бўйича шифрланади.

Натижада тезкор шифрлаш билан биргалиқда калитларнинг кулагай таксимланиши амалга оширилади.

Шифрлашнинг комбинацияланган усулида симметрик хам асимметрик криптотизимларнинг криптографик калитларидан фойдаланилади. Равшанки, криптотизимнинг ҳар бир тури учун калитлар узунлигини шундай танлаш лозимки, нияти бузук одамга комбинацияланган криптотизим химоясининг ҳар қандай механизмига хужум килиш бир хил кийинчиллик туғдирсан.

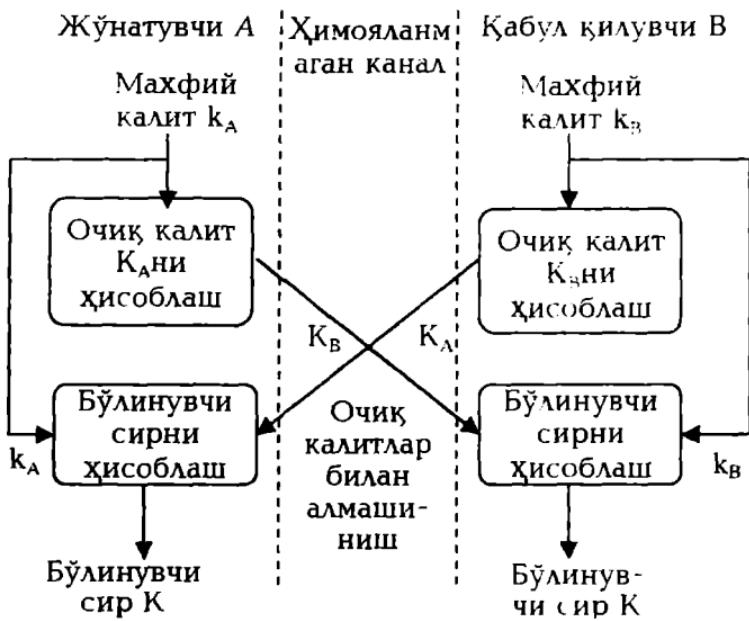
4.1-жадвалда кўп учрайдиган симметрик ва асимметрик криптотизимлар калитларининг узунлиги келтирилган.

#### 4.1-жадвал

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

У. Диффи ва М.Хеллман томонидан кашф этилган калитларни очиқ тақсилаш усули фойдаланувчиларга калитларни химояланмаган алоқа каналлари оркали алмашишга имкон беради. Унинг хавфсизлиги чегараланган соҳада дискрет логарифмларни хисоблашнинг мушкуллигига асосланади.

Диффи-Хеллман усулиниңг мөхияти куйидагича (4.19-расм).



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

Ахборот алмашинувида иштирок этувчи фойдаланувчилар А ва В мустакил равишда ўзларининг маҳфий калитларини  $k_A$  ва  $k_B$  ни генерациялайдишиар ( $k_A$  ва  $k_B$  калитлар-фойдаланувчилар А ва В лар сир сакловочи тасодифий катта бутун сонлар).

Сүнгра фойдаланувчи А ўзининг махфий калити  $k_A$  асосида очиқ калитни ҳисоблайди:

$$K_A = g^{K_1} \pmod{N}.$$

Бир вактнинг ўзида фойдаланувчи  $B$  ўзининг махфий калити  $k_B$  асосида очик калитни хисоблайди:

$$K_\beta = g^{K_\beta} \pmod{N}.$$

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

Сүнгра фойдаланувчилар А ва В ўзларининг очик калитларини химояланмаган камал орқали алмашадилар ва умумий сессия маҳфий калити Кни (бўлинувчи сирни) хисоблашда ишлатадилар:

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

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 килиб, ушбу амаллар натижасида иккала маҳфий калит  $k_A$  ва  $k_B$  көлгалинг функцияси бўлган умумий сессия маҳфий калити ҳосил килинади.

Очиқ калитлар  $K_A$  ва  $K_B$  киймагларини ушлаб қолган нияти бузук одам сессия маҳфий калити  $K$  ни ҳисоблай олмайди, чунки у маҳфий калитлар  $k_A$  ва  $k_B$  кийматларини билмайди. Бир томонлама функцияниң ишлатилиши сабабли очик калитни ҳисоблашга амали қайтарилилмайдиган амал, яъни абонентнинг очик калити қиймати бўйича унинг маҳфий калитини ҳисоблаш мумкин эмас.

Диффи-Хеллман усулиниң ноёблиги шундан иборатки, абонентлар жуфти тармоқ орқали очик калитларни узатганларида факат ўзларига маълум маҳфий сонни олиш имкониятига эга. Сўнгра абонентлар узатилаётган ахборотни маълум текширилган усусли – олинган умумий сессия маҳфий калитидан фойдаланган холда симметрик шифрлашни ишлатиб химоялашга киришишлари мумкин.

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

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

Маълумотлар яхлитлигини ва конфиденциаллигини бир вактда ҳимоялаш учун шифрлаш ва электрон ракамли имзодан комплекс фойдаланиш мақсадгага мувофик ҳисобланади. Диффи-Хеллман схемаси ишлашининг ораёнк натижаларидан узатилаётган маълумотларнинг яхлитлигини ва конфиденциаллагини комплекс ҳимоялаш усулини амалга оширишда фойдаланиш мумкин. Ҳақикатан, ушбу алгоритмга биноан фойдаланувчилар *A* ва *B* аввал ўзларининг маҳфий калитлари  $k_A$  ва  $k_B$  ни генерациялайдилар ва очик калитлари  $K_A$

ва  $K_B$  ни хисоблайдилар. Сүнгра абонентлар  $A$  ва  $B$  бу оралиқ на-тижалардан маълумотларни симметрик шифрлашда фойдаланилиши мумкин бўлган умумий бўлинувчи маҳфий калити  $K$  ни бир вактда хисоблаш учун ишлатади.

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

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

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

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

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

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

Диффи-Хеллман схемаси асосида тармок сатҳида ҳимояланган виртуал тармоклар VPN қурилишида кўлланилувчи 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 харакатланувчи жараён) билан уни бир маънода идентификацияловчи ахборот боғлик.

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 (конуний), акс ҳолда легал бўлмаган (ноконуний) фойдаланувчи хисобланади. Компьютер ресурсларидан фойдаланишдан аввал фойдаланувчи компьютер тизимининг идентификация ва аутентификация жараёнидан ўтиши лозим.

*Идентификация* (Identification) – фойдаланувчини унинг идентификатори (номи) бўйича аниклаш 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 ҳакикий эканлигини текшириш муолажаси. Бу гекшириш фойдаланувчи (жараён ёки курилма) ҳакикатан айнан ўзи эканлигига ишонч ҳосил қилишга имкон беради. Аутентификация ўтказишида текширувчи тараф текширилувчи тарафнинг ҳакикий эканлигига ишонч ҳосил қилиши билан бир каторда 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 тасдиклайди.

Идентификация ва аутентификация субъектларнинг (фойдаланувчиларнинг) ҳакикий эканлигини аниклаш ва текширишнинг 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 хисобот ахбороти хавфсизлик нуктаи назаридан тармоқдаги хавфсизлик ходисаларини ошкор килиш, таҳлиллаш ва уларга мос реакция кўрсатиш учун жуда мухимдир.

Маълумотларни узатиш каналларини химоялашда субъектларнинг ўзаро аутентификацияси. Яъни алока каналлари оркали боғланадиган субъектлар ҳакиқийлигининг ўзаро тасдиғи бажарилиши шарт. Ҳакиқийликтининг тасдиғи одатда, сеанс бошида, абонентларнинг бир-бирига уланиш жараёнида амалга оширилади. «Улаш» атамаси оркали тармокнинг иккита субъекти ўртасида мантикий боғланиш тушунилади. Ушбу муолажанинг мақсади – ўлаш конуний субъект билан амалга оширилганлигига ва барча ахборот мўлжалланган манзилга боришлигига ишончни таъминлаштирди.

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

- бирор нарсанни билishi асосида. Мисол сифатида парол, шахсий идентификация коди PIN (Personal Identification Number) ҳамда «сўров жавоб» хилидаги протоколларда намойиш этилувчи маҳфий ва очик калитларни кўрсатиш мумкин;

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

- қандайдир даҳлсиз характеристикалар асосида. Ушбу категория ўз таркибига фойдаланувчининг биометрик характеристикаларига (овозлар, кўзининг рангдор пардаси ва тўр

пардаси, бармок излари, кафт геометрияси ва х.) асосланган усулларни олади. Бу категорияда криптографик усуллар ва воситалар ишлатилмайди. Геометрик характеристикалар бинодан ёки кандайдир техникадан фойдаланишни назоратглашда ишлатиласди.

Парол – фойдаланувчи хамда унинг ахборот алмашинуидаги шериги биладиган нарса. Ўзаро аутентификация учун фойдаланувчи ва унинг шериги ўртасида парол алмашиниши мумкин. Пластик карга ва смарт-карта эгасини аутентификациясида шахсий идентификация номери PIN синалган усул хисобланади. PIN – коднинг маҳфий киймати факат карта эгасига маълум бўлиши шарт.

*Динамик* – (бир марта тик) парол – бир марта ишлатилганидан сүнг бошка умуман ишлатилмайдиган парол. Амалда одатда доимий паролга ёки таянч иборога асосланувчи мунтазам ўзгариб турувчи киймат ишлатилиди.

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

*Сертификатлар ва рақалы имзолар – агар аутентификация учун сертификатлар ишлатилса, бу сертификатларда ракамли имзонинг ишлатилиши талаб этилади. Сертификатлар фойдаланувчи ташкилотининг масъул шахси, сертификатлар сервери ёки ташки ишончли ташкилот томонидан берилади. Internet доирасида очик калит сертификатларини тарқатиш учун очик калитларни бошкарувчи катор тижорат инфратузилмалари PKI (Public Key Infrastructure) пайдо бўлди. Фойдаланувчилар турли даражада сертификатларини олишлари мумкин.*

Аутентификация жарёnlарини таъминланувчи хавфсизлик даражаси бўйича ҳам туркумлаш мумкин. Ушбу ёндашишга биноан аутентификация жараёnlари куйидаги турларга бўлинади:

пароллар ва ракамли сертификатлардан фойдаланувчи аугентификация;

криптографик усуллар ва воситалар асосидағы көттөшкін аутентификация;

- ноллик билан исботлаш хусусиятига эга бўлган аутентификация жараёнлари (протоколлари);
- фойдаланувчиларни биометрик аутентификацияси.

Хавфсизлик нуктаи 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 кизикиш амалий характерга нисбатан кўпроқ назарий характерга эга. Балким, яқин 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 имтиёzlарига эга бўлишни мўлжаллайди;
- аутентификация алмашинуви *тарафини алмаштириб* қўйши (interleaving attack). Нияти бузук одам ушбу хужум мобайнида икки тараф орасидаги аутентификацион алмашиниш жараённида трафикни модификациялаш ниятида катнашади. Алмаштириб қўйишнинг куйидаги хили мавжуд: иккита фойдаланувчи ўртасидаги аутентификация муваффакиятли ўтиб, уланиш ўрнатилганидан сўнг бузғунчи фойдаланувчилардан бирини чиқариб ташлаб, унинг номидан ишни давом эттиради;
- *такрорий узатиш* (gerplay attack). Фойдаланувчиларнинг бирин томонидан аутентификация маълумотлари такроран узатилади;
- *узатишни қайтариш* (reflection attack). Оддинги хужум варианtlаридан бирин бўлиб, хужум мобайнида нияти бузук одам протоколнинг ушбу сессия доирасида ушлаб қолинган ахборотни орқага қайтаради;
- *мажбурий кечикиши* (forced delay). Нияти бузук одам қандайдир маълумотни ушлаб қолиб, бирор вактдан сўнг узатали;
- *матн танлаши* ҳужум ( chosen text attack). Нияти бузук одам аутентификация графигини ушлаб қолиб, узок муддатли криптографик қалитлар хусусидаги ахборотни олишга уринади.

Юкорида көлтирилгән хужумларни бартараф килиш учун аутентификация протоколларини куришда күйидаги усуллардан фойдаланилади:

- «сўров-жавоб», вакт белгилари, тасодифий сонлар, индентификаторлар, ракамли имзолар каби механизмлардан фойдаланиш;

- аутентификация натижасини фойдаланувчиларнинг тизим доирасидаги кейинги ҳаракатларига боғлаш. Бундай ёндашишга мисол тарикасида аутентификация жараёнида фойдаланувчиларнинг кейинги ўзаро алоқаларида ишлатилувчи маҳфий ссанс қалитларини алмашишни кўрсатиш мумкин;

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

«Сўров-жавоб» механизми күйидагича. Агар фойдаланувчи *A* фойдаланувчи *B* дан оладиган хабари ёлғон эмаслигига ишонч хосил килишни истаса, у фойдаланувчи *B* учун юборадиган хабарга олдиндан билиб бўлмайдиган элемент - *X* сўровини (масалан, кандайдир тасодифий сонни) қўшади. Фойдаланувчи *B* жавоб беришда бу амал устида маълум амални (масалан, кандайдир  $f(X)$  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 ҳақиқий эканлигига ишонч хосил килиши мумкин. Ушбу усулнинг камчилиги - сўров ва жавоб ўртасидаги қонуниятни аниглаш мумкинлиги.

Вактни белгилаш механизми ҳар бир хабар учун вактни кайдлашни кўзда тутади. Бунда тармокнинг ҳар бир фойдаланувчиси келган хабарнинг қанчалик эскирганини аниглаши ва уни қабул килмаслик қарорига келиши мумкин. Чунки у ёлғон бўлиши мумкин. Вактни белгилашдан фойдаланишда сеанснинг ҳақиқий эканлигини тасдиқлаш учун кечикишининг жоиз вакт оратиги муаммоси найдо бўлади. Чунки, «вакт тамғаси»ли хабар, умуман, бир лахзада узатилиши мумкин эмас. Ундан ташкари, қабул кијувчи ва жўнатувчининг соатлари мутлако синхронланган бўлиши мумкин эмас.

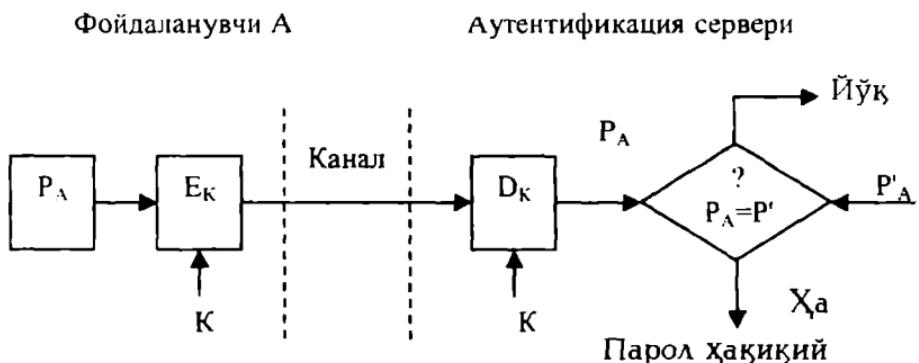
Аугентификация протоколларини тақкослашда ва танлашда күйидаги характеристикаларни хисобга олиш зарур:

- ўзаро аутентификациянинг мавжудлиги. Ушбу хусусият аутентификацион алмашинув тарафлари ўртасида иккиёклама аутентификациянинг зарурлигини акс эттиради;
- хисобланы санарадорлиги. Протоколни бажаришда зарур бўлган амаллар сони;
- коммуникацион санарадорлик. Ушбу хусусият аутентификацияни бажариш учун зарур бўлган хабар сони ва узунлигини акс эттиради;
- учинчи тарафнинг мавжудлиги. Учинчи тарафга мисол тарикасида 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;
- сирни саклаш. Жиддий калитли ахборотни саклаш 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 кўйидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган фойдаланувчи компютер клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аугентификация серверида сакланётган фойдаланувчи идентификатори бўйича маълумотлар базасидан мос ёзув гопилади, ундан паролни топиб фойдаланувчи киритган парол билан тақкосланади. Агар улар мос келса, аугентификация муваффакиятни ўтган хисобланади ва фойдаланувчи тегал (конуний) макомини ва авторизация гизими оркали унинг макоми учун аникланган хукукларни ва тармок ресурсларидан фойдаланишга рухсатни олади.

Паролдан фойдаланган ҳолда оддий аутентификациялаш схемаси 5.1-расмда келтирилган.



5.1-расм. Паролдан фойдаланган ҳолда оддий аутентификациялаш.

Равшанки, фойдаланувчининг паролини шифрламасдан узатиш оркали аутентификациялаш варианти хавфсизликнинг ҳатто минимал даражасини кафолатламайди. Паролни химоялаш учун уни химояланмаган канал оркали узатишдан олдин шифрлаш зарур. Бунинг учун схемага шифрлаш  $E_K$  ва расшифровка килиш  $D_K$  воситалари киритилганди. Бу воситалар бўлинувчи махфий калит  $K$  оркали бошқарилади. Фойдаланувчининг ҳакиқийлигини текшириш фойдаланувчи юборган парол  $P_A$  билан аутентификация серверида сакланувчи дастлабки киймат  $P'_A$  ни тақкослашга асосланган. Агар  $P_A$  ва  $P'_A$  кийматлар мос келса, парол  $P_A$  ҳакиқий. фойдаланувчи  $A$  эса конуний ҳисобланади.

Оддий аутентификацияни ташкил этиш схемалари нафакат паролларни узатиш, балки уларни саклаш ва текшириш турлари билан ажралиб туради. Энг кенг таркалган усул – фойдаланувчилар паролини тизимли файлларда, очик ҳолда саклаш усулидир. Бунда файлларга ўкиш ва ёзищдан химоялаш атрибулари ўрнатилади (масалан, операцион тизимдан фойдаланишни назоратлаш рўйхатидаги мос имтиёзларни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида сакланаётган ёзув билан солиширади. Бу усулда шифрлаш ёки бир томонлама функ-

циялар каби криптографик механизмлар ишлатишмайды. 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 хисобланади. Бу холда фойдаланувчи паролнинг очик шакли урнита унинг бир томонлама функция  $h(\cdot)$  дан фойдаланиб олинган тасвирини юбориши шарт. Бу ўзгартириш ғаним томонидан паролни унинг тасвири орқали ошкор кила олмаганлигини кафолатлади, чунки ғаним ечилибдишган сонли масалага дуч келади.

Кўп мартали паролларга асосланган оддий аутентификациялаш тизимининг бардоштиги паст, чунки уларда аутентификацияловчи ахборот маъноли сўзларнинг нисбатан катта бўлмаган тўпламидан жамланади. Кўп мартали паролларнинг таъсир муддати ташкилотнинг хавфсизлиги сиёсатида белгиланиши ва бундай паролларни мунтазам 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 ишлагилади. Бир мартали динамик парол факат тизимдан бир марта фойдаланишга ярокли. Агар, ҳатто кимдир уни ушлаб колса ҳам парол фойда бермайди. Одатда, бир мартали паролларга асосланган аутентификациялаш тизими масофадаги фойдаланувчиларни текширишда кўлланилади.

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 курилмалар кўринишида амалга оширади. Одатда, калитлар деб аталувчи бундай карталар клавиатурага ва катта бўлмаган дисплей дарчасига эга.

Фойдаланувчиларни аутентификациялаш учун бир мартали паролларни кўллашнинг қўйидаги усуллари маълум:

1. Ягона вакт тизимига асосланган вакт белгилари механизмидан 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 сифатига SecurID аутентикациялаш технологиясини кўрсатиш мумкин. Бу технология Security Dynamics компанияси томонидан ишлаб чиқилиган бўлиб, катор компанияларнинг хусусан Cisco Systems компаниясининг серверларида амалга оширилган.

Вакт синхронизациясидан фойдаланиб аутентификациялаш схемаси тасодифий сонларни вактнинг маълум оралигидан сўнг генерациялаш алгоритмига асосланган. Аутентификация схемаси куйидаги иккита параметрдан фойдаланади:

- хар бир фойдаланувчига аталган ва аутентификация серверида ҳамда фойдаланувчининг апарат калигида сақланувчи ноёб 64-битли сондан иборат маҳфий калит;
- жорий вакт қиймати.

Масофадаги фойдаланувчи тармоқдан фойдаланишга уринганида ундан шахсий идентификация раками PINни киритиш таклиф этилади. PIN тўртта ўнли ракамдан ва апарат калити дисплейида аксланувчи тасодифий соннинг олтига ракамидан иборат. Сервер фойдаланувчи томонидан киритилган PIN-коддан фойдаланиб маълумотлар базасидаги фойдаланувчининг маҳфий калити ва жорий вакт қиймати асосида тасодифий сонни генерациялаш алгоритмини бажаради. Сўнгра сервер генерацияланган сон билан фойдаланувчи киритган сонни таккослайди. Агар бу сонлар мос келса, сервер фойдаланувчига тизимдан фойдаланишга рухсат беради.

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

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

- аппарат калити ишлаб чиқилаётганида унинг таймер частотасининг меъёридан четлашиши аник ўлчанади. Четлашишнинг бу киймати сервер алгоритми параметри сифатида хисобга 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 вакт оралиғи мобайнида хакикий парол хисобланади. Шу сабабли, умуман, қисқа муддатли вазият содир бўлиши мумкинки, хакер PIN-кодни ушлаб қолиши ва уни тармоқдан фойдаланишга ишлатиши мумкин. Бу вакт синхронизациясига асосланган аутентификация схемасининг энг заиф жойи хисобланади.

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 узатади. Фойдаланувчининг аппарат калити бу тасодифий сонни, масалан, DES алгоритми ва фойдаланувчининг аппарат калити хоти-расида ва сервернинг маълумотлар базасида сакланувчи маҳфий калити ёрдамида расшифровка килади. Тасодифий сон – сўров шифрланган кўринишда серверга кайтарилади. Сервер ҳам ўз навбатида ўша DES алгоритми ва сервернинг маълумотлар базасидан олинган фойдаланувчининг маҳфий калити ёрдамида ўзи генера-циялаган тасодифий сонни шифрлайди. Сўнгра сервер шифрлаш натижасини аппарат калитидан келган сон билан таккослайди. Бу сонлар мос келганида фойдаланувчи тармоқдан фойдаланишга рухсат олади. Таъкидлаш лозимки, «сўров-жавоб» аутентификациялаш схемаси ишлатишда вакт синхронизациясидан фойдаланувчи аутентификация схемасига караганда мураккаброқ.

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

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

Фойдаланувчини аутентификациялаш учун бир марта 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 марта пароллар кетма-кетлиги. Навбатдаги аутентификациялаш сессиясида фойдаланувчи айнан шу сессия учун олдинги сессия паролидан олинган маҳфий калитда шифрланган паролни яратади ва узатади;

- бир томонлама функцияга асосланган пароллар кетма-кетлиги. Ушбу усулнинг мохиятини бир томонлама функцияниг кетма-кет ишлатилиши (Лампартнинг машҳур схемаси) ташкил этади. Хавфсизлик нуктаи назаридан бу усул кетма-кет ўзгартирилувчи пароллар усулига нисбатан афзал хисобланади.

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

### 5.3. Сертификатлар асосида аутентификациялаш

Тармоқдан фойдаланувчилар сони миллионлаб ўлчанганида фойдаланувчилар паролларининг тайинланиши ва сакланиши билан боғлик фойдаланувчиларни дастлабки рўйхатга олиш муолажаси жуда катта ва амалга оширилиши кийин бўлади. Бундай шароитда рақамли сертификатлар асосидаги аутентификациялаш пароллар кўлланишига рационал альтернатива хисобланади.

Рақамли сертификатлар ишлатилганида компютер тармоғи фойдаланувчилар хусусидаги ҳеч кандай ахборотни сакламайди. Бундай ахборотни фойдаланувчиларнинг ўзи сўров-сертификатларида тақдим этадилар. Бунда маҳфий ахборотни, хусусан маҳфий калитларни саклаш вазифаси фойдаланувчиларнинг ўзига юкланади.

Фойдаланувчи шахсини тасдикловчи рақамли сертификатлар фойдаланувчилар сўрови бўйича маҳсус ваколатли ташкилот-сертификация маркази CA (Certificate Authority) томонидан, маълум шартлар бажарилганида берилади. Таъкидлаш лозимки, сертификат олиш муолажасининг ўзи хам фойдаланувчининг ҳакикийлигини текшириш (яни, аутентификациялаш) боскичини ўз ичига олади. Бунда текширувчи тараф сертификацияловчи ташкилот (сертификация маркази CA) бўлади.

Сертификат олиш учун мижоз сертификация марказига шахсини тасдикловчи маълумотни ва очик калитини тақдим этиши лозим. Зарурий маълумотлар рўйхати олинадиган сертификат турига боғлик. Сертификацияловчи ташкилот фойдаланувчининг ҳакикий-лиги тасдиғини текширганидан сўнг ўзининг рақамли имзосини очик калит ва фойдаланувчи хусусидаги маълумот бўлган файлга жойлаштиради хамда ушбу очик калитнинг муайян шахсга тегишли эканлигини тасдиклаган холда фойдаланувчига сертификат беради.

Сертификат электрон шакл бўлиб, таркибида қўйидаги ахборот бўлади:

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

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

Очик калитларнинг сертификатлар билан узвий боғликлигини алоҳида таъкидлаш лозим. Сертификат нафакат шахсни, балки очик калит мансублигини тасдикловчи ҳужжатдир. Рақамли сертификат очик калит ва унинг эгаси ўртасидаги мосликин 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 ракамли имзосини ушбу сертификация марказининг очик калити ёрдамида текшириши ва очик калит манзили ва бошқа маълумотлари сертификатда қўрсатилган фойдаланувчига тегишли эканлигига ишонч ҳосил килиши мумкин. Сертификатлардан фойдаланилганда фойдаланувчилар рўйхатини уларнинг пароллари билан корпорация серверларида саклаш зарурияти йўколади. Серверда сертификацияловчи ташкилотларнинг номлари ва очик калитларининг бўлиши етарли.

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

Сертификатлар асосида аутентификациялаш жараёсини амалга оширишда сертификацияловчи ташкилот вазифасини ким бажариши хусусидаги масалани счиш мухим хисобланади. Ходимларни сертификат билан таъминлаш масаласини корхонанинг ўзи ечиши жуда табиий хисобланади. Корхона ўзининг ходимларини яхши билади ва улар шахсини тасдиқлаш вазифасини ўзига олиши мумкин. Бу сертификат берилишидаги дастлабки аутентификациялаш муолажасини осоипаштиради. Корхоналар сертификатларни генерациялаш, бериш ва уларга хизмат қўрсатиш 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 мустакил марказлар ҳам жалб этилиши мумкин. Бундай хизматларни, хусусан, Verisign компаниясининг сертификацияловчи маркази таклиф этади. Бу компаниянинг сертификатлари халкаро стандарт X.509 талабларига жавоб беради. Бу сертификатлар маълумотлар ҳимоясининг катор маҳсулотларида, жумладан, ҳимояланган канал SSL протоколида ишлатилади.

## 5.4. Қатъий аутентификациялаш

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

Энг муҳими, исботловчи тараф факат сирни билишигини намойиш этади, сирни ўзи эса аутентификацион алмашиш мобайнида очилмайди. Бу текширувчи тарафнинг турли сўровларига исботловчи тарафнинг жавоблари ёрдами билан таъминланади. Бунда якуний сўров факат фойдаланувчи сирига ва протокол бошланишида ихтиёрий танланган катта сондан иборат бошлангич сўровга боғлик бўлади.

Аксарият холларда катъий аутентификациялашга биноан ҳар бир фойдаланувчи ўзининг маҳфий калитига эгалиги аломати бўйича аутентификацияланади. Бошкacha айтганда фойдаланувчи алоқа бўйича шеригининг тегишли маҳфий калитга эгалигини ва у бу калитни ахборот алмашинуви бўйича ҳақиқий шерик эканлигини исботлашга ишлата олиши мумкинлигини аниқлаш имкониятига эга.

X.509 стандарти тавсияларига биноан катъий аутентификациялашнинг куйидаги муолажалари фарқланади:

- 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 факат бир тарафини ҳақиқийлигини тасдиқлаш;

- узатилаётган ахборот яхлитлигининг бузилишини аниқлаш;
- «узатишнинг такрори» гипидаги ҳужумни аниқлаш;

- узатилаётган аутентификацион маълумотлардан факат текширувчи тараф фойдаланишини кафолатлаш.

*Икки томонлама аутентификацилашда* бир томонлилигига нисбатан исботловчи тарафга текширувчи тарафнинг қўшимча жавоби бўлади. Бу жавоб текширувчи томонни алоканинг айнан аутентификация маълумотлари мўлжалланган тараф билан ўрнатилаётганига ишонтириши лозим.

*Уч томонлама аутентификациялаш* таркибида исботловчи тарафдан текширувчи тарафга қўшимча маълумотлар узатилиши мавжуд. Бундай ёндашиш аутентификация ўтказишида вакт белгиларидан фойдаланишдан воз кечишга имкон беради.

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

Қатъий аутентификациялашнинг муайян вариантиларини кўришдан олдин бир мартали параметрларнинг вазифалари ва имкониятларига тўхташ лозим. Бир мартали параметрлар баъзида «*ponces*» – бир максадга бир маргадан ортиқ ишлатилмайдиган катталик деб аталади.

Хозирда ишлатиладиган бир мартали параметрлардан тасодифий сонлар, вакт белгилари ва кетма-кетликларнинг ракамларини кўрсатиш мумкин.

Бир мартали параметрлар узагишининг тақорланишини, аутентификацион алмашинув тарафларини алмаштириб қўйишни ва очик матнни танлаш билан хужум килишни олдини олишга имкон беради. Бир мартали параметрлар ёрдамида узатиладиган хабарларнинг ноёблигини, бир маънолилигини ва вактий кафолатларини таъминлаш мумкин. Бир мартали параметрларнинг турли хиллари алоҳида ишлатилиши, ёки бир-бирини тўлдириши мумкин.

Бир мартали параметрларнинг куйидаги ишлатилиш мисолларини кўрсатиш мумкин:

- «сўров-жавоб» принципида курилган протоколларда ўз вактидалигини текшириш. Бундай текширишда тасодифий сонлар, соатларни синхронлаш билан вакт белгилари ёки муайян жуфт

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

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

– хабарни ёки хабарлар кетма-кетлигини бир маъноли идентификациялаш. Бир оҳангда ўсувчи кетма-кетликнинг бир мартали кийматини (масалан, серия номерлари ёки вакт белгилари кетма-кетлиги) ёки мос узунликдаги тасодифий сонларни тузиш оркали 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 боғлик ҳолда куйидаги гурухларга 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 рақами имзо алгоритмлари асосидаги қатъий аутентификациялаш протоколлари.

### **Симметрик алгоритмларга асосланган қатъий аутентификациялаш. Kerberos протоколи**

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

Ушбу ёндашиш солда бўлиб туюлсада, аслида бундай аутентификациялаш протоколини ишлаб чикиш мураккаб ва хавфсизлик нукстай назаридан шубхасиз эмас.

Куйила шифрлашнинг симметрик алгоритмларига асосланган, ISO/IEC 9798-2да спецификацияланган аутентификациялаш протоколларининг учта мисоли келтирилган. Бу протоколлар бўлинувчи маҳфий қалитларни олдиндан таҳсиланишини кўзда гутади. Аутентификациялашнинг куйидаги варианларини кўриб чиқамиз.

- вакт белгиларидан фойдаланувчи бир томонлама аутентификациялаш;
- тасодифий сонлардан фойдаланувчи бир томонлама аутентификациялаш;
- икки томонлама аутентификациялаш.

Бу варианларнинг ҳар бирида фойдаланувчи маҳфий қалитни билишини намойиш килган холда, ўзининг ҳакиқийлигини исботлайди, чунки ушбу маҳфий қалит ёрдамида сўровларни расшифровка киласди. Аутентификациялаш жараёнида симметрик шифрлашни кўляшда узатиладиган маълумотларнинг яхлитлигини таъминлаш механизмини расм бўлиб колган усуслар асосида амалга ошириш ҳам зарур.

Куйидаги белгилашларни киритамиз:

$t_A$  - катнашувчи A генерациялаган тасодифий сон;

$t_B$  - катнашувчи B генерациялаган тасодифий сон;

$t_A$  - катнашувчи A генерациялаган вакт белгиси;

$E_K$  - қалит K да симметрик шифрлаш (қалит K олдиндан A ва B ўртасига таҳсиланиши шарт).

Вакт белгиларига асосланган бир томонлама аутентификациялаш:

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

Ушбу хабарни олиб расшифровка килганидан сўнг катнашувчи B вакт меткаси  $t_A$  ҳакиқий эканлигига ва хабарда кўрсатилган идентификатор ўзиники билан мос келишига ишонч хосил киласди. Ушбу хабарни кайгадан узатишни олдини олиш қалитни билмасдан туриб вакт меткаси  $t_A$  ни ва индентификатор Bни ўзгартириш мумкин эмаслигига асосланади.

Тасодифий сонлардан фойдаланишига асосланган бир томонлама аутентификациялаш:

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

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

Катнашувчи  $B$  катнашувчи  $A$  га тасодифий сон  $r_B$  ни жўнатади.

Катнашувчи  $A$  олинган сон  $r_B$  ва идентификатор  $B$  дан иборат хабарни шифрлайди ва шифрланган хабарни катнашувчи  $B$  га жўнатади. Катнашувчи  $B$  олинган хабарни расшифровка килади ва хабардаги тасодифий сонни катнашувчи  $A$  га юборгани билан таккослади. Қўшимча у хабардаги исмни текширади.

*Тасодифий 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 катнашувчи  $B$  олдинги протоколдаги текширишни амалга оширади ва катнашувчи  $A$  га аталган учинчи хабарга киритиш учун қўшимча тасодифий сон  $r_A$  ни расшифровка килади. Катнашувчи  $A$  учинчи хабарни олганидан сўнг  $r_A$  ва  $r_B$  ларнинг қийматларини текшириш асосида айнан катнашувчи  $B$  билан ишлаётганига ишонч хосил килади.

Аутентификация жараёнида учинчи тарафни жалб этиш билан фойдаланувчиларни аутентификациялашни таъминловчи протоколларнинг машхур намуналари сифатида Нидҳэм ва Шредернинг маҳфий калитларни тақсимлаш протоколини ва Kerberos протоколини кўрсатиш мумкин.

Kerberos протоколи «мижоз-сервер» ва хам локал ва хам глобал тармокларда 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 кизикиш ўйғотади.

Kerberos ишонч козонмаган тармокларда аутентификациялашни таъминлайди, яъни Kerberos ишлашида нияти бузук одамлар қуидаги харакатларни бажаришлари мумкин:

- ўзини тармок уланишининг эътироф этилган тарафларидан бири деб кўрсатиш;
- уланиша иштирок этаётган компьютерларнинг биридан фойдалана олиш;
- хар кандай пакетни ушлаб колиш, уларни модификациялаш ва ёки иккинчи марта узатиш.

Kerberos протоколида хавфсизлик таъминоти юкорида келтирилган нияти бузук одамларнинг харакатлари натижасида пайдо бўладиган хар кандай муаммоларнинг бетарафланишини таъминлайди.

Kerberos протоколи олдинги асрнинг 80-йилларида яратилган ва шу пайтгача бешта версияда ўз аксини топган катор 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 харакат килиб, тармоқ ресурсларидан мижознинг (мижоз иловасининг) фойдалинишини авторизациялаш билан тармоқда ишончли аутентификациялашни таъминлайди. Kerberos хизмати алоҳида маҳфий калитни тармоқнинг хар бир субъекти билан бўлишади ва бундай маҳфий калитни билиш тармоқ субъекти ҳақиқийлигининг исботига тенг кучлиdir.

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) алока килувчи иккита тараф ва калитларни тақсимлаш маркази KDC (Key Distribution Center) вазифасини бажарувчи ишонилган сервер KS иштирок этади.

Чакирувчи обьект А оркали, чакирилувчи обьект В оркали белгиланади. Сеанс катнашчилари, мос холда  $Id_A$  ва  $Id_B$  ноёб идентификаторларга эга. А ва В тарафлар, хар бири алоҳида, ўзининг маҳфий калитини сервер KS билан бўлишади.

Айтайлик. А тараф  $B$  тараф билан ахборот алмашып максадида сеанс калитини олмокчи. А тараф тармок оркали сервер  $KS$ га  $Id_A$  ва  $Id_B$  идентификаторларни юбориш билан калитлар тассималаниши даврини бошлаб беради:

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

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

Сўнгра сервер  $KS$   $B$  тарафга тегишли вактий белги  $T$ , таъсир муддати  $L$ , тасодифий калит  $K$ , идентификатор  $Id_B$  ни олиб уни  $A$  тараф билан бўлинган маҳфий 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 маҳфий калити билан расшифровка килиди ва ушбу хабар калитлар тассимотининг олдинги муолажасининг қайтарилиши эмаслигига ишонч хосил қилиш максадида вакт белгиси  $T$  ни текширали. Сўнгра  $A$  тараф ўзининг идентификатори  $Id_A$  ва вакт белгиси билан хабарни генерациялаб, уни сеанс калити  $K$  ёрдамида шифрлайди ва  $B$  тарафга узагади. Ундан ташкил,  $A$  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 факат  $B$  тараф расшифровака килиши мумкин.  $B$  тараф вакт белгиси  $T$ , таъсир муддати  $L$ , сеанс калити  $K$  ва идентификатор  $Id_A$  ни олади. Сўнгра  $B$  тараф сеанс калит  $K$  ёрдамида хабарнинг иккичи кисмини расшифровка килиди. Хабарнинг иккала кисмидаги  $T$  ва  $Id_A$  кийматларининг мос келиши  $A$  нинг  $B$  га нисбатан ҳакиқийлигини тасдиклайди.

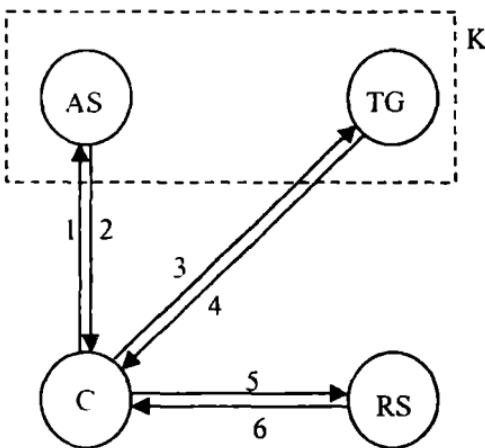
Ҳакиқийликни ўзаро тасдиклаш максадида  $B$  тараф вакт белгиси  $T$  плюс 1 дан иборат хабар яратали. уни  $K$  калит ёрдамида шифрлайди ва  $A$  тарафга жўнатади.

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

Агар бу хабар расшифровка килинганидан кейин *A* тараф күтилгандай натижани олса, у алоқа линиясининг бошка тарафида ҳакикатан *B* турғанлигига ишонч ҳосил килади.

Бу протокол барча қатнашувчиларнинг соатлари сервер *KS* соатлари билан синхронланганида муваффакиятли ишлайди. Таъкидлаш лозимки, бу протоколда *A* гарафнинг *B* тараф билан алоқа ўрнатишга ҳар бир хохишида сеанс қалитини олиш учун *KS* билан алмашинув зарур бўлади. Протоколнинг *A* ва *B* объектларни ишончли улаши учун, хеч бир қалит обрўсизланмаслиги ва сервер *KS* нинг химояланиши талаб этилади.

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



Белгилашлар:  
KS – *Kerberos* тизими сервери;  
AS – аутентификация сервери;  
TGS – мандатларни ажратиш хизмати сервери;  
RS – ахборот ресурслари сервери;  
С – *Kerberos* тизими-нинг мижози;

5.2-расм. *Kerberos* протоколининг ишлаш схемаси.

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

Ахборот ресурсларининг муайян максадли сервери *RS* дан фойдаланиш учун мижоз *C* *TGS* дан максадли сервер *RS* га мурожаат килишига мандат сўрайди. Ҳамма нарса тартибда бўлса *TGS* керакли тармок ресурсларидан фойдаланишга рухсат берилади. Клиент *C* га мандатни юборади.

Kerberos тизими ишлашининг асосий қадамлари (5.2.-расмга каралсун):

1.  $C \rightarrow AS$  – мижоз  $C$  нинг  $TGS$  хизматига мурожаат килишга 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 рухсати (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 хакикийлигини тасдиқлаш ва мижоз  $C$  га ахборот ресурсини (хизматни) тақдим этиш.

Мижоз билан сервер алоқасининг ушбу модели факат узатиладиган бошқарувчи ахборотнинг конфиденциаллиги ва яхшилиги 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 максадида Kerberos тармоқда ҳар кандай бошқариш ахбороти узатилганида маҳфий калитлар комплекси (мижознинг маҳфий калити, сервернинг маҳфий калити, мижоз-сервер жуфтининг маҳфий сеанс калитлари) ёрдамида кўп марта шифрлашни ишлатади. Kerberos шифрлашнинг алмаштириш ва хўш-функциялардан фойдаланиши мумкин, аммо маададлаш учун Triple DES ва MD5 алгоритмлари ўрнатилган.

Kerberos тизимида ишонч хужжатларининг 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 мандагдан фойдаланаётган мижознинг хакикий эканлигини текширишда фойдаланиши мумкин.

*Аутентификатор* – мандат билан бирга кўрсатилувчи кўшимча атрибути (аломат). Куйида Kerberos хужжатларида ишлатилувчи белгиланишлар тизими келтирилган:

*C* – мижоз;

*S* – сервер;

*a* – мижознинг тармок манзили;

*v* – мандат таъсири вақтининг бошланиши ва охири;

*m* – вакт белгиси;

$K_x$  – маҳфий калит  $x$ ;

$K_{x,v}$  –  $x$  ва у учун сеанс калити;

{ $m$ } $K_x$  – субъект  $x$  нинг маҳфий калити  $K_v$  билан шифрланган хабар  $m$ ;

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

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

### ***Kerberos мандати***

Kerberos мандати куйидаги шаклга эга:

$$T_{c,s} = S, \{C, a, v, K_{c,s}\} K_s.$$

Мандат битта мижозга катъий белгиланган сервердан фойдаланиш учун катъий белгиланган вактга берилади. Унинг таркибида мижоз исми, унинг тармок манзили, мижоз ҳаракатининг бошланиш ва тугаш вакти ва сервернинг маҳфий калити  $K_s$  шифрланган сеанс калити  $K_{c,s}$  бўлади. Мижоз мандатни расшифровка қила олмайди (у сервернинг маҳфий калитини билмайди), аммо у мандатни шифрланган шаклда серверга кўрсатиши мумкин. Мандат тармок оркали узатилаётганда тармокдаги яширинча эшишиб турувчиларнинг бирортаси хам уни ўқий олмайди ва ўзгартира олмайди.

### ***Kerberos аутентификатори***

Kerberos аутентификатори куйидаги 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, вакт 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 да-лолат беради. Иккинчидан, шифрланган очик матнда вакт белгиси мавжуд. Бу вакт белгиси аутентификатор ва мандатни ушлаб

колган нияти бузук одамга улардан бирор вакт ўтганидан сўнг аутентификациялаш муолжасини ўтишда ишлатишига имкон бермайди.

### *Kerberos хабарлари*

Kerberosнинг 5-версиясида хабарларниң куйпидаги турлари ишлатилади (5.2-расмга каралсинг).

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 фойдаланишини батайсан кўрайлик.

### *Дастлабки мандатни олиш*

Мижоздан шахсини исботловчи ахборогнинг кисми унинг пароли мавжуд. Мижозни паролини тармок орқали жўнатишига мажбур килиб бўлмайди. Kerberos протоколи паролини обрўсизлантириш эҳтимолини 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 киригади, 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 генерациялади. Kerberos бу сеанс калитини мижознинг маҳфий калити билан шифрлайди. Сўнгра у TGS хизматига мижознинг ҳакиқийлигини исботловчи TGT (*Ticket Granting Ticket*) мандатининг ажратилиши учун мижозга мандат яратади. TGS нинг маҳфий калитида TGT шифрланади ва унинг таркибида мижоз ва сервер идентификатори, TGS – мижоз жуфтининг сеанс калити ҳамда TGT таъсирининг бошланиш ва охирги вактлари

бўлади. Аутентификациялаш сервери бу иккита шифрланган хабарни мижозга юборади.

Энди мижоз бу хабарларни қабул қиласи, биринчи хабарни ўзининг маҳфий калити  $K_C$  билан расшифровка килиб, сеанс калити  $K_{C,igs}$  ни хосил қиласи. Маҳфий калит мижоз паролининг бир томонлама хэш-функцияси бўлганилиги сабабли конуний фойдаланувчига хеч қандай муаммо туғилмайди. Нияти бузук одам тўғри 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-кыйматни, уларнинг обрўсизланиш эҳтимолликларини пасайтириш максадида, ўчиради. Агар нияти бузук одам мижоз хотираси таркибининг нусхасини олишга ўринса, у фактат  $TGT$  ва сеанс калитини олади. Бу маълумотлар фактат  $TGT$  таъсири вақтидагина мухим хисобланади.  $TGT$  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 хар бир хизмат учун алоҳида мандат олиши мумкин. Шу мақсадда мижоз  $TGS$  хизматига  $TGT$  мандати ва аутентикатордан иборат сўров юбориши лозим. (Амалда сўровни дастурий таъминот автоматик тарзда, яъни фойдаланувчига билдирилсанда юборади.) Мижоз ва  $TGS$  сервери жуфтининг калитида шифрланган аутентикатор таркибида мижоз ва унга керакли сервернинг идентификатори, тасодифий сеанс калити ва вакт белгиси бўлади.

$TGS$  сўровни олиб, ўзининг маҳфий калитида  $TGT$  ни расшифровка қиласи. Сўнгра  $TGS$   $TGT$  даги сеанс калитидан аутентикаторни расшифровка килишда фойдаланади. Ниҳоясида аутентикатордаги ахборотни мандат ахбороти билан тақкосланади. Аниқроғи, чиптадаги мижознинг тармок манзили сўровда кўрсатилган тармок манзили билан ҳамда вакт белгиси жорий вакт

билин солиширилади. Агар барчаси мос келса, *TGS* сўровни бажа-ришга рухсат беради.

Вакт белгиларини текширишда барча компьютерларнинг соатлари, бўлмаганда, бир неча минут аниклигида синхронланганлиги кўзда тутилади. Агар сўровда кўрсатилган вакт жорий ондан анчагина фарқ килса, *TGS* бундай сўровни олдинги сўровни қайтаришга уриниш деб хисоблайди.

*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 вакт белгиси билан килинган бошқа сўров кайтарилади.

Тўғри сўровга жавоб тарикасида *TGS* мижозга мақсад сервердан фойдаланиш учун мандат тақдим этади. *TGS* мижоз ва мақсад сервери учун мижоз ва *TGS* га умумий бўлган сеанс калитидаги шифрланган сеанс калитини хам яратади. Бу иккала хабар мижозга юборилади. Мижоз хабарни расшифровка килади ва сеанс калитини чикариб олади.

### *Хизмат сўрови*

Энди мижоз ўзининг ҳакикийлигини мақсад серверига исботлаши мумкин. Мақсад серверида аутентификациядан муваффакиятли ўтиш учун мижоз таркибида ўзининг исми, тармоқ манзили, вакт белгиси бўлган ва сеанс калити «мижоз-сервер»да шифрланган аутентификаторни яратади ва уни *TGS* хизматидан олиб берилган мақсад серверининг маҳфий калитидаги шифрланган мандат билан бирга жўнатади.

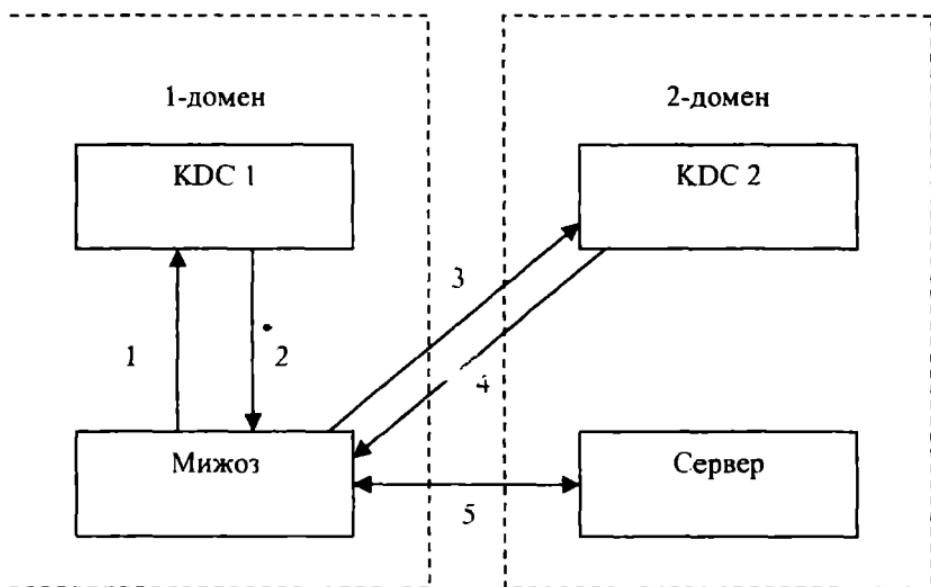
Мақсад сервери мижоздан маълумотларни олиб, аутентификаторни ўзининг маҳфий калитидаги расшифровка килади ва ундан «мижоз-сервер» сеанс калитини чикариб олади. Мандат хам текширилади. Текшириш муолажаси «мижоз-*TGS*» сессиясида ўтказила-диган муолажага ўхшаш, яъни тармоқ манзиллари ва вакт белгисининг мослиги текширилади. Агар барчаси мос келса, сервер мижознинг ҳакикийлигига ишонч хосил килади.

Агар илова ҳакикийликнинг ўзаро текширилишини талаб этса, сервер мижозга таркибида сеанс калитидаги шифрланган вакт белгиси бўлган хабарни юборади. Бу серверга тўғри маҳфий калитнинг

маълум эканлигини ва у мандат ва гувохномани расшифровка кила олишини исботлайди. Зарурият тугилганида мижоз ва сервер кеинги хабарларни умумий калитга шифрлашлари мумкин. Чунки бу калит фактат уларга маъчум, бу калит билан шифрланган охирги хабар иккинчи тарафдан юборилганига иккала тараф ишонч хосил килишлари мумкин. Амалда бу барча мураккаб муолажалар автоматик тарзда бажарилади ва мижозга қандайdir нокулайликлар етказилмайди.

### *Доменлараро аутентификациялаш ҳусусиятлари*

Kerberos дан доменлараро аутентификациялашда ҳам фойдаланиш мумкин. Мижоз бошқа домендаги сервердан фойдаланиш мақсадида калитларни тақсимлаш маркази *KDC* га мурожаат килса, *KDC* мижозга сўралаётган сервер жойлашган доменнинг *KDC* ига мурожаат этишга қайта манзиллаш мандатини (*referal ticket*) тақдим этади (5.3-расм).



5.3-расм. Kerberos протоколида доменлараро аутентификациялаш схемаси.

Расмда куйидаги белгилашлар кабул килинган:

1. Аутентификациялашга сўров.

2. *KDC1* учун *TGT*
3. *KDC2* учун *TGT*.
4. Сервердан фойдаланиш мандати.
5. Маълумотларни аутентификациялаш ва алмашиш.

Кайта манзиллаш мандати иккита домен KDCсиининг жуфтли алоқа калитида шифрланган *TGT*дир. Бунда мижозга сервердан фойдаланишга мандатни сўралаётган сервер жойлашган KDC тақдим этади.

Жуда кўп доменли тармоқда аутентификациялаш учун Kerberosдан фойдаланиш назарий жиҳатдан мумкин бўлсада, мурожаатлар сонининг доменлар сонига муганосиб равишда ошиши сабабли, сўровларни муайян KDCларга бир маънода кайта манзил-ловчи қандайдир марказий домен куришга тўғри келади.

### *Kerberos хавфсизлиги*

Kerberos, криптографик химоялашнинг бошка хар қандай дастурий воситаси каби ишончсиз дастурий мухитда ишлайди. Ушбу мухитнинг хужжатлаштирилмаган имкониятлари ёки нотўғри конфигурацияси жиддий ахборотнинг чиқиб кетишига олиб келиши мумкин. Ҳатто, калитлар фойдаланувчи ишлаш ссансида факат оператив хотиграда сакланса ҳам операцион тизимдаги бузилиш калитларнинг каттиқ дискда нусхаланишига олиб келиши мумкин.

Kerberos дастурий таъминоти ўрнатилган ишчи станциясидан кўпчилик фойдаланувчи режимнинг ишлатилиши ёки ишчи станциялардан фойдаланишнинг назорати бўлмаслиги дастурзакладкани киритиш ёки криптографик дастурий таъминотни модификациялаш имкониятини туғдиради.

Шу сабабли, Kerberos хавфсизлиги кўп жиҳатдан ушбу протокол ўрнатилган ишчи станцияси химоясининг ишончлилигига боғлиқ.

Kerberos протоколининг ўзига қўйидаги катор талаблар қуилади:

- Kerberos хизмати хизмат килишдан воз кечишга йўналтирилган ҳужумлардан химояланиши шарт;
- вакт белгиси аутентификация жараёнида қатнашиши сабабли, тизимдан фойдаланувчиларининг барчаси учун тизимли вактни синхронлаш зарур;
- Kerberos паролни саралаш орқали ҳужум килишдан химояламайди. Муаммо шундаки, *KDC* да сакланувчи фойдаланувчи ка-

лити унинг паролини хэш-функция ёрдамида қайта ишлаш натижасидир. Паролининг бўштигига уни сарашиб тошиш мумкин.

— Kerberos хизмати рухсатсиз фойдаланишининг барча турлиридан ишончли химояланиши шарт;

мижоз олган маидатлар ҳамда маҳфий қалитлар рухсатсиз фойдаланишдан химояланиши шарт.

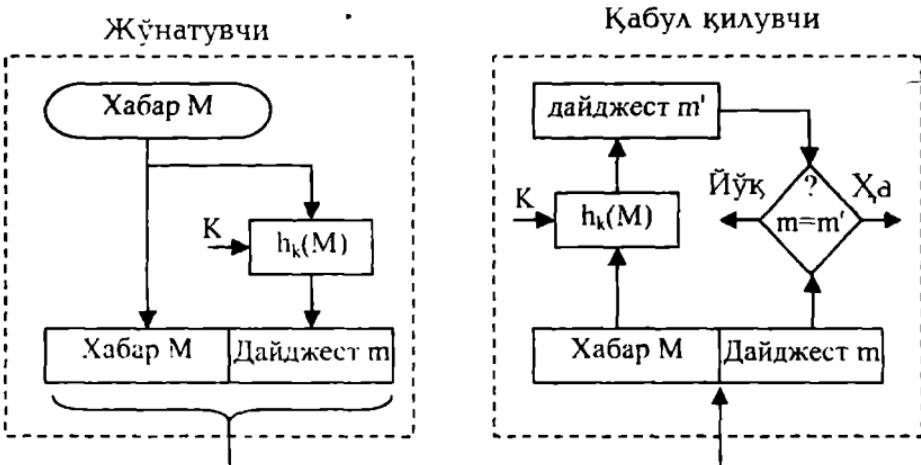
Юкорида келтирилган таъабларнинг бажарилмаслиги муваффакиятли хужумгага сабаб бўлиши мумкин.

Хозирда Kerberos протоколи аутентификациялашнинг кенг таркалган воситаси хисобланади. Kerberos турли криптографик схемалар, хусусан, очик қалитли шифрлаш билан биргаликда ишлатилиши мумкин.

### Бир томонлама қалиғли хэш-функциялардан фойдаланишга асосланган протоколлар

Бир томонлама хэш-функция ёрдамида шифрлашнинг ўзига хос хусусияти шундаки, у мохияти бўйича бир томонламадир, яъни тескари ўзгартириш-кабул қилувчи тарафда расшифровка килиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва кабул қилувчи) бир томонлама шифрлаш муолажасидан фойдаланади.

Шифрланадиган маълумот  $M$  га қўлланилган  $K$  параметр-қалитли бир томонлама хэш-функция  $h_k(\cdot)$  натижада, байтларнинг белгиланган катта бўлмагани сонидан иборат хэш-кыймат (дайджест)  $m$  ни беради (5.4-расм).



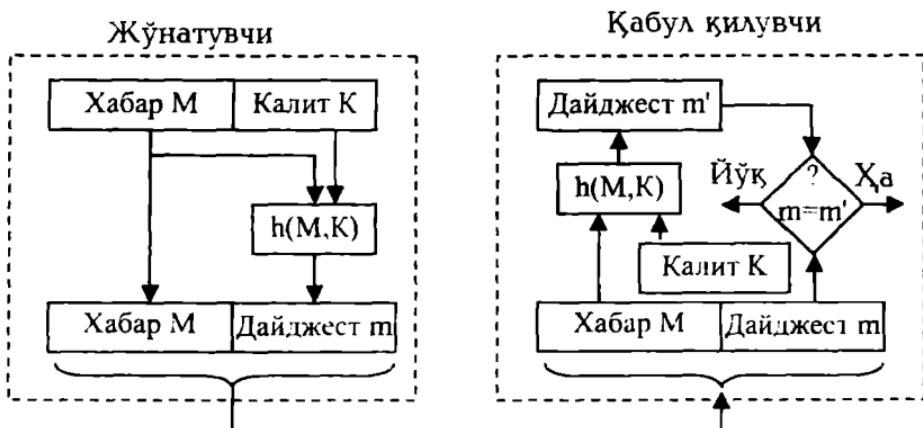
5.4-расм. Маълумотлар яхшилигини текширишда бир томонлама хэш-функцияини ишлатилиши (I-вариант).

Дайджест тарабул килувчига дастлабки хабар  $M$  билан бергә узатылади. Хабарни тарабул килувчи, дайджест олинишида қандай бир томонлама хэш-функция ишлатылғанлыгини билған холда, расшифровка килингандай хабар  $M$  дан фойдаланиб, дайджестни бошкадан хисоблайди. Агар олингандай дайджест билан хисобланған дайджест мөс 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 йигиндиси сифатида караш мумкин. Аммо, дайджест ва оддий назорат йигиндисидан орасида жиддий фарқ хам мавжуд. Назорат йигиндисидан алоканинг ишончсиз линияси бўйича узатиладиган хабарларнинг ахлитлигини текшириш воситаси сифатида фойдаланилади. Текширишнинг бу воситаси нияти бузук одамлар билан кўрашишга мўлжалланмаган. Чунки, бу холда назорат йигиндисининг янги кийматини кўшиб хабарни алмаштириб кўйишга уларга ҳеч ким халақит бермайди. Кабул килувчи бунда ҳеч нарсани сезмайди.

Дайджестни хисоблашда, оддий назорат йигиндисидан фаркли равишда, маҳфий калитлар ишлатилади. Агар дайджест олинишида фактат жўнатувчи ва тарабул килувчига 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 бошка варианти келтирилган.



5.5-расм. Маълумотлар яхлитлигини текширишда бир томонлама хэш-функцияни ишлатиши (II-вариант).

Бу холда бир томонлама хэш-функция  $h(\cdot)$  параметр-калитга эга эмас, аммо у маҳфий калит билан тўлдирилган хабарга кўлланилади, яъни жўнатувчи дайджест  $m=h(M, K)$ ни хисоблайди. Кабул килувчи дастглабки хабарни чиқариб олиб, уни ўша маълум маҳфий калит билан тўлдиради. Сўнгра олинган маълумотларга бир томонлама хэш-функция  $h(\cdot)$ ни кўллайди. Хисоблаш натижаси – дайджест  $m$  тармок орқали олинган дайджест  $m$  билан таккосланади.

### **Асимметрик алгоритмларга асосланган қатъий аутентификациялаш**

Қатъий аутентификациялаш протоколларида очик калитли асимметрик алгоритмлардан фойдаланиш мумкин. Бу холда исботловчи маҳфий калитни билишилигини қўйидаги усулларнинг бири ёрдамида намойиш этиши мумкин:

- очик калитда шифрланган сўровни расшифровка килиш;
- сўров сўзига рақамли имзосини қўйиш.

Аутентификацияга зарур бўлган калитларнинг жуфти, хавфсизлик муроҳазасига кўра, бошқа мақсадларга (масалан, шифрлашда) ишлатилмаслиги шарт. Очик калитли танланган тизим шифрланган матнни танлаш билан хужумларга, ҳатто бузғунчи ўзини текширувчи деб қўрсатиб ва унинг номидан харакат килганда ҳам, бардош бериши лозимлигига фойдаланувчиларни огохлантириш керак.

### **Шифрлашнинг асимметрик алгоритмларидан фойдаланиб аутентификациялаш.**

Шифрлашнинг асимметрик алгоритмларидан фойдаланишга асосланган протоколга мисол тариқасида аутентификациялашнинг қўйидаги протоколини келтириш мумкин:

$$A \leftarrow B : h(r), B, P_A(r, B),$$

$$A \rightarrow B : r.$$

Катнашувчи  $B$  тасодифий холда  $r$  ни танлайди ва  $x=h(r)$  кийматини хисоблайди ( $x$  киймати  $r$  нинг кийматини очмасдан туриб  $r$  ни билишилигини намойиш этади), сўнгра у  $e = P_A(r, B)$  кийматни хисоблайди.  $P_A$  орқали асимметрик шифрлаш алгоритми фараз килинса,  $h(\cdot)$  орқали хэш-функция фараз килинади. Катнашувчи  $B$  ахборот хабарни катнашувчи  $A$  га жўнатади. Катнашувчи  $A$   $e = P_A(r, B)$  ни расшифровка килади ва  $r'$  ва  $B'$  кийматларни олади ҳамда  $x'=h(r')$  ни хисоблайди. Ундаи кейин

$x=x'$  эканлигини ва  $B'$  идентификатор хакиқатан қатнашувчи  $B$  га күрсатаётганини тасдиқловчи қатор таққослашлар бажарилади. Таққослаш муваффакиятли ўтса қатнашувчи  $A$  га қатнашувчини  $B$  гани узатади. Қатнашувчи  $B$   $r$  ни олганидан сўнг уни биринчи хабарда жўнатган киймат эканлигини текширади.

Кейинги мисол сифатида асимметрик шифрлашга асосланган Нидхем ва Шредернинг модификацияланган протоколини келтирамиз. Факат аутентификациялашда ишлатилувчи Нидхем ва Шредер протоколи вариантини кўришда  $P_B$  орқали қатнашувчи  $B$  нинг очик калити ёрдамида шифрлаш алгоритми фараз килинади. Протокол куйидаги 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, вакт белгиси ва тасодифий сонлардан фойдаланиш асосидаги аутентификациялаш схемаси спецификацияланган. Ушбу схемани тавсифлаш учун куйидаги белгилашларни киритамиз:

- $t_A$ ,  $r_A$  ва  $r_B$  – мос холда вакт белгиси ва тасодифий сонлар;
- $S_A$  – қатнашувчи  $A$  генерациялаган имзо;
- $S_B$  – қатнашувчи  $B$  генерациялашган имзо;
- $cert_A$  – қатнашувчи  $A$  очик калитининг сертификати;
- $cert_B$  – қатнашувчи  $B$  очик калитининг сертификати.

Мисол тариқасида аутентификациялашнинг куйидаги протоколларини келтирамиз:

1. Вакт белгисидан фойдаланиб бир томонлама аутентификациялаш:

$$A \rightarrow B : cert_A, t_A, B, S_A(t_A, B)$$

Қатнашувчи  $B$  ушбу хабарни олганидан сўнг вакт белгиси  $t_A$  нинг, олинган идентификатор  $B$  нинг тўғрилигини ва сертификат  $cert_A$  даги очик калитдан фойдаланиб рақамли имзо  $S_A(t_A, B)$  нинг корректигигини 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 қиласди; сертификат  $cert_A$  дан олинган катнашувчи  $A$  очик қалитидан 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 вактда инсоннинг физиологик параметрлари ва характеристикаларини, хулкининг хусусиятларини ўлчаш орқали фойдаланувчини ишончли аутентификациялашга имкон берувчи биометрик аутентификациялаш кенг тарқалмоқда.

Биометрик аутентификациялаш усуллари анъанавий усулларга нисбатан қўйидаги афзалликларга эга:

- биометрик аломатларни ноёблиги туфайли аутентификациялашнинг ишончлилик даражаси юкори;
- биометрик аломатларнинг ишга лаёкатли шахсдан ажратиб бўлмаслиги;
- биометрик аломатларни сохталаштиришнинг кийинлиги.

Фойдаланувчини аутентификациялашда фаол ишлатиладиган биометрик аломатлари қўйидагилар:

- бармок излари;
- кўл панжасининг геометрик шакли;
- юзнинг шакли ва ўлчамлари;
- овоз хусусиятлари;
- кўз ёйи ва тўр пардасининг накши.

Аутентификациянинг биометрик кисм тизими ишлашининг намунавий схемаси қўйидагича. Гизимда рўйхатга олинишида фойдаланувчидан ўзининг характерли аломатларини бир ёки бир неча марта намойиш килиниши талаб этилади. Бу аломатлар

(хакикий сифатида маълум) тизим томонидан конуний фойдаланувчининг киёфаси сифатида рўйхатга олинади. Фойдаланувчи нинг бу киёфаси тизимда электрон шаклда сакланади ва ўзини конуний фойдаланувчи деб даъво килган хар бир одамни текширишда ишлатилади. Тақдим этилган аломатлар мажмуаси билан рўйхатга олингандарининг мослиги ёки мос келмаслигига караб карор кабул килинади. Истеъмолчи нуктаи назаридан биометрик аутентификациялаш тизими куйидаги иккита параметр орқали характерланади:

- хатолик инкорлар коэффициенти FRR (false-reject rate);
- хатолик тасдиклар коэффициенти FAR (false-alarm rate).

*Хатолик инкор* тизим конуний фойдаланувчи шахсини тасдикламаганда пайдо бўлади (одатда FRR киймати тахминан 100 дан бирни ташкил этади). *Хатолик тасдиқ* тизим ноконуний фойдаланувчи шахсини тасдиклаганида пайдо бўлади (одатда, FAP киймати тахминан 10000 дан бирни ташкил этади). Бу иккала коэффициент бир бири билан боғлиқ: хатолик инкор коэффициентининг хар бирига маълум хатолик тасдик коэффициенти мос келади. Муқаммал биометрик тизимда иккала хатоликнинг иккала параметри нолга тенг бўлиши шарт. Афсуски, биометрик тизим идеал эмас, шу сабабли ниманидур қурбон килишга тўғри келади. Одатда, тизимли параметрлар шундай созланадики, мос хатолик инкорлар коэффициентини аникловчи хатолик тасдикларнинг исталган коэффициентига эришилади.

## **Биометрик аутентификациялашнинг дактилоскопик тизими**

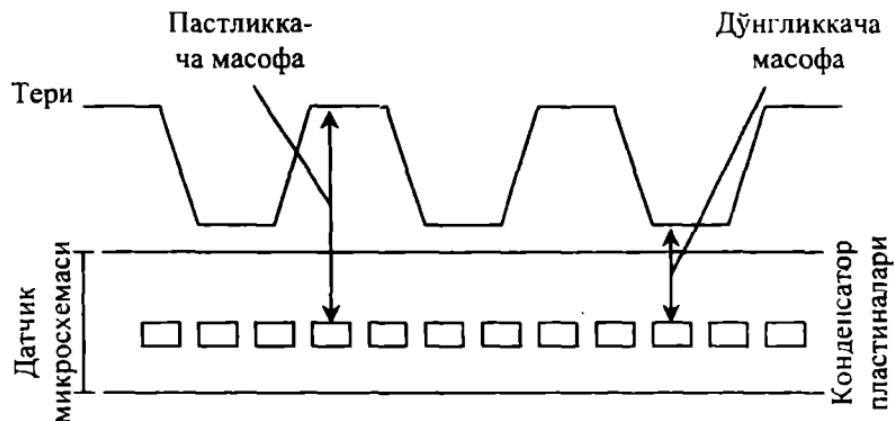
Биометрик тизимларнинг аксарияти идентификациялаш параметри сифатида бармок изларидан фойдаланади (аутентификациянинг дактилоскопик тизими). Бундай тизимлар содда ва куляй, аутентификациялашнинг юқори ишончлилигига эга. Бундай тизимларнинг кенг тарқалишига асосий сабаб бармок излари бўйича катта маълумотлар баъзасининг мавжудлигидир. Бундай тизимлардан дунёда асосан полиция, турли давлат ва баъзи банк ташкилотлари фойдаланади.

Аутентификациянинг дактилоскопик тизими куйидагича ишлайди. Аввал фойдаланувчи рўйхатга олинади. Одатда, сканерда бармокнинг турли холатларида сканерлашнинг бир неча варианти амалга оширилади. Табиийки, намуналар бир-биридан бир оз фарқланади ва қандайдир умумлаштирилган намуна, «паспорт» шакллантирилиши талаб этилади. Натижалар аутентификациянинг маълумотлар базасида хотирланади. Аутентификациялашда сканерланган бармок изи маълумотлар базасидаги «паспортлар» билан тақкосланади.

**Бармок изларининг сканерлари.** Бармок изларини сканерловчи анъанавий курилмаларда асосий элемент сифатида бармокнинг характерли расмини ёзувчи кичкина оптик камера ишлатилади. Аммо, дактилоскопик курилмаларни ишлаб чиқарувчиларнинг кўпчилиги интеграл схема асосидаги сенсорли курилмаларга эътибор бермоқдалар. Бундай тенденция бармок изларига асосланган аутентификациялашни кўллашнинг янги соҳаларини очади.

Бундай технологияларни ишлаб чиқувчи компаниялар бармок изларини олишда турли, хусусан электрик, электромагнит ва бошка усулларни амалга оширувчи воситалардан фойдаланадилар.

Сканерлардан бири бармок изи гасвирини шакллантириш мақсадида тери кисмларининг сифим қаршилигини ўлчайди. Масалан, Veridicom компаниясининг дактилоскопик курилмаси ярим-ўтказгичли датчик ёрдамида сифим қаршилигини аниклаш орқали ахборотни йиғади. Сенсор ишлашининг принципи куйидагича: ушбу асбобга куйилган бармок конденсатор пластиналарининг бири вазифасини ўтайди (5.6-расм). Сенсор сиртида жойлашган иккинчи пластина конденсаторнинг 90000 сезигир пластинкали кремний микросхемасидан иборат. Сезигир сифим датчиклари бармок сирти дўнгликлари ва пастликлари орасидаги электрик майдон кучининг ўзгаришини ўлчайди. Натижада, дўнгликлар ва пастликларгача бўлган масофа аникланиб, бармок изи тасвири олинади.



5.6-расм. Сенсор ишлашининг принципига.

Интеграл схема асосидаги сенсорли текширишда AuthenTec компаниясида ишлатилувчи усул аникликни яна ҳам оширишга имкон беради.

Катор ишлаб чиқарувчилар биометрик тизимларни смарт-карталар ва карта-калитлар билан комбинациялайдилар.

Интеграл схемалар асосидаги бармоқ излари датчикларининг кичик ўлчамлари ва юкори бўлмаган нархи уларни химоя тизими учун мукаммал интерфейсга айлантиради. Уларни калитлар учун брелокларга ўрнатиш мумкин. Натижада, фойдаланувчи компьютердан бошлаб то кириш йўли, автомобиллар ва банкоматлар эшикларидан химояли фойдаланишини таъминлайдиган универсал калитга эга бўлади.

*Кўл панжасининг геометрик шакли бўйича аутентификациялаш тизимлари.* Кўл панжаси шаклини ўкувчи курилмалар бармоқлар узунлигини, кўл панжа қалинлиги ва юзасини ўлчаш оркали кўл 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 кўл панжасини индивидуал сканерида ёки марказлаштирилган маълумотлар базасида сакланиши мумкин. Кўл панжасини сканерловчи курилмалар нархининг юкорилиги ва ўлчамларининг катталиги сабабли тармок мухитида камдан-кам ишлатилсада, улар қатъий хавфсизлик режимига ва шиддатли трафикка эга бўлган хисоблаш мухити (сервер хоналари ҳам бунга киради) учун куляй хисобланади. Уларнинг аниқлиги юкори ва инкор коэффициенти яъни инкор этилган конуний фойдаланувчилар фоизи кичик.

*Юзниг тузилиши ва овоз бўйича аутентификацияловчи тизимлар.* Бу тизимлар арzonлиги туфайли энг фойдаланувчан хисобланадилар. чунки аксарият замонавий компьютерлар видео ва аудео воситаларига эга. Бу синф тизимлари телекоммуникация тармокларида масофадаги фойдаланувчи субъектни идентификациялаш учун ишлатилади. *Юз тузилишини сканерлаш технологияси* бошка биометрик технологиялар яроксиз бўлган иловалар учун тўғри келади. Бу холда шахсни идентификациялаш ва верификациялаш учун кўз, бурун ва лаб хусусиятлари ишлатилади. Юз тузилишини аниқловчи курилмаларни ишлаб чиқарувчилар фойдаланувчини идентификациялашда хусусий математик алгоритмлардан фойдаланадилар.

Маълум бўлишича, кўпгина ташкилотларнинг ҳодимлари юз тузилишини сканерловчи курилмаларга ишонмайдилар. Уларнинг

фирми камера уларни расмга олади, сўнгра суратни монитор экранига чиқаради. Камеранинг сифати эса паст бўлиши мумкин. Ундан ташкари юз тузилишини сканерлаш биометрик аутентификациялаш усуллари ичидаги ягона, текширишга рухсатни талаб килемайдиган (яширинган камера ёрдамида амалга оширилиши мумкин) усул хисобланали.

Таъкидлаш лозимки, юз тузилишини аниклаш технологияси янада такомиллаштирилиши талаб этади. Юз тузилишини аникловчи аксарият алгоритмлар куёш ёруғлиги жадаллигининг кун бўйича тебраниши натижасидаги ёруғлик ўзгаришига таъсирчан бўладилар. Юз холатининг ўзгариши ҳам аниклаш натижасига таъсир этади. Юз холатининг  $45^{\circ}$  га ўзгариши аниклашни самарасиз бўлишига олиб келади.

*Овоз бўйича аутентификациялаш тизимлари.* Бу тизимлар арzonлиги туфайли фойдаланувчан хисобланадилар. 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 аниклаш нуткни аниклашдан фаркланади. Чунки нуткни аникловчи технология абонент сўзини изохласа, овозни аниклаш технологияси сўзловчининг шахсини тасдиқлайди. Сўзловчи шахсини тасдиқлаш баъзи чегараланишларга эга. Турли одамлар ўхшаш овозлар билан гапириши мумкин, ҳар кандай одамнинг овози вакт мобайнида кайфияти, хиссийтлик холати ва ёшига боғлик ҳолда ўзгариши мумкин. Унинг устига телефон аппаратларнинг турли-туманлиги ва телефон орқали боғланишларнинг сифати сўзловчи шахсини аниклашни кийинлаштиради. Шу сабабли овоз бўйича аниклашни юз тузилишини ёки бармок изларини аниклаш каби бошка усуллар билан биргаликда амалга ошириш максадга мувофик хисобланади.

*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 хисобланади. Кўз туби қон томирларининг расми ҳатто эгизакларда ҳам фаркланади. Идентификациялашнинг бу воситаларидан хавфсизликнинг юкори даражаси талаб этилганида (масалан,

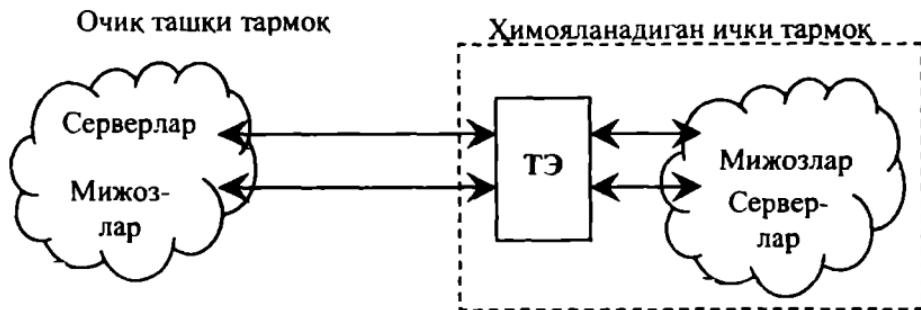
харбий ва мудофаа объектларининг режимли зоналарида) фойдаланилади.

Биометрик ёндашиш «ким бу ким» эканлигини аниклаш жараёнини соддалаштиришга имкон беради. Дактилоскопик сканерлар ва овозни аникловчи қурилмалардан фойдаланиш ходимларни тармокқа киришларида мураккаб паролларни эслаб қолищдан халос этади. Қатор компаниялар корхона масштабидаги бир мартали аутентификация SSO (Single Sign-On) га биометрик имкониятларни интеграциялайдилар. Бундай бириктириш тармок маъмурларига паролларни бир мартали аутентификациялаш хизматини биометрик технологиялар билан алмаштиришга имкон беради. Шахсни биометрик аутентификациялашнинг биринчилар каторида кенг тарқалган соҳаларидан бири мобил тизимлари бўлди. Муаммо факат компьютер ўғирланишидаги йўқотишларда эмас, балки ахборот тизимининг бузилиши катта заарга олиб келиши мумкин. Ундан ташқари, ноутбуклар дастурий боғланиш (мобил компьютерларда сакланувчи пароллар ёрдамида) орқали корпоратив тармоқдан фойдаланишин тез-тез амалга оширади. Бу муаммоларни кичик, арzon ва катта энергия талаб этмайдиган бармок излари датчиклари ечишга имкон беради. Бу қурилмалар мос дастурий таъминот ёрдамида ахборотдан фойдаланишнинг мобил компьютерда сакланадиган тўргта сатхи – рўйхатга олиш, экранни саклаш режимидан чиқиш, юклаш ва файлларни дешифрациялаш учун аутентификацияни бажаришга имкон беради.

Фойдаланувчини биометрик аутентификациялаш маҳфий калитдан фойдаланишин модул кўринишида шифрлашда жиддий ахамиятга эга бўлиши мумкин. Бу модул ахборотдан факат хакикий хусусий калит эгасининг фойдаланишига имкон беради. Сўнгра калит эгаси ўзининг маҳфий калитини ишлатиб хусусий тармоклар ёки Internet орқали узатилаётган ахборотни шифрлаши мумкин.

## 6.1. Тармоқларапро экранларнинг ишлаш хусусиятлари

Тармоқларапро экран (ТЭ) – брандмауэр ёки *firewall* системаси деб ҳам аталувчи тармоқларапро химоянинг ихтиослаштирилган комплекси. Тармоқларапро экран умумий тармоқни икки ёки ундан кўп қисмларга ажратиш ва маълумот пакетларини чегара оркали умумий тармоқнинг бир қисмидан иккинчисига ўтиш шартларини белгиловчи коидалар тўпламини амалга ошириш имконини беради. Одатда, бу чегара корхонанинг корпоратив (локал) тармоғи ва Internet глобал тармоқ орасида ўтказилади. Тармоқларапро экранлар гарчи корхона локал тармоғи уланган корпоратив интрагармоғидан килинувчи хужумлардан химоялашда ишлатилишлари мумкин бўлсада, одатда, улар корхона ички тармоғини Internet глобал тармоқдан сукилиб киришдан химоялайди. Аксарият тижорат ташкилотлари учун тармоқларапро экранларнинг ўрнатилиши ички тармоқ хавфсизлигини таъминлашнинг зарурый шарти хисобланади.



6. 1-расм. Тармоқларапро экранни улаш схемаси.

Рухсат этилмаган тармоқларапро фойдаланишга карши таъсир кўрсатиш учун тармоқларапро экран ички тармоқ хисобланувчи

ташкилотнинг химояланувчи тармоғи ва ташки ғаним тармок орасида жойланиши лозим (6.1-расм). Бунда бу тармоқлар орасидаги барча алоқа факат тармоқлараро экран орқали амалга оширилиши лозим. Ташкилий нуқтаи назаридан тармоқлараро экран химояланувчи тармок таркибига киради.

Ички тармокнинг кўпгина узелларини бирданига химояловчи тармоқлараро экран кўйидаги иккита вазифани бажариши керак:

- ташки (химояланувчи тармокка нисбатан) фойдаланувчиларнинг корпоратив тармокнинг ички ресурсларидан фойдаланишини чегаралаш. Бундай фойдаланувчилар каторига тармоқлараро экран химояловчи маълумотлар базасининг серверидан фойдаланишга уринувчи шериклар, масофадаги фойдаланувчилар, хакерлар, ҳатто компаниянинг ходимлари киритилиши мумкин;

- химояланувчи тармокдан фойдаланувчиларнинг ташки ресурслардан фойдаланишларини чегаралаш. Бу масаланинг ечилиши, масалан, сервердан хизмат вазифалари талаб этмайдиган фойдаланишни тартибга солишга имкон беради.

Хозирда ишлаб чиқарилаётган тармоқлараро экранларнинг тавсифларига асосланган холда, уларни қўйидаги асосий аломатлари бўйича туркумлаш мумкин:

#### *OSI модели сатҳларида ишлаши бўйича:*

- пакетли фильтр (экранловчи маршрутизатор – screening router);
- сеанс сатҳи шлюзи (экранловчи транспорт);
- татбикӣ шлюз (application gateway);
- эксперт сатҳи шлюзи (stateful inspection firewall).

#### *Ишлатиладиган технология бўйича:*

- протокол ҳолатини назоратлаш (Stateful inspection);
- воситачилар модуллари асосида (proxy);

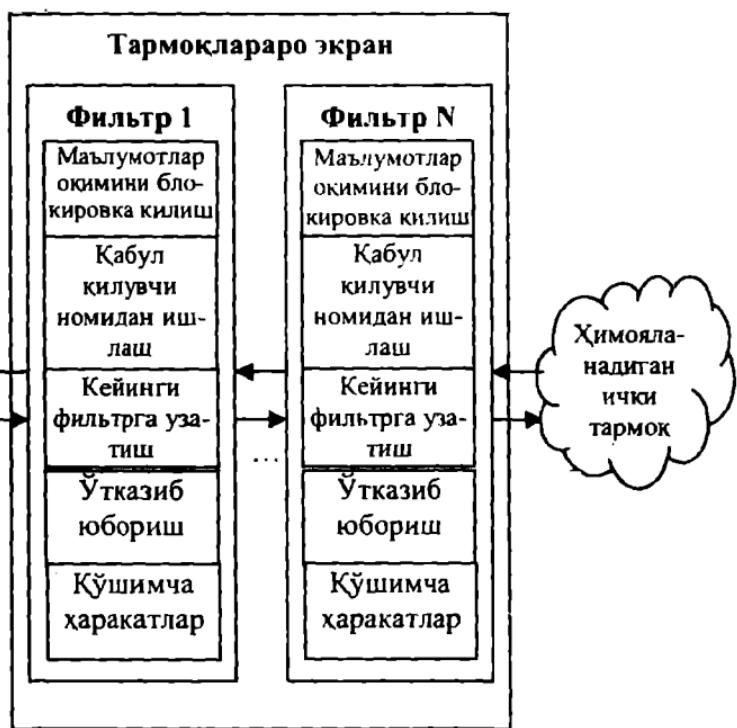
#### *Бажарилиши бўйича:*

- аппарат-дастурӣ;
- дастурӣ;

#### *Улании 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 фильтрлаш.** Ахборот оқимларини фильтрлаш уларни экран оркали, баъзида қандайдир ўзгартиришлар билан, ўтказишдан иборат. Фильтрлаш кабул килинган хавфсизлик сиёсатига мос келувчи, экранга олдиндан юкланган қоидалар асосида амалга оширилади. Шу сабабли тармоқлараро экранни ахборот оқимларини ишловчи фильтрлар кетма-кетлиги сифатида тасаввур этиш кулай (6.2-расм).



6.2-расм. Тармоқлараро экран тузилмаси.

Фильтрларнинг ҳар бири қуйидаги харакатларни бажариш оркали фильтрлашнинг алоҳида қоидаларини изохлашга аталган:

1. Ахборотни изохланувчи қоидалардаги берилган мезонлар бўйича тахлиллаш, масалан, кабул килувчи ва жўнатувчи манзиллари ёки ушбу ахборот аталган илова хили бўйича.

2. Изохланувчи қоидалар асосида қуйидаги ечимлардан бирини кабул килиш:

- маълумотларни ўтказмаслик;

- маълумотларни кабул килувчи номидан ишлаш ва натижани жўнатувчига қайтариш;
- тахлиллашни давом эттириш учун маълумотларни кейинги фильтрга узатиш;

—кейинги фильтрларга эътибор килмай маълумотларни узатиш.

Фильтрлаш коидалари воситачилик функцияларига оид кўшимча, масалан, маълумотларни ўзгартириш, ҳодисаларни кайдлаш ва х. каби харакатларни ҳам бериши мумкин. Мос ҳолда, фильтрлаш коидалари куйидагиларнинг амалга оширилишини таъминловчи шартлар рўйхатини аниклади:

- маълумотларни кейинги узатишга рухсат бериш ёки рухсат бермаслик;

— химоялашнинг кўшимча функцияларини бажариш.

Ахборот оқимини тахлиллаш мезони сифатида куйидаги параметрлардан фойдаланиш мумкин:

- таркибида тармоқ манзиллари, идентификаторлар, интерфейслар манзили, портлар раками ва бошка муҳим маълумотлар бўлган хабар пакетларининг хизматчи ҳошиялари;
- масалан, компьютер вируслари борлигига текширилувчи хабар пакетларининг бевосита таркиби;
- ахборот оқимининг ташки характеристикалари, масалан, вакт ва частота характеристикалари маълумотлар ҳажми ва х.

Ишлатилувчи тахлиллаш мезонлари фильтрлашни амалга оширувчи OSI моделининг сатҳларига боғлиқ. Умумий ҳолда, пакетни фильтрлашни 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 маҳсус дастурлар ёрдамида бажаради. Бу дастурлар резидент дастурлар хисобланади ва ташки ва ички тармоқ орасида хабарлар пакетини бевосита узатишни тақиқлади.

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 компьютерида ишловчи воситачи-дастур билан таъминланади.

терлари орасида ахборот алмашиш, хабарлар оқимини фильтрлашни ҳамда бошқа ҳимоялаш функцияларини бажарувчи дастурий воситачи орқали амалга оширилади.

Таъкидлаш лозимки, тармоклараро экран фильтрлаш функциясини воситачи-дастур иштирокисиз амалга ошириб, ташки ва ички тармок орасида ўзаро алоканинг шаффоғлигини таъминлаши мумкин. Шу билан бирга воситачи дастурлар хабарлар оқимини фильтрлашни амалга оширмаслиги ҳам мумкин.

Умуман, воситачи-дастурлар, хабарлар оқимини шаффоғ узатилишини блокировка килган ҳолда, қуидаги функцияларни бажариши мумкин:

- узатилувчи ва қабул қилинувчи маълумотларнинг ҳақиқийлигини текшириш;
- ички тармок ресурсларидан фойдаланишни чегаралаш;
- ташки тармок ресурсларидан фойдаланишни чегаралаш;
- ташки тармоқдан сўралувчи маълумотларни кэшлаш;
- хабарлар оқимини фильтрлаш ва ўзгартериш, масалан, вирусларни динамик тарзда кидириш ва ахборотни шаффоғ шифрлаш;
- фойдаланувчиларни идентификациялаш ва аутентификациялаш;
- ички тармок манзилларини трансляциялаш;
- ходисаларни кайдлаш, ходисаларга реакция кўрсатиш ҳамда кайдланган ахборотни таҳлиллаш ва хисоботларни генерациялаш.

*Узатилувчи ва қабул қилинувчи маълумотларнинг ҳақиқийлигини текшириш* нафакат электрон хабарларни, балки соҳталашибирлиши мумкин бўлган миграцияланувчи дастурларни (Java, Active X Controls) аутентификациялаш учун долзарб хисобланади. Хабар ва дастурларнинг ҳақиқийлигини текшириш уларнинг ракамли имзосини текширишдан иборатdir.

*Ички тармоқ ресурсларидан фойдаланишни чегаралаш* усууллари операцион тизим сатҳида мададланувчи чегаралаш усуулларидан фарқ килмайди.

*Ташки тармоқ ресурсларидан фойдаланишни чегарлаша*да кўпинча қуидаги ёндашишлардан бири ишлатилади:

- факат ташки тармоқдаги берилган манзил бўйича фойдаланишга рухсат бериш;

– янгиланувчи ножоиз манзиллар рўйхати бўйича сўровларни фильтрлаш ва ўринсиз калит сўзлари бўйича ахборот ресурсларини кидиришни блокировка қилиш:

– маъмур томонидан ташки тармоқнинг конуний ресурсларини брандмаузринг дискли хотирасида тўплаш ва янгилаш ва ташки тармоқдан фойдаланиши тўла такикалаш.

Ташки тармоқдан сўралувчи маълумотларни хэшлиш махсус воситачилар ёрдамида мададланади. Ички тармоқ фойдаланувчилари ташки тармоқ ресурсларидан фойдаланганларида барча ахборот, роҳу-сервер деб аталувчи брандмаузр қаттиқ диски маконида тўпланади. Шу сабабли, агар навбатдаги сўровда керакли ахборот роҳу-серверда бўлса, воситачи уни ташки тармоқка мурожаатсиз тақдим этади. Бу фойдаланиши жiddий тезлаштиради. Маъмурга факат роҳу-сервер таркибини вакти-вакти билан янгилаш туриш вазифаси колади.

Хэшлиш функцияси ташки тармоқ ресурсларидан фойдаланиши чегаралашда муваффакиятли ишлатилиши мумкин. Бу холда ташки тармоқнинг барча конуний ресурслари маъмур томонидан роҳу-серверда тўпланади ва янгиланади. Ички тармоқ фойдаланувчиларига факат роҳу-сервернинг ахборот ресурсларидан фойдаланишга рухсат берилади, ташки тармоқ ресурсларидан бевосита фойдаланиш эса ман килинади.

*Хабарлар оқимини фильтраш ва ўзгартириш* воситачи томонидан коидаларнинг берилган тўплами ёрдамида бажарилади. Бунда воситачи-дастурларнинг икки хили фарқланади:

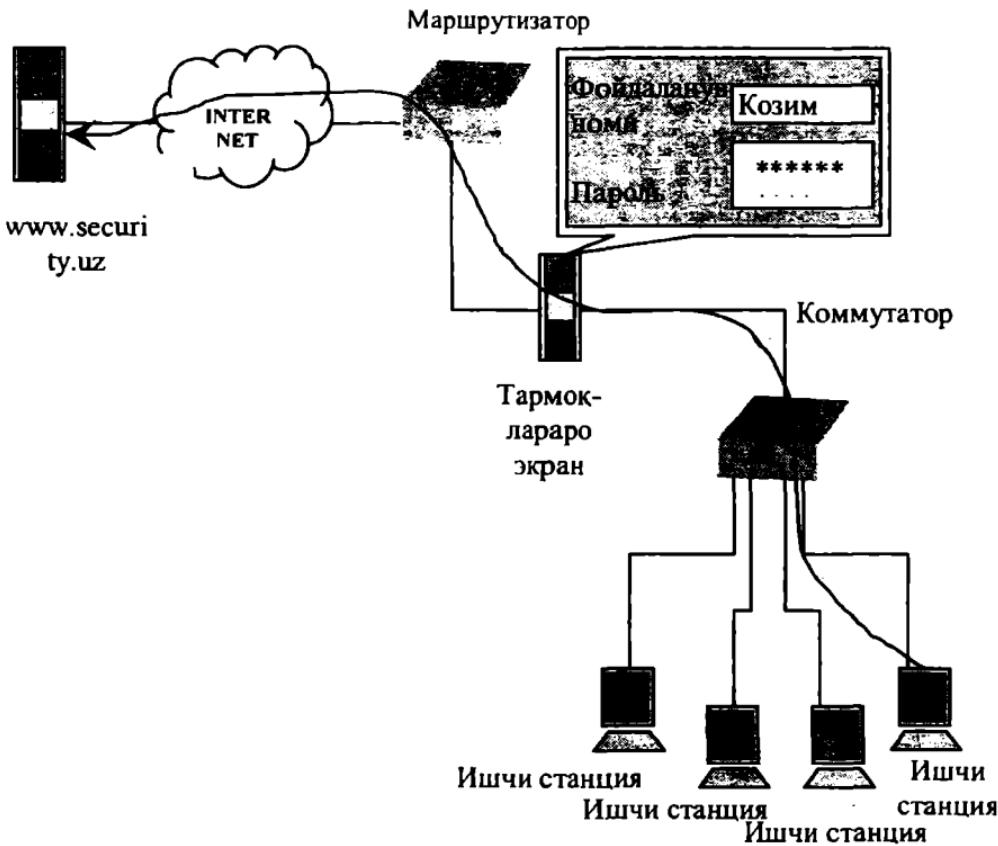
– сервис турини аниклаш учун хабарлар оқимини таҳлиллашга мўлжалланган экранловчи агентлар, масалан, FTP, HTTP, Telnet;

– барча хабарлар оқимини ишловчи универсал экранловчи агентлар, масалан, компьютер вирусларини кидириб заарсизлантиришга ёки маълумотларни шаффоф шифрлашга мўлжалланган агентлар.

Дастурий воситачи унга келувчи маълумотлар пакетини таҳлиллайди ва агар қандайдир обьект берилган мезонларга мос келмаса, воситачи унинг кейинги силжишини блокировка киласи ёки мос ўзгаришини, масалан, ошкор қилинган компьютер вирусларни заарсизлантиришни бажаради. Пакетлар таркибини

тахилиллашда экранловчи агентнинг ўтувчи файлли архивларни автоматик тарзда оча олиши мухим хисобланади.

**Фойдаланувчиларни идентификациялаш** ва аутентификациялаш баъзида оддий идентификаторни (исм) ва паролни тақдим этиш билан амалга оширилади (6.3-расм). Аммо бу схема хавфсизлик нуктаи назаридан заиф хисобланади, чунки паролни бегона шахс ушлаб колиб ишлатиши мумкин. Internet тармоғидаги кўпгина можаролар кисман анъанавий кўп марта ишлатилувчи паролларнинг заифлигидан келиб чиқкан.



6.3-расм. Пароль бўйича фойдаланувчини аутентификациялаш схемаси.

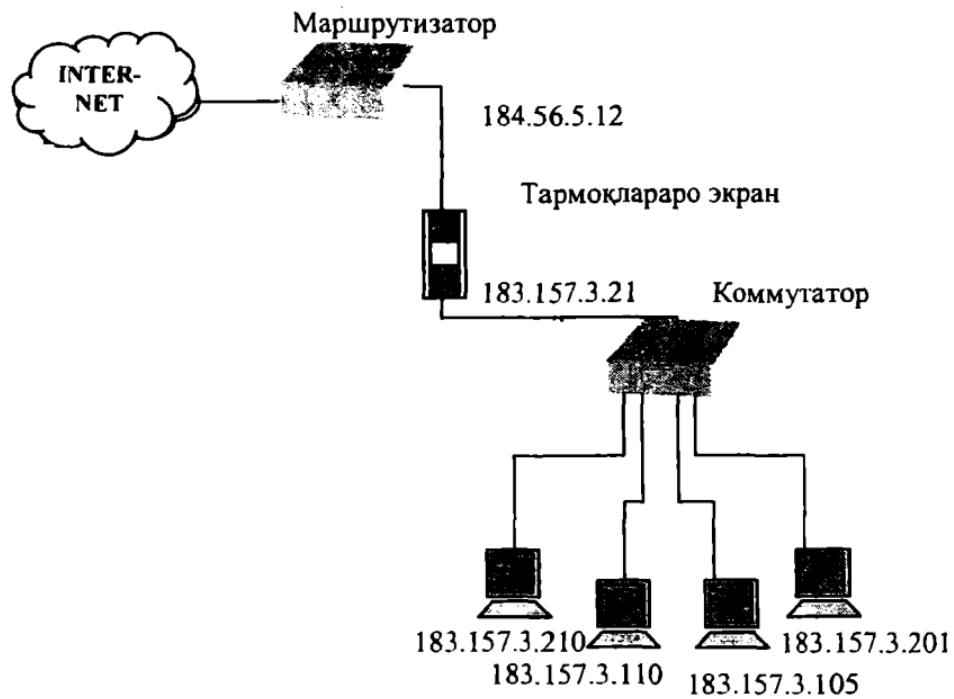
Аутентификациялашнинг ишончлирок усули – бир марта ишлатилувчи пароллардан фойдаланишдир. Бир марта паролларни генерациялашда аппарат ва дастурий воситалардан фойдаланилади. Аппарат воситалари компьютернинг слотига ўрнатилувчи қурилма бўлиб, уни ишга тушириш учун фойдаланувчи кандайдир маҳфий ахборотни билиши зарур. Масалан, смарт-карта ёки фойдаланувчи токени ахборотни генерациялади ва бу ахборотни хост анъанавий 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 таксимлаш маркази томонидан берилувчи ракамли сертификатларни ишлатиш ҳам қулай ва ишончли. Кўпгина воситачи дастурлар шундай ишлаб чикиладики, фойдаланувчи фактат тармоклараро экран билан ишлаш сеансининг бошида аутентификациялансин. Бундан кейин маъмур белгиланган вакт мобайнида ундан кўшимча аутентификацияланниш талаб этилмайди.

Тармоклараро экранлар тармокдан фойдаланишни бошқариши марказлаштиришлари мумкин. Демак, улар кучайтирилган аутентификациялаш дастурлари ва қурилмаларини ўрнатишга муносиб жой хисобланади. Гарчи кучайтирилган аутентификация воситалари ҳар бир хостда ишлатилиши мумкин бўлсада, уларнинг тармоклараро экранларда жойлаштириш қулай. Кучайтирилган аутентификациялаш чораларидан фойдаланувчи тармоклараро экранлар бўлмаса, Telnet ёки FTP каби иловаларнинг аутентификацияланмаган трафиги тармокнинг ички тизимларига тўғридан-тўғри ўтиши мумкин.

Катор тармоклараро экранлар аутентификациялашнинг кенг тарқалган усулларидан бири – Kerberosни мададлайди. Одатда, аксарият тижорат тармоклараро экранлар аутентификациялашнинг турли схемаларини мададлайди. Бу эса тармок хавфсизлиги маъмурига ўзининг шароитига караб энг мақбул схемани танлаш имконини беради.

*Ички тармоқ манзилларини трансляциялаш.* Күпгина 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 ташки 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 усулдинамик ва статик усулларда амалга оширилиши мумкин. Динамик усулда манзил узелга тармоқлараро экранга мурожаат онда ажратилади. Уланиш тугалланганидан сўнг манзил бўшайди ва уни кор-

поратив тармокнинг бошқа узели ишлатиши мумкин. Статик усулда узел манзили барча чикувчи пакетлар узатиладиган тармоклараро экраннинг битта манзилига доимо боғланади. Тармоклараро экраннинг IP- манзили ташки тармокка тушувчи ягона фаол IP- манзилга айланади. Натижада, ички тармокдан чикувчи барча пакетлар тармоклараро экрандан жўнатилган бўлади. Бу авторизацияланган ички тармок ва хавфли бўлиши мумкин бўлган ташки тармок орасида тўғридан-тўғри алокани истисно килади.

Бундай ёндашишда ички тармок топологияси ташки фойдаланувчилардан яширинган, демак, рухсатсиз фойдаланиш масаласи кийинлашади. Манзилларни трансляциялаш тармок ичидаги ташки тармок, масалан, Internetдаги манзиллаш билан келишилмаган манзиллашнинг хусусий тизимига эга бўлишига имкон беради. Бу ички тармокнинг манзил маконини кенгайтириш ва ташки манзил танқислиги муаммосини самарали ечади.

*Ходисаларни қайдлаш, ҳодисаларга реакция қўрсатиш ҳамда қайдланган ахборотни таълилаш ва ҳисоботларни генерациялаш тармоклараро экранларнинг мухим вазифалари хисобланади. Корпоратив тармокни химоялаш тизимининг жиҳдий элементи сифатида тармоклараро экран барча ҳаракатларни рўйхатга олиш имкониятига эга. Бундай ҳаракатларга нафакат тармок пакетларини ўтказиб юбориши ёки блокировка килиш, балки хавфсизлик маъмури томонидан фойдаланишни чегирилиши коидасини ўзгартириш ва х. ҳам тааллукли. Бундай рўйхатга олиш зарурият туғилганда (хавфсизлик можароси пайдо бўлганида ёки суд инстанцияларига ёки ички тергов учун далилларни йиғишда) яратилувчи журнallарга мурожаат этишга имкон беради.*

Шубҳали ходисалар (alarm) хусусидаги сигналтарни қайдлаш тизими тўғри созланганида тармоклараро экран ўзи ёки тармок хужумга дучор бўлганилиги ёки зондланганилиги тўғрисидаги багафсил ахборотни бериши мумкин. Тармокдан фойдаланиш ва унинг зондланганилигининг исботи статистикасини йиғиши катор сабабларга кўра мухимдир. Аввало. тармоклараро экраннинг зондланнишга ва хужумларга бардошлигини аниқ билиш зарур ва тармоклараро экранни химоялаш тадбирларининг адэқватлигини аниклаш лозим. Ундан ташқари, тармокдан фойдаланиш статистикаси гармок асбоб-ускуналарига ва дастурларига талабларни ифодалаш максадида хавф-хатарни тадқиқлаш ва таҳлиллашда дастлабки маълумотлар сифатида мухим хисобланади.

Кўпгина тармоклараро экранлар статистикани қайдловчи, йигувчи ва таҳлилловчи кувватли тизимга эга. Мижоз ва сервер

манзили, фойдаланувчилар идентификатори, сеанс вактлари, уланиш вактлари, узатилган ва кабул килинган маълумотлар сони, маъмур ва фойдаланувчилар харакатлари бўйича хисоб олиб борилиши мумкин. Хисоб тизимлари статистикани таҳлиллашга имкон беради ва маъмурларга батафсил хисоботларни тақдим этади. Тармок-лараро экранлар махсус протоколлардан фойдаланиб, маълум ходисалар тўғрисида реал вакт режимида масоғдан хабар бериши бажариши мумкин.

Рұксатсиз харакатларни килишга уринишларни аникланнишинга бўладиган мажбурий реакция сифатида маъмурнинг хабари, яъни огохлантирувчи сигналларни бериш белгиланиши лозим. Ҳужум килинганлиги аникланганда огохлантирувчи сигналларни юборишига кодир бўлмаган тармоклараро экранни тармоклараро химоянинг самарали воситаси деб бўлмайди.

## 6.2. Тармоклараро экранларнинг асосий компонентлари

Тармоклараро экранлар тармоклараро алоқа хавфсизлигини OSI моделининг турли сатҳларида мададлайди. Бунда этalon модельнинг турли сатҳларида бажариладиган химоя функциялари бирбиридан жиддий фарқланади. Шу сабабли, тармоклараро экранлар комплексини, ҳар бири OSI моделининг алоҳида сатҳига мўлжалланган, бўлинмайдиган экранлар мажмуи кўринишида тасаввур этиш мумкин.

Экранлар комплекси кўпинча этalon модельнинг тармок, сеанс, татбикӣ сатҳларида ишлайди. Мос ҳолда, куйидаги бўлинмайдиган брандмауэрлар фарқланади (6.5-расм).

- экранловчи маршрутизатор;
- сеанс сатҳи шлюзи (экранловчи транспорт);
- татбикӣ сатҳи шлюзи (Экранловчи шлюз).

Тармокларда ишлатиладиган протоколлар (TCP/IP, SPX/IPX) OSI этalon моделига батамом мос келмайди, шу сабабли санаб ўтилган экранлар хили функцияларини амалга оширишда этalon модельнинг кўшни сатҳларини ҳам камраб олишлари мумкин. Масалан, татбикӣ экран хабарларнинг гашқи тармоқка узатилишида уларни автоматик тарзда шифрлашни ҳамда кабул килинүвчи криптографик беркитиган маълумотларни автоматик тарзда расшифровка килишни амалга ошириши мумкин. Бу ҳолда бундай экран OSI моделининг нафакат татбикӣ сатҳида, балки тақдимий сатҳида ҳам ишлайди.



6.5-рас.и. OSI моделининг алоҳида сатҳларида ишлайдиган тармоклараро экранлар тури.

Сеанс сатхи шлюзи ишлашида OSI моделининг транспорт ва тармок сатхларини камраб олади. Экранловчи маршрутизатор хабарлар пакетини таҳлиллашда уларнинг нафакат тармок, балки транспорт сатхи сарлавҳаларини ҳам текширади.

Юкорида келтирилган тармоклараро экранларнинг хиллари ўзининг афзалликлари ва камчиликларига эга. Ишлатиладиган брандмаузларнинг кўпчилиги ёки татбиқий шлюзлар ёки экранловчи маршрутизаторлар бўлиб, тармоклараро алоканинг тўлик хавфсизлигини таъминламайди. Ишончли химояни эса факат ҳар бири экранловчи маршрутизатор, сеанс сатхи шлюзи ҳамда татбиқий шлюзни бирлаштирувчи тармоклараро экранларнинг комплекси таъминлайди.

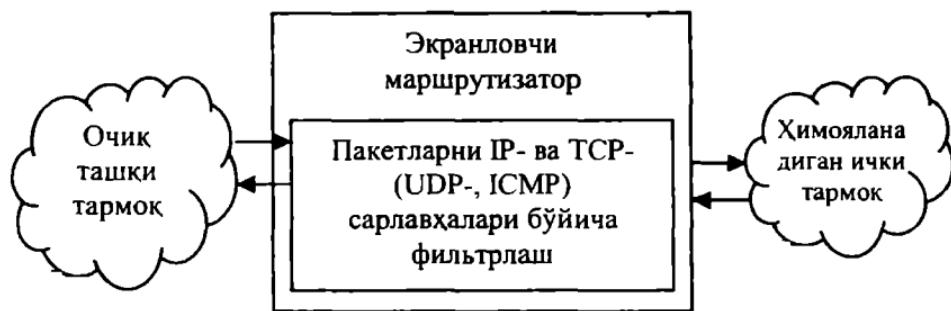
*Экранловчи маршрутизатор* (screening router) (пакетли фильтр packet filter деб ҳам аталади) хабарлар пакетини фильтрлашга аталган ва ички ва ташки тармоклар орасида шаффоф алокани таъминлайди. У OSI моделининг тармок сатхидаги ишлайдиган алоҳида тармоклараро экранларнинг транспорт сатхини ҳам камраб олиши мумкин.

Маълумотларни ўтказиш ёки яроксиз ҳолга чиқариш хусусидаги карор фильтрлашнинг берилган коидаларига биноан ҳар бир пакет учун мустакил қабул килинади. Карор қабул килишда гармок 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 раками;
- қабул килувчи порт раками.



6.6-расм. Пакетли фильтрни ишлаш схемаси.

Биринчи тўртга параметр пакетнинг IP-сарлавҳасига, кейингилари эса TCP-ёки UDP сарлавҳасига тааллукли. Жўнатувчи ва қабул килувчи манзиллари IP-манзиллар хисобланади. Бу манзиллар пакетларни шакллантиришда тўлдирилади ва уни тармок бўйича узатганда ўзгармайди.

Пакет хили хошиясида тармок сатхига мос келувчи ICMP протокол коди ёки таҳлилланувчи IP-пакет тааллукли бўлган транспорт сатхи протоколининг (TCP ёки UDP) коди бўлади.

Пакетни фрагментлаш байроғи IP-пакетлар фрагментлашининг борлиги ёки йўклигини аниклади. Агар таҳлилланувчи пакет учун фрагментлаш байроғи ўрнатилган бўлса, мазкур пакет фрагментланган IP-пакетнинг кисм пакети хисобланади.

Манба ва қабул килувчи портлари ракамлари TCP ёки UDP драйвер томонидан ҳар бир жўнатилувчи хабар пакетларига кўшилади ва жўнатувчи иловасини ҳамда ушбу пакет аталган ило-

вани бир маънода идентифиқациялайди. Портлар номерлари бўйича фильтрлаш имконияти учун юкори сатҳ протоколларига порт ракамларини ажратиш бўйича тармоқда кабул қилинган келишувни билиш лозим.

Ҳар бир пакет ишланишида экранловчи маршрутизатор берилган коидалар жадвалини, пакетнинг тўлик ассоциациясига мос келувчи коидани топгучи, кетма-кет кўриб чиқади. Бу ерда ассоциация деганда берилган пакет сарлавҳаларида кўрсатилган параметрлар мажмуми тушунилади. Агар экранловчи маршрутизатор жадвалдаги коидаларнинг бирортасига ҳам мос келмайдиган пакетни олса, у, хавфсизлик нуктаи назаридан, уни яроксиз ҳолга келтирилади.

Пакетли фильтрлар аппарат ва дастурий амалга оширилиши мумкин. Пакетли фильтр сифатида оддий маршрутизатор ҳамда кирувчи ва чикувчи пакетларни фильтрлашга мослаштирилган, серверда ишловчи дастурдан фойдаланиш мумкин. Замонавий маршрутизаторлар ҳар бир порт билан бир неча ўнлаб коидаларни боғлаши ва киришда, ҳам чиқишида пакетларни фильтрлаши мумкин.

Пакетли фильтрларнинг камчилиги сифатида кўйидагиларни кўрсатиш мумкин. Улар хавфсизликнинг юкори даражасини таъминламайди, чунки факат пакет сарлавҳаларини текширадилар ва қўлгина керакли функцияларни мададламайди. Бу функцияларга, масалан, охирги узелларни аутентификациялаш, хабарлар пакетларини криптографик беркитиш ҳамда уларнинг яхлитлигини ва ҳакиқийлигини текшириш киради. Пакетли фильтрлар дастлабки манзилларни алмаштириб қўйиш ва хабарлар пакети таркибини рухсатсиз ўзгартириш каби кенг таркалган тармок хужумларига заиф ҳисобланадилар. Бу хил бранд-мауэрларни «алдаш» кийин эмас –фильтрлашга рухсат берувчи коидаларни кондирувчи пакет сарлавҳаларини шакллантириш кифоя.

Аммо, пакетли фильтрларнинг амалга оширилишининг соддалиги, юкори унумдорлиги, дастурий иловалар учун шаффоғлиги ва нархининг пастлиги, уларнинг ҳамма ерда тарқалишига ва тармок хавфсизлиги тизимининг мажбурий элементи каби ишлатилишига имкон яратди.

*Сеанс сатҳи шлюзи, (экранловчи транспорт деб ҳам юритилади) виртуал уланишларни назоратлашга ва ташки гармок билан ўзаро алоқа килишда IP-манзилларни трансляциялашга аталган. У*

OSI моделининг сеанс сатҳида ишлайди ва ишлаш жараёнида эталон моделнинг транспорт ва тармок сатҳларини ҳам қамраб олади. Сеанс сатҳи шлюзининг химоялаш функциялари воситачилик функцияларига тааллукли.

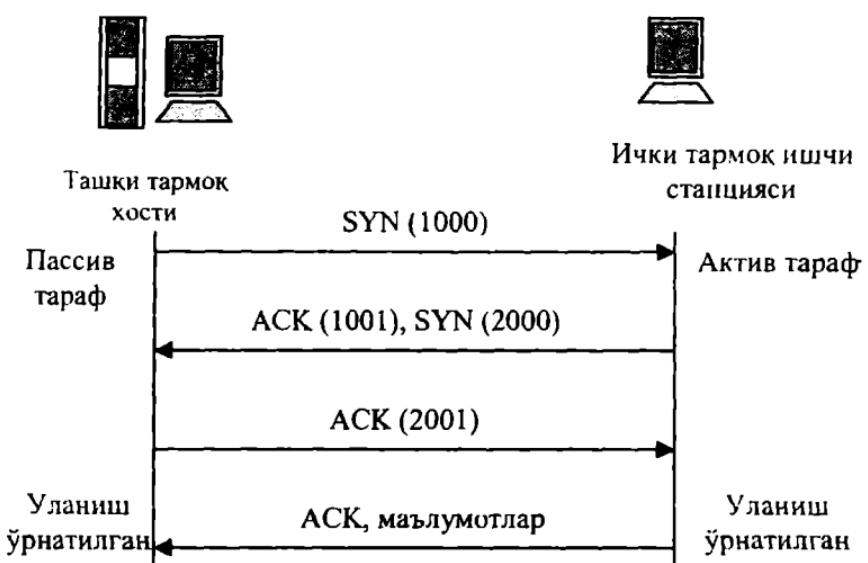
Виртуал уланишларнинг назорати алокани квитирлашни кузатишдан ҳамда ўрнатилган виртуал каналлар бўйича ахборот узатилишининг назоратлашдан иборат. Алокани квитирлашнинг назоратида сеанс сатҳида шлюз ички тармок ишчи станцияси ва ташки тармок компьютери орасида виртуал уланишни кузатиб, сўралаётган алока сеансининг жоизлигини аниклади.

Бундай назорат TCP протоколининг сеанс сатҳи пакетларининг сарлавҳасидаги ахборотга асосланади. Аммо TCP-сарлавҳаларни таҳлиллашда пакетли фильтр факт манба ва қабул килувчи портларининг ракамини текширса, экранловчи транспорт алокани квиртираш жараёнига тааллукли бошка ҳошияларни таҳлиллайди.

Алока сеансига сўровнинг жоизлигини аниклаш учун сеанс сатҳи шлюзи қуидаги харакатларни бажаради. Ишчи станция (мижоз) ташки тармок билан боғланишни сўраганида, шлюз бу сўровни қабул қилиб унинг фильтрлашнинг базавий мезонларини каноатлантиришини, масалан, сервер мижоз ва у билан ассоциацияланган исмнинг IP-манзилини аниклай олишини текширади. Сўнгра шлюз, мижоз исмидан харакат қилиб, ташки тармок компьютери билан уланишни ўрнатади ва TCP протоколи бўйича квиртираш жараёнининг бажарилишини кузатади.

Бу муолажа SYN (синхронлаш) ва ACK (тасдиқлаш) байроклари оркали белгиланувчи TCP-пакетларни алмашишдан иборат (6.7-расм).

SYN байрок билан белгиланган ва таркибида ихтиёрий сон, масалан, 1000, бўлган TCP сеансининг биринчи пакети мижознинг сеанс очишига сўрови хисобланади. Бу пакетни олган ташки тармок компьютери жавоб тарикасида ACK байрок билан белгиланган ва таркибида олинган пакетдагидан биттага катта (бизнинг ҳолда 1001) сон бўлган пакетни жўнатади. Шу тарика, мижоздан SYN пакети олинганлиги тасдиқланади. Сўнгра, тескари муолажа амалга оширилади: ташки тармок компьютери ҳам мижозга узатилувчи маълумотлар биринчи байтининг тартиб раками билан (масалан, 2000) SYN пакетини жўнатади, мижоз эса уни олганлигини, таркибида 2001 сони бўлган пакетни узатиш оркали тасдиқлади. Шу билан алокани квиртираш жараёни тугалланади.



6.7-расм. TCP протоколи бўйича алоқани квиртираш схемаси.

Сеанс сатҳи шлюзи (6.8-расм) учун сўралган сеанс жоиз ҳисобланади, качонки алоқани квиртираш жараёни бажарилишида SYN ва ACK байроқлар ҳамда TCP-пакетлари сарлавҳаларидағи сонлар ўзаро мантикий боғланган бўлса.



6.8-расм. Сеанс сатҳи шлюзи ишлаш схемаси.

Ички гармоқнинг ички станцияси ва гашки гармоқнинг компьютери TCP сеансининг авторизацияланган қатнашчилари эканлиги ҳамда ушбу сеанснинг жоизлиги тасдиқланганидан сўнг шлюз

уланишни ўрнатади. Бунда шлюз уланишларининг махсус жадвалига мос ахборотни (жўнатувчи ва кабул килувчи манзиллари, уланиш ҳолати, кетма-кетлик рақами хусусидаги ахборот ва х.) киритади.

Шу ондан бошлаб шлюз пакетларни нусхалайди ва иккала томонга йўналтириб, ўрнатилган виртуал канал бўйича ахборот узатилишини назорат килади. Ушбу назорат жараёнида сеанс сатхи шлюзи пакетларни фильтрламайди. Аммо у узатилувчи ахборот сонини назорат килиши ва қандайдир чегарадан ошганида уланишни узиши мумкин. Бу эса, ўз навбатида, ахборотнинг рухсатсиз экспорт килинишига тўсик бўлади. Виртуал уланишлар хусусидаги кайдлаш ахборотининг тўпланиши хам мумкин.

Сеанс сатхи шлюзларида виртуал уланишларни назоратлашда канал *воситачилари* (pipe proxy) деб юритилувчи махсус дастурлардан фойдаланилади. Бу воситачилар ички ва ташки тармоклар 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 татбикӣ сатҳ шлюзлари имкониятларини кенгайтиришда сеанс сатҳ шлюзларидан фойдаланиш мумкин.

Сеанс сатхи шлюзи ташки тармок билан ўзаро алокада тармок сатхи ички манзилларини (IP-манзилларини) трансляциялашни хам таъминлайди. Ички манзилларни трансляциялаш ички тармокдан ташки тармокка жўнатилувчи барча пакетларга нисбатан бажарилади.

Амалга оширилиши нуктаи назаридан сеанс сатхи шлюзи етарлича оддий ва нисбатан ишончли дастур хисобланади. У экранловчи маршрутизаторни виртуал уланишларни назоратлаш ва ички IP-манзилларни трансляциялаш функциялари билан тўлдиради.

Сеанс сатхи шлюзининг камчиликлари – экранловчи маршрутизаторларнинг камчиликларига ўхшаш. Ушбу технологиянинг яна бир жиддий камчилиги маълумотлар ҳошиялари таркибини назоратлаш мумкин эмаслиги. Натижада, нияти бузук одамларга зарар келтирувчи дастурларни химояланувчи тармокка узатиш имконияти туғилади. Ундан ташки, TCP-сессиясининг (TCP hijacking)

ушлаб колинишида нияти бузук одам хужумларини хатто рухсат берилган сессия доирасида амалга ошириши мумкин.

Амалда аксарият сеанс сатҳ шлюзлари мустакил маҳсулот бўймай, татбиқий сатҳ шлюзлари билан комплектда тақдим этилади.

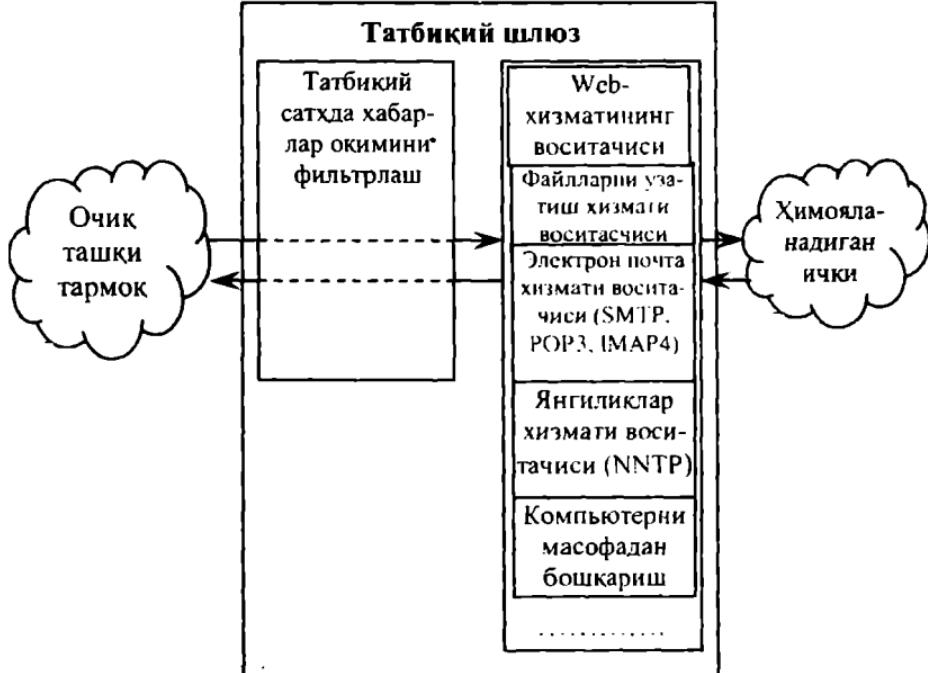
*Татбиқий сатҳ шлюзи* (экранловчи шлюз деб ҳам юритилади) OSI моделининг татбиқий сатҳида ишлаб, тақдими сатҳни ҳам камраб олади ва тармоқлараро алоканинг энг ишончли химоясини таъминлайди. Татбиқий сатҳ шлюзининг химоялаш функциялари, сеанс сатҳи шлюзига ўхшаб, воситачилик функцияларига тааллукли. Аммо, 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 ҳакиқийлигини текшириш;
- ички ва ташки тармок ресурсларидан фойдаланишни чегаралаш;
- ахборотлар оқимини фильтрлаш ва ўзгартириш, масалан, вирусларни динамик тарзда кидириш ва ахборотни шаффоғ шифрлаш;
- ходисаларни қайдлаш, ходисаларга реакция кўрсатиш ҳамда қайдланган ахборотни таҳлиллаш ва хисоботларни генерациялаш;
- ташки тармоқдан сўралувчи маълумотларни кэшлаш.

Татбиқий сатҳ шлюзи функциялари воситачилик функцияларига тааллукли бўлганлиги сабабли, бу шлюз универсал компьютер хисобланади 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 тааллукли хабарларни ишлашга ва химоялаш функцияларини бажаришга мўлжалланган.

Татбиқий сатҳ шлюзи мос экранловчи агентлар ёрдамида кирувчи ва чикувчи пакетларни ушлаб колади, ахборотни пусха тайди ва кайта жўнатади, яъни ички ва ташки тармоқлар орасидаги тўғридан-тўғри уланишни истисно қилган ҳолда, сервер-воситачи функциясини бажаради (6.9-расм).

## Татбиқий шлюз



6.9-расм. Татбиқий шлюз ишлаш схемаси.

Татбиқий сатҳ шлюзи ишлатадиган воситачилар сеанс сатҳи шлюзларининг канал воситачиларидан жиддий фарқланади. Биринчидан, татбиқий сатҳ шлюзлари муайян иловалар (дастурий серверлар) билан боғланган, иккинчидан улар OSI моделининг татбиқий сатҳида хабарлар оқимини фильтрлашлари мумкин.

Татбиқий сатҳ шлюзлари воситачи сифатида мана шу мақсадлар учун маҳсус ишлаб чиқилган TCP/IPнинг муайян хизматларининг дастурий серверлари – HTTP, FTP, SMTP, NNTP ва х. – серверларидан фойдаланади. Бу дастурий серверлар брандмаузрларда резидент режимида ишлайди ва TCP/IPнинг мос хизматларига тааллукли химоялаш функцияларини амалга оширади. UDP трафигига UDP-пакетлар таркибининг маҳсус транслятори хизмат кўрсатади.

Ички тармок ишчи сервери ва ташки тармок компьютери орасида иккита уланиш амалга оширилади: ишчи станциядан брандмаузргача ва брандмаузрдан белгиланган жойгача. Канал воситачиларидан фаркли ҳолда, татбиқий сатҳ шлюзининг воситачилари факат ўзлари хизмат килувчи иловалар генерациялаган пакетларни

ўтказади. Масалан, НТТР хизматининг воситачи-дастури фактат шу хизмат генерациялаган трафикни ишлайди.

Агар кандайдир иловада ўзининг воситачиси бўлмаса, татбикӣ сатҳдаги шлюз бундай иловани ишлай олмайди ва у блокировка қилинади. Масалан, агар татбикӣ сатҳдаги шлюз фактат НТТР, FTP ва Telnet воситачи-дастурларидан фойдаланса, у фактат шу хизматларга тегишли пакетларни ишлайди ва колган хизматларнинг пакетларини блокировка килади.

Татбикӣ сатҳ шлюзи воситачилари. канал воситачиларидан фарқли ҳолда, ишланувчи маълумотлар таркибини текширишни тъминлайди. Улар ўзлари хизмат кўрсатадиган татбикӣ сатҳ протоколларидаги командаларнинг алоҳида хилларини ва хабарлардаги ахборотларни фильтрлашлари мумкин.

Татбикӣ сатҳ шлюзини созлашда ва хабарларни фильтрлаш коидаларини тавсифлашда куйидаги параметрлардан фойдаланилади: сервис номи, ундан фойдаланишнинг жоиз вакт оралиғи, ушбу сервисга боғлиқ хабар таркибига чегаралашлар, сервис ишлатадиган компьютерлар, фойдаланувчи идентификатори, аутентификациялаш схемалари ва х.

Татбикӣ сатҳ шлюзи куйидаги афзалликларга эга:

- аксарият воситачилик функцияларини бажара олиши туфайли локал тармок химоясининг юкори даражасини тъминлайди;

- иловалар сатҳида химоялаш кўпгина қўшимча текширишларни амалга оширишга имкон беради, натижада, дастурий тъминот камчиликларига асосланган муваффакиятли хужумлар ўтказиш эҳтимоллиги камаяди;

- татбикӣ сатҳ шлюзининг ишга лаёкатлиги бузилса, бўлинувчи тармоқлар орасида пакетларнинг тўппа-тўғри ўтиши блокировка қилинади, натижада, ради килиниши туфайли химояланувчи тармоқнинг хавфсизлиги пасаймайди.

Татбикӣ сатҳ шлюзининг камчиликларига куйидагилар киради:

- нархининг нисбатан юкорилиги;
- брандмауэрнинг ўзи ҳамда уни ўрнатиш ва конфигурациялаш муолажаси етарлича мураккаб;
- компьютер платформаси унумдорлигига ва ресурслари ҳажмига қўйиладиган талабларнинг юкорилиги;

- фойдаланувчилар учун шаффофликнинг йўклиги ва тармоклараро алока ўрнатилишида ўтказиш кобилиятигининг сусайиши.

Охирги камчиликка батафсил тўхталамиз. Воситачилар сервер ва мижоз орасида пакетлар узатилишида оралиқ ролини бажаради. Аввал воситачи билан уланиш ўрнатилади, сўнгра воситачи манзилат билан уланишни яратиш ёки яратмаслик хусусида карор қабул қиласди. Мос холда татбикий сатҳ шлюзи ишлаши жараёнида ҳар қандай рухсат этилган уланишни кайталайди. Натижада, фойдаланувчилар учун шаффофлик йўколади ва уланишга хизмат килишга кўшимча харажат сарфланади.

*Эксперт сатҳи шлюзи.* Татбикий сатҳ шлюзининг фойдаланувчилар учун шаффофлигининг йўклиги ва тармоклараро алока ўрнатилишида ўтказиш кобилиятигининг сусайиши каби жиддий камчиликларини бартараф этиш максадида пакетларни фильтрлашнинг янги технологияси ишлаб чикилган. Бу технологияни баъзида уланиш ҳолатини назоратлашили фильтрлаш (stateful inspection) ёки эксперт сатҳидаги фильтрлаш деб юритишиди. Бундай фильтрлаш пакетлар ҳолатини кўп сатҳли тахлиллашнинг маҳсус усуслари (SMLT) асосида амалга оширилади.

Ушбу гибрид технология тармок сатҳида пакетларни ушлаб колиш ва ундан уланишни назорат килишда ишлатилувчи татбикий сатҳ ахборотини чикариб олиш оркали уланиш ҳолатини кузатишга имкон беради.

Ишлаши асосини ушбу технология ташкил этувчи тармоклараро экран эксперт сатҳ брандмауэри деб юритишиди. Бундай брандмауэрлар ўзида экранловчи маршрутизаторлар ва татбикий сатҳ шлюзлари элементларини уйгунлаштиради. Улар ҳар бир пакет таркибини берилган хавфсизлик сиёсатига мувофик баҳолайдилар.

Шундай килиб эксперт сатҳидаги брандмауэрлар куйидагиларни назоратлашга имкон беради:

- мавжуд коидалар жадвали асосида ҳар бир узатилувчи пакетни;

- ҳолатлар жадвали асосида ҳар бир сессияни;

- ишлаб чикилган воситачилар асосида ҳар бир иловани.

Эксперт сатҳ тармоклараро экранларининг афзалликлари сифатида уларнинг фойдаланувчилар учун шаффофлигини, ахборот

окимиини ишлашининг юкори тезкорлигини ҳамда улар орқали ўтувчи пакетларнинг IP-манзилларини ўзгартирмаслигини кўрсатиш мумкин. Охирги афазаллик. IP-манзилдан фойдаланувчи татбиқий сатхнинг ҳар қандай протоколининг бундай брандмауэрлардан хеч қандай ўзгаришсиз ёки маҳсус дастурлашсиз бирга ишлай олишини англаади.

Бундай брандмауэрларнинг авторизацияланган мижоз ва ташқи тармок компьютери орасида тўғридан-тўғри уланишга йўл кўйиши, химоянинг унчалик юкори бўлмаган даражасини таъминлайди. Шу сабабли амалда эксперт сатхини фильтрлаш технологиясидан комплекс брандмауэрлар ишлаши самарадорлигини оширишда фойдаланилади. Эксперт сатхнинг фильтрлаш технологиясини ишлатувчи комплекс брандмауэрларга мисол тарикасида Fire Wall-1 ва ON Guard ларни кўрсатиш мумкин.

### **6.3. Тармоқлараро экранлар асосидаги тармоқ ҳимоясининг схемалари**

Тармоқлараро алоқани самарали химоялаш учун брандмауэр тизими тўғри ўрнатилиши ва конфигурацияланиши лозим. Ушбу жараён куйидагиларни ўз ичига олади:

- тармоқлараро алоқа сиёсатини шакллантириш;
- брандмауэрни улаш схемасини танлаш ва параметрларини созлаш.

#### ***Тармоқлараро алоқа сиёсатини шакллантириши***

Тармоқлараро алоқа сиёсатини шакллантиришда куйидагиларни аниқлаш лозим:

- тармоқ сервисларидан фойдаланиш сиёсати;
- тармоқлараро экран ишлаши сиёсати.

*Тармоқ сервисларидан фойдаланиш сиёсати* химояланувчи компьютер тармоқнинг барча сервисларини тақдим этиш ҳамда улардан фойдаланиш коидаларини белгилайди. Ушбу сиёсат доирасида тармоқ экрани орқали тақдим этилувчи барча сервислар ва ҳар бир сервис учун мижозларнинг жоиз манзиллари берилиши лозим. Ундан ташкари, фойдаланувчилар учун қачон ва қайси фойдаланувчилар кайси сервисдан ва қайси компьютерда фойдаланишларини тавсифловчи коидалар кўрсатилиши лозим. Фойдаланиш усуулларига чегаралашлар ҳам берилади. Бу чегаралашлар фойдаланувчиларнинг Internet нинг ман этилган сервисларидан айланма йўл

оркали фойдаланишларига йўл қўймаслик учун зарур. Фойдаланувчилар ва компьютерларни аутентификациялаш коидалари хамда ташкилот локал тармоғи ташкарисидаги фойдаланувчиларнинг ишлаш шароитлари алоҳида белгиланиши лозим.

Тармоқлараро экран ишлаши сиёсатида тармоқлараро алокани бошқаришнинг брандмауэр ишлаши асосидаги базавий принципи берилади. Бундай принципларнинг қуидаги иккитасидан бири танланиши мумкин:

- ошкора рухсат этилмагани ман килинган;
- ошкора ман этилмаганига рухсат берилган.

«Ошкора рухсат этилмагани ман килинган» принципи танланганида тармоқлараро экран шундай созланадики, ҳар қандай рухсат этилмаган тармоқлараро алоқалар блокировка килинади. Ушбу принцип ахборот хавфсизлигининг барча соҳаларида ишлатилувчи фойдаланишнинг мумтоз моделига мос келади. Бундай ёндашиш, имтиёзларни минималлаштириш принципини адекват амалга оширишга имкон бериши сабабли, хавфсизлик нуктаи назаридан яхширок хисобланади. Моҳияти бўйича «ошкора рухсат этилмагани ман килинган» принципи билмаслик зарар келтириши фактини эътироф этишдир. Таъкидлаш лозимки, ушбу принципга асосан таърифланган фойдаланиш коидалари фойдаланувчиларга маълум нокулайликлар туғдириши мумкин.

«Ошкора ман этилмаганига рухсат берилган» принципи танланганида тармоқлараро экран шундай созланадики, факат ошкора ман этилган тармоқлараро алоқалар блокировка килинади. Бу ҳолда, фойдаланувчилар томонидан тармоқ сервисларидан фойдаланиш кулиялиги ошади, аммо тармоқлараро алоқа хавфсизлиги пасаяди. Фойдаланувчиларнинг тармоқлараро экранни четлаб ўтишларига имкон туғилади, масалан улар сиёсат ман қилмаган (хатто, сиёсатда кўрсатилмаган) янги сервисларидан фойдаланишлари мумкин. Ушбу принцип амалга оширилишида ички тармоқ хакерларнинг ҳужумларидан камрок химояланган бўлади. Шу сабабли, тармоқлараро экранларни ишлаб чиқарувчи-лари одатда, ушбу принципдан фойдаланмайдилар.

Тармоқлараро экран симметрик эмас. Унга ички тармоқнинг ташки тармоқдан ва аксинча фойдаланишни чегараловчи коидалар алоҳида берилади. Умумий ҳолда, тармоқлараро экраннинг иши қуидаги иккита гурӯх функцияларни динамик тарзда бажаришга асосланган:

- у орқали ўтаётган ахборот оқимини фильтрлаш;
- тармоклараро алока амалга оширилишида воситачилик.

Оддий тармоклараро экранлар бу функцияларнинг бирини бажаришга мўлжалланган. Комплекс тармоклараро экранлар химоялашнинг кўрсатилган функцияларининг биргаликда бажарилишини таъминлади.

### *Тармоклараро экранларни улашнинг асосий схемалари.*

Корпоратив тармокни глобал тармокларга улаганда химояланувчи тармокнинг глобал тармокдан ва глобал тармокнинг химояланувчи тармоқдан фойдаланишини чегаралаш ҳамда уланувчи тармоқдан глобал тармокнинг масофадан рухсатсиз фойдаланишидан химоялашни таъминлаш лозим. Бунда ташкилот ўзининг тармоғи ва унинг компонентлари хусусидаги ахборотни глобал тармок фойдаланувчиларидан беркитишга манфаатдор. Масофадаги фойдаланувчилар билан ишлаш химояланувчи тармок ресурсларидан фойдаланишнинг катъий чегараланишини талаб этади.

Ташкилотдаги корпоратив тармок таркибида кўпинча химояланышнинг турли сатҳли бир неча сегментларга эга бўлиши эктиёжи туғилади:

- бемалол фойдаланиувчи сегментлар (масалан, реклама WWW-серверлари);
- фойдаланиш чегараланган сегментлар (масалан, ташкилотнинг масофадаги узеллари ходимларининг фойдаланиши учун);
- ёпик сегментлар (масалан, ташкилотнинг молия локал кисм тармоғи).

Тармоклараро экранларни улашда турли схемалардан фойдаланиш мумкин. Бу схемалар химояланувчи тармок ишлаши шароитига ҳамда ишлатиладиган брандмаузларнинг тармок интерфейслари сонига ва бошқа характеристикаларига боғлик. Тармоклараро экранни улашнинг куйидаги схемалари кенг тарқалган:

- экранловчи маршрутизатордан фойдаланилган химоя схемалари;
- локал тармокни умумий химоялаш схемалари;
- химояланувчи ёпик ва химояланмайдиган очик кисм тармоқли схемалар;
- ёпик ва очик кисм тармокларни алоҳида химояловчи схемалар.

Экранловчи маршрутизатордан фойдаланилган ҳимоя схемаси.

Пакетларни фильтрлашга асосланган тармоқлараро экран кенг таркалган ва амалга оширилиши осон. У ҳимояланувчи тармок ва бўлиши мумкин бўлган ганим очик тармок орасида жойлашган экранловчи маршрутизатордан иборат (6.10-расм).



6.10-расм. Тармоқлараро экран – экранловчи маршрутизатор.

Экранловчи маршрутизатор (пакетли фильтр) кирувчи ва чиқувчи пакетларни уларнинг манзиллари ва портлари асосида блокировка қилиш ва фильтрлаш учун конфигурацияланган.

Ҳимояланувчи тармоқдаги компьютерлар Internetдан тўғридан-тўғри фойдаланаолади, Internetнинг улардан фойдаланишининг кўп кисми эса блокировка килинади. Умуман, экранловчи маршрутизатор юкорида тавсифланган ҳимоялаш сиёсатидан исталганини амалга ошириши мумкин. Аммо, агар маршрутизатор пакетларни манба порти ва кириш йўли ва чикиш йўли портлари рақами бўйича фильтрламаса, «ошкора рухсат этилмагани ман килинган» сиёсатини амалга ошириш кийинлашади.

Пакетларни фильтрлашга асосланган тармоқлараро экраннинг камчиликлари кўйидагилар:

– фильтрлаш коидаларининг мураккаблиги; баъзи холларда бу коидалар мажмую бажарилмаслиги мумкин;

– фильтрлаш коидаларини тўлик тестлаш мумкин эмаслиги; бу тармоқни тестланмаган хужумлардан ҳимояланмаслигига олиб келади;

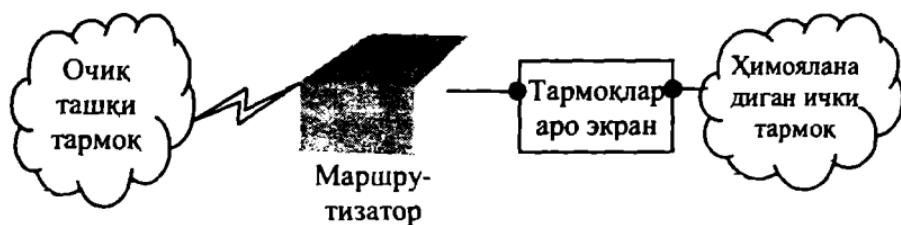
– ҳодисаларни рўйхатга олиш имкониятининг йўклиги; натижада маъмурга маршрутизаторнинг хужумга дуч келганлигини ва обўрўсизлантирилганлигини аниглаш кийинлашади.

*Локал тармоқни умумий ҳимоялаш схемалари.* Битта тармок интерфейсли брандмауэрлардан фойдаланилган ҳимоялаш схема-

лари (6.11-расм) хавфсизлик ва конфигурациялашнинг қулийлиги нуткай назаридан самарасиз хисобланади. Улар ички ва ташки тармоқларни физик ажратмайдилар, демак, тармоқлараро алоқанинг ишончли химоясини таъминлай олмайдилар.



6.11-расм. Битта тармоқ интерфейсли firewall ёрдамида локал тармоқни химоялаш.



6.12-расм. Локал тармоқни умумий химоялаш схемаси.

Локал тармоқни умумий химоялаш схемаси энг оддий ёним бўлиб, унда брандмауэр локал тармоқни ташки ганим тармоқдан бутунлай экранлайди (6.12-расм). Маршрутизатор ва брандмауэр орасида факат битта йўл бўлиб, бу йўл орқали бутун трафик ўтади. Брандмауэрнинг ушбу варианти «ошкора рухсат этилмагани ман килинган» принципига асосланган химоялаш сиёсатини амалга оширили. Одатда, маршрутизатор шундай созланадики. брандмауэр ташкаридан кўринадиган ягона машина бўлади.

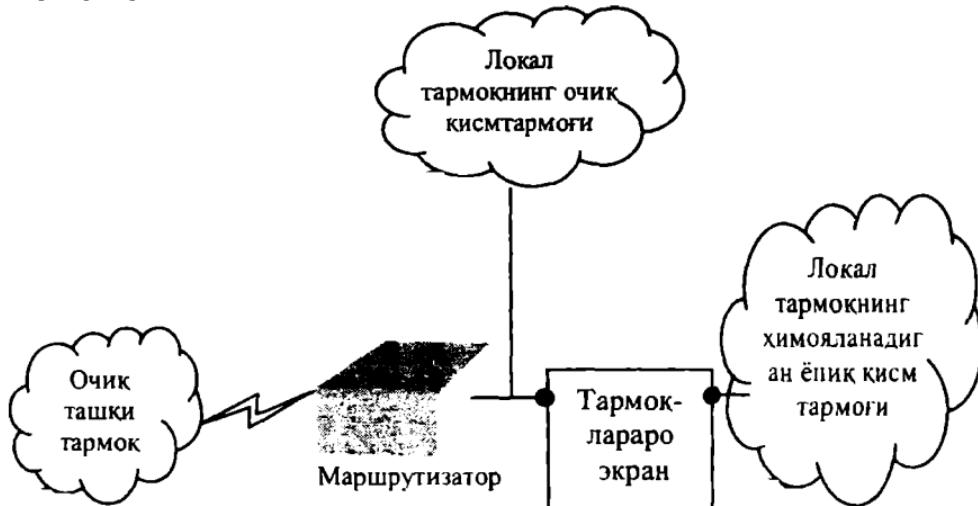
Локал тармоқ таркибидаги очик серверлар ҳам гармоқлараро экранлар томонидан химояланади. Аммо, ташки тармоқ фойдалана оладиган серверларни химоялапувчи локал тармоқларнинг бошқа

ресурслари билан бирлаштириш тармоклараро алоқа хавфсизлиги-ни жиддий пасайтиради.

Тармоклараро экран фойдаланадиган хостга фойдаланувчиларни қучайтирилган аутентификациялаш учун дастур ўнатилиши мумкин.

*Химояланувчи ёпик ва химояланмайдиган очик кисм тармокли схемалар.* Агар локал тармок таркибида умумфойдаланувчи очик серверлар бўлса уларни тармоклараро экрандан олдин очик кисм тармок сифатида чиқариш мақсадга мувофик хисобланади (6.13-расм).

Ушбу усул локал тармок ёпик кисмининг кучли химояланишини, аммо тармоклараро экрангача жойлашган очик серверларнинг пасайган химояланишини таъминлайди.



6.13-расм. Химояланадиган ёпик ва химояланмайдиган очик кисм тармокли схема.

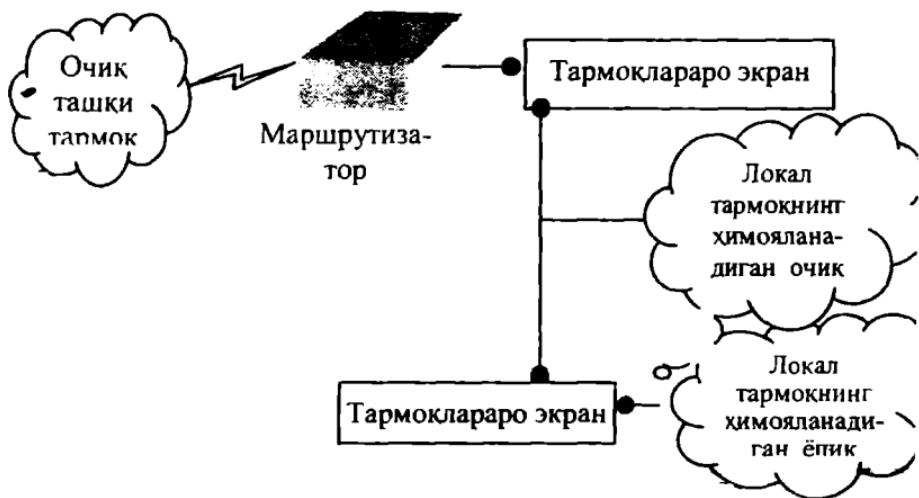
Баъзи брандмауэрлар бу серверларни ўзида жойлаштиради. Аммо бу брандмауэрнинг хавфсизлиги ва компьютернинг юкланиши нуткаи назаридан яхши очим хисобланмайди. Химояланувчи ёпик ва химояланмайдиган очик кисм тармокли схемани очик кисм тармок хавфсизлигига кўйиладиган талабларнинг юкори бўлмаган ҳолларида ишлатилиши мақсадга мувофик хисобланади. Агар очик сервер хавфсизлигига юкори талаблар кўйилса, ёпик ва очик кисм тармокларни алоҳида химоялаш схемаларидан фойдаланиш зарур.

**Ёпиқ ва очик қисм тармоқларни алоҳида ҳимояловчи схемалар.** Бундай схемалар учта тармок интерфейсли битта брандмауэр (6.14-расм) ёки иккита тармок интерфейсли иккита брандмауэр (6.15-расм) асосида курилиши мумкин. Иккала ҳолда ҳам очик ва ёпиқ қисм тармоқлардан факат тармоқлараро экран оркали фойдаланиш мумкин. Бунда очик қисм тармоқдан фойдаланиш ёпиқ қисм тармоқдан фойдаланишга имкон бермайди.

Иккита брандмауэрли схема тармоқлараро алоқа хавфсизлигининг юкори даражасини таъминлайди. Бунда ҳар бир брандмауэр ёпиқ тармоқни ҳимоялашнинг алоҳида эшелонини хосил килади, ҳимояланувчи очик қисм тармоқ эса экранловчи қисм тармоқ сифатида иштирок этади.



6.14 -расм. Учта тармок интерфейсли бир брандмауэр асосида ёпиқ ва очик қисм тармоқларни алоҳида ҳимоялаш схемаси.



6.15-расм. Иккита тармок интерфейсли иккита брандмауэр асосида ёпиқ ва очик қисм тармоқларни алоҳида ҳимоялаш схемаси.

Одатда, экранловчи кисм тармок шундай конфигурацияланади, кисм тармок компьютеридан ғаним ташки тармок ва локал тармокнинг ёпик кисм тармоғи фойдалана олсин. Аммо ташки тармок ва ёпик кисм тармок орасида тўғридан-тўғри ахборот пакетларини алмашиш мумкин эмас. Экранловчи кисм тармокли тизимни хужум қилишда, бўлмаганида химоянинг иккита мустакил чизигини босиб ўтишга тўғри келади. Бу эса жуда мураккаб масала ҳисобланади. Тармокларо экран ҳолатларини мониторинглаш воситалари бундай уринишни доимо аниклаши ва тизим маъмури ўз вактида рухсатсиз фойдаланишга қарши зарурый чоралар кўриши мумкин.

Таъкидлаш лозимки, алоканинг коммутацияланувчи линияси оркали уланувчи масофадаги фойдаланувчиларнинг иши ҳам ташкилотда ўтказилувчи хавфсизлик сиёсатига мувофик назорат қилиниши шарт. Бундай масаланинг намунавий ҳал этилиши – зарурый функционал имкониятларга эга бўлган масофадан фойдаланиш серверини (терминал серверни) ўрнатиш. Терминал сервер бир неча асинхрон портларга ва локал тармокнинг битта интерфейсига эга бўлган тизим ҳисобланади. Асинхрон портлар ва локал тармок орасида ахборот алмашиш факат ташки фойдаланувчини аутентификациялашдан кейин амалга оширилади.

Терминал серверни улаш шундай амалга ошириш лозимки, унинг иши факат тармоклараро экран оркали бажарилсин. Бу масофалаги фойдаланувчиларнинг ташкилот ахборот ресурслари билан ишлаш хавфсизлигининг керакли даражасини таъминлашга имкон беради.

Терминал серверни очик кисм тармок таркибига киритилганида бундай уланиш жоиз ҳисобланади. Терминал сервернинг дастурний таъминоти коммутацияланувчи каналлар оркали алоқа сеансларини маъмурлаш ва назоратлаш имкониятини таъминлаши лозим. Замонавий терминал серверларни бошқариш модуллари серверни ўзини хавфсизлигини таъминлаш ва мижозларнинг фойдаланишини чегаралаш бўйича етарлича ривожланган имкониятларга эга ва куйидаги функцияларни бажаради:

- кегма-кет портлардан, PPP протоколи бўйича масофадан, ҳамда маъмур консолидан фойдаланишда локал паролни ишлатиш;
- локал тармокнинг қандайдир машинасининг аутентификациялашга сўровидан фойдаланиш; .

- аутентификациялашнинг ташки воситаларидан фойдаланиш;
- терминал сервери портларидан фойдаланишни назоратловчи рўйхатни ўрнатиш;
- терминал сервер орқали алока сеансларини протоколлаш.

**Шахсий ва тақсимланган тармоқ экранлари.** Охири 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. Яқиндаёк бундай чегара барча маршрутизаторлар ёки бошка курилмалар (масалан, модемлар) орқали ўтар ва улар ёрдамида ташки тармокларга чикилар эди. Аммо ҳозирда тармоклараро экран орқали химояланувчи тармоқнинг тўла хукукли эгаси – химояланувчи периметр ташқарисидаги ходим хисобланади. Бундай ходимлар сирасига уйдаги ёки меҳнат сафаридағи ходимлар киради. Шубҳасиз, уларга ҳам химоя зарур. Аммо барча анъанавий тармоклараро экранлар шундай қурилганки, химояланувчи фойдаланувчилар ва ресурслар уларнинг химоясида корпоратив ёки локал тармоқнинг ички томонида бўлишлари шарт. Бу эса мобил фойдаланувчилар учун мумкин эмас.

Бу муаммони ечиш учун куйидаги ёндашишлар тақлиф этилган:

- таксимланган тармоклараро экранлардан (distributed firewall) фойдаланиш;
- виртуал ҳусусий тармоқ VPNлар имкониятидан фойдаланиш.

**Тақсимланган тармоқлараро** экран тармоқнинг алоҳида компьютерини химояловчи марказдан бошқарилувчи тармоқ мини-экранлар мажмуидир.

Таксимланган брандмауэрларнинг катор функциялари (масалан, марказдан бошқариш, хавфсизлик сиёсатини тарқатиш) шахсий фойдаланувчилар учун ортиқча бўлгандиги сабабли, таксимланган брандмауэрлар модификацияланди. Янги ёндашиш *шахсий тармоқти экранлаш технологияси* номини олди. Бунда тармоқли экран химояланувчи шахсий компьютерда ўрнатилади. Компьютернинг шахсий экрани (personal firewall) ёки тармоқти экранлаш гизими деб аталувчи бундай экран, бошка барча тизимни химоялаш воситаларига боғлиқ бўлмаган холда бугун чиқувчи ва

кирувчи трафикни назоратлайди. Алоҳида компьютерни экранлашда тармок сервисдан фойдаланувчаник мададланади, аммо ташки фаолликнинг юкланиши пасаяди. Натижада, шу тариқа химояланувчи компьютер ички сервисларининг заифлиги пасаяди, чунки четки нияти бузук одам олдин, химоялаш воситалари син-чиклаб ва катъий конфигурацияланган, экранни босиб ўтиши лозим.

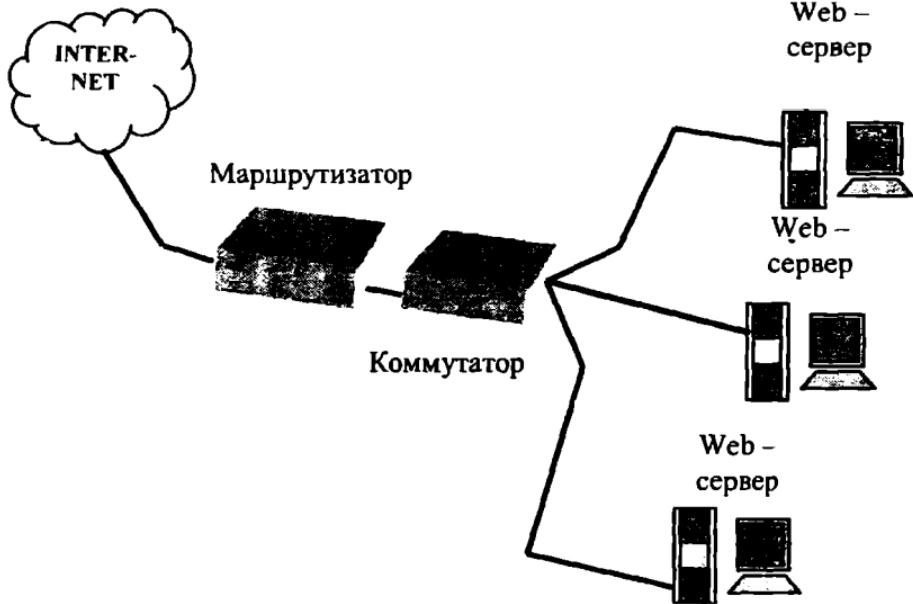
Таксимланган тармоклараро экраннинг шахсий экрандан асосий фарқи-таксимланган тармоклараро экранда марказдан бошқариш функциясининг борлиги. Агар шахсий тармокли экранлар улар ўрнатилган компьютер орқали бошқарилса (уй шароитида қўлланишга жуда мос), таксимланган тармоклараро экранлар ташкилотнинг бош офисида ўрнатилган бошқаришнинг умумий консоли томонидан бошқарилиши мумкин.

Корпоратив тармок рухсатсиз фойдаланишдан ҳакикатан ҳам химояланган хисобланади, қачонки, унинг Internetдан кириш нуқтасида химоя воситалари ҳамда ташкилот локал тармоғи фрагментларини, корпоратив серверларини ва алоҳида компьютерлар хавфсизлигини таъминловчи ечимлар мавжуд бўлса. Таксимланган ёки шахсий тармоклараро экран асосидаги ечимлар алоҳида компьютерлар, корпоратив серверлар ва ташкилот локал тармок фрагментлари хавфсизлигини таъминлашни аъло дараҷада бажаради.

Таксимланган тармоклараро экранлар, анъанавий тармоклараро экранлардан фарқли равишда, кўшимча дастурий таъминот бўлиб, хусусан корпоратив серверларни, масалан, Internet-серверларни ишончли химоялаши мумкин. Корпоратив тармокни химоялашнинг оқилона ечими – химоялаш воситасини у химоя килувчи сервери билан бир платформада жойлаштиришдир. 6.16-расмда корпоратив серверларни таксимланган тармоклараро экранлар ёрдамида химоялаш схемаси келтирилган.

Анъанавий ва таксимланган тармоклараро экранларни қўйидаги кўрсаткичлари бўйича таққослайлик.

*Самарадорлик.* Анъанавий брандмауэр кўпинча тармок периметри бўйича жойлаштирилади, яъни у химоянинг бир катламини таъминлайди холос. Агар бу ягона катлам бузилса, тизим ҳаркандай хужумга бардош берадилмайди. Шахсий брандмауэр опс操цион тизимнинг ядро сатҳида ишлайди ва барча кирувчи ва чиқувчи пакетларни текшириб корпоратив серверларни ишончли химоялайди.



6. /6 -расм. Тақсимланган тармоқлараро экранлар ёрдамида корпоратив серверларни химоялаш.

Тақсимланган брандмауэр дастурый таъминот бўлиб, санокли дақикаларда ўрнатилади ва олиб ташланади.

**Бошқарши.** Анъанавий брандмауэр тармок маъмури томонидан бошқарилади. Тақсимланган брандмауэр тармок маъмури ёки локал тармок фойдаланувчиси томонидан бошқарилиши мумкин.

**Унумдорлик.** Анъанавий брандмауэр тармоқлараро алмашишини таъминловчи курилма бўлиб, унумдороиги (пакет/дақика бўйича) белгиланган чегараланишга эга. У бир-бири билан коммутацияланувчи маҳаллий тармок оркали боғланган ўсувчи сервер парклари учун тўғри келмайди. Тақсимланган брандмауэр кабул килинган хавфсизлик сиёсатига зиён етказмасдан сервер паркларини ўсишига имкон беради.

**Нархи.** Анъанавий брандмауэр, одатда, функциялари белгиланган, нархи етарлича юқори гизим хисобланади. Брандмауэрнинг тақсимланган махсулотлари дастурый 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 қуриш концепцияси

Internet нинг гуриллаб ривожланиши натижасида дунёда ахборотни тарқатиш ва фойдаланишда сифатий ўзгариш содир бўлди. Internet фойдаланувчилари арzon ва кулай коммуникацияга эга бўлдилар. Корхоналар Internet каналларидан жиддий тижорат ва бошқарув ахборотларини узатиш имкониятларига қизикиб қолдилар. Аммо Internetнинг қурилиши принципи нияти бузук одамларга ахборотни ўғирлаш ёки атайн бузиш имкониятини яратди. Одатда, TCP/IP протоколлар ва стандарт Internet-иловалар (e-mail, Web, FTP) асосида қурилган корпоратив ва идора тармоқлари сукилиб киришдан кафолатланмаганлар.

Internetнинг ҳамма ерда тарқалишидан манфаат кўриш мақсадида тармоқ ҳужумларига самарали қаршилик 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 вактинча деб кўрилишини таъкидлаш мақсадида киритилган. Ҳакиқатан, бу уланиш доимий, қатъий бўлмай, фақат очик тармоқ бўйича трафик ўтганида мавжуд бўлади.

Виртуал тармоқ VPNларни қуриш концепцияси асосида етарлича оддий гоя ётади: агар глобал тармоқда ахборот алмашинувчи иккита узел бўлса, бу узеллар орасида очик тармоқ орқали узатилаётган ахборотнинг конфиденциаллигини ва яхлитлигини таъминловчи виртуал ҳимояланган туннел қуриш зарур ва бу виртуал туннелдан барча мумкин бўлган ташки фаол ва пассив кузатувчиларнинг фойдаланиши ҳаддан ташкари кийин бўлиши лозим.

Шундай килиб, VPN туннели очик тармок орқали ўтказилган уланиш бўлиб, у орқали виртуал тармокнинг криптографик химояланган ахборот пакетлари узатилади. Ахборотни VPN туннели бўйича узатилиши жараёнидаги химоялаш қуидаги вазифаларни бажаришга асосланган:

- ўзаро алоқадаги тарафларни аутентификациялаш;
- узатилувчи маълумотларни криптографик беркитиш (шифрлаш);
- етказиладиган ахборотнинг ҳакиқийлигини 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 тармок, масалан, Internet доирасида, сафланади. VPN қурилмалари виртуал хусусий тармокларда VPN-мижоз, VPN-сервер ёки VPN хавфсизлиги шлюзи вазифасини ўташи мумкин.

*VPN-мижоз* одатда шахсий компьютер асосидаги дастурий ёки дастурий-аппарат комплекси бўлиб, унинг тармок дастурий таъминоти у бошка 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 ташки тармокларнинг рухсатсиз фойдаланишидан серверларни химоялашни ҳамда алоҳида компьютерлар ва мос VPN-маҳсулотлари орқали химояланган локал тармок сегментларидағи компьютерлар билан химояланган уланишларни ташкил этишни таъминлайди. VPN-сервер VPN-мижознинг сервер платформалари учун функционал аналог хисобланади. У аввало, VPN-мижозлар билан кўпгина уланишларни маддадловчи кенгайтирилган ресурслари билан ажралиб туради. VPN-сервер мобил фойдаланувчилар билан уланишларни ҳам мададлаши мумкин.

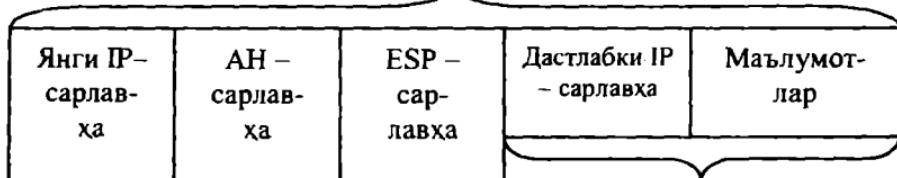
*VPN* хавфсизлик шлюзи. (Security gateway) иккита тармокка уланувчи тармок курилмаси бўлиб, ўзидан кейин жойлашган кўп сонли хостлар учун шифрлаш ва аутентификациялаш вазифаларини бажаради. *VPN* хавфсизлиги шлюзи шундай жойлаштирилади, ички корпоратив тармокка аталган барча трафик у орқали ўтади. *VPN* хавфсизлиги шлюзининг манзили кирувчи туннелланувчи пакетнинг ташки манзили сифатида кўрсатилади, пакетнинг ички манзили эса шлюз орқасидаги муайян хост манзили хисобланади. *VPN* хавфсизлиги шлюзи алоҳида дастурий ечим, алоҳида аппарат курилмаси хамда *VPN* вазифалари билан тўлдирилган маршрутизаторлар ёки тармоқлараро экран кўринишида амалга оширилиши мумкин.

Ахборот узатишнинг очик ташки мухити маълумот узатишнинг тезкор каналларини (*Internet* мухити) ва алоканинг секин ишлайдиган умумфойдаланувчи каналларини (масалан, телефон тармоғи каналларини) ўз ичига олади. Виртуал хусусий тармок *VPN*нинг самарадорлиги алоканинг очик каналлари бўйича аланувчи ахборотнинг ҳимояланиш даражасига боғлик. Очик тармок орқали маълумотларни хавфсиз узатиш учун инкапсуляциялаш ва туннеллаш кенг ишлатилади. Туннеллаш усули бўйича маълумотлар пакети умумфойдаланувчи тармок орқали худди оддий икки нуктали уланиш бўйича узатилганидек узатилади. Ҳар бир «жўнатувчи-қабул килувчи» жуфтлиги орасига бир протокол маълумотларини бошқасининг пакетига инкапсуляциялашга имкон берувчи ўзига хос туннел-мантикий уланиш ўрнатилади.

Туннеллашга биноан, узатилувчи маълумотлар порцияси хизматчи ҳошиялар билан бирга янги «конверт»га «жойлаш» амалга оширилади. Бунда пастрок сатҳ протоколи пакети юқорироқ ёки худди шундай сатҳ протоколи пакети маълумотлари майдонига жойлаштирилади. Таъкидлаш лозимки, туннелашибнинг ўзи маълумотларни рухсатсиз фойдаланишдан ёки бузишдан ҳимояламайди, аммо туннеллаш туфайли инкапсуляцияланувчи дастлабки пакетларни тўла криптографик ҳимоялаш имконияти пайдо бўлади. Узатилувчи маълумотлар конфиденциаллигини таъминлаш мақсадида жўнатувчи дастлабки пакетларни шифрлайди, уларни, янги IP-сарлавҳа билан ташки пакетга жойлади ва транзит тармок бўйича жўнатади (7.1-расм).

Очик тармок бўйича маълумотларни ташишда ташки пакет сарлавҳасининг очик каналларидан фойдаланилади.

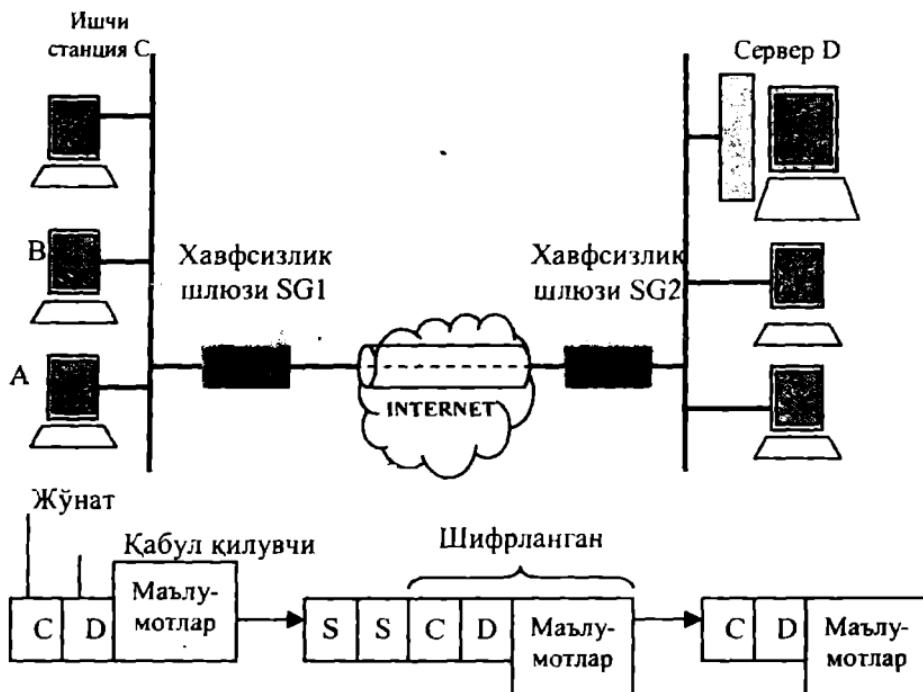
## Янги пакет



## Дастлабки пакет

7.1-расм. Туннеллашга тайёрланган пакет мисоли.

Ташки пакет химояланган каналнинг охирги нуктасига келиши билан ундан ички дастлабки пакет чиқариб олиниб, расшифровка килинади ва унинг тикланган сарлавхаси ички тармок бўйича кейинги узатиш учун ишлатилади (7.2-расм).



7.2-расм. Виртуаль химояланган туннел схемаси.

Туннеллашдан пакет таркибини нафакат конфиденциаллигини, балки унинг яхлитлигини ва аутентлигини таъминлашда фойдала-

нилади. Бунда электрон ракамли имзони пакетнинг барча ҳошияларига тарқатиш мумкин.

Internet билан боғланмаган локал тармок яратилганда компания ўзининг тармок қурилмалари ва компьютерлари учун хохлаган IP-манзилдан фойдаланиши мумкин. Олдин яккаланган тармокларни бирлаштиришда бу манзиллар бир-бирлари ва Internetда ишлатилаётган манзиллар билан тўқнашишлари мумкин. Пакетларни инкапсулациялаш бу муаммони ечади, чунки у дастлабки манзилларни беркитишга ва Internet IP - манзиллари маконидаги ноёб манзилларни қўшишга имкон беради. Бу манзиллар кейин маълумотларни ажратилувчи тармоклар бўйича узатишда ишлатилади. Бунга локал тармокка уланувчи мобил фойдаланувчиларнинг IP-манзилларини ва бошқа параметрларини созлаш масаласи ҳам киради.

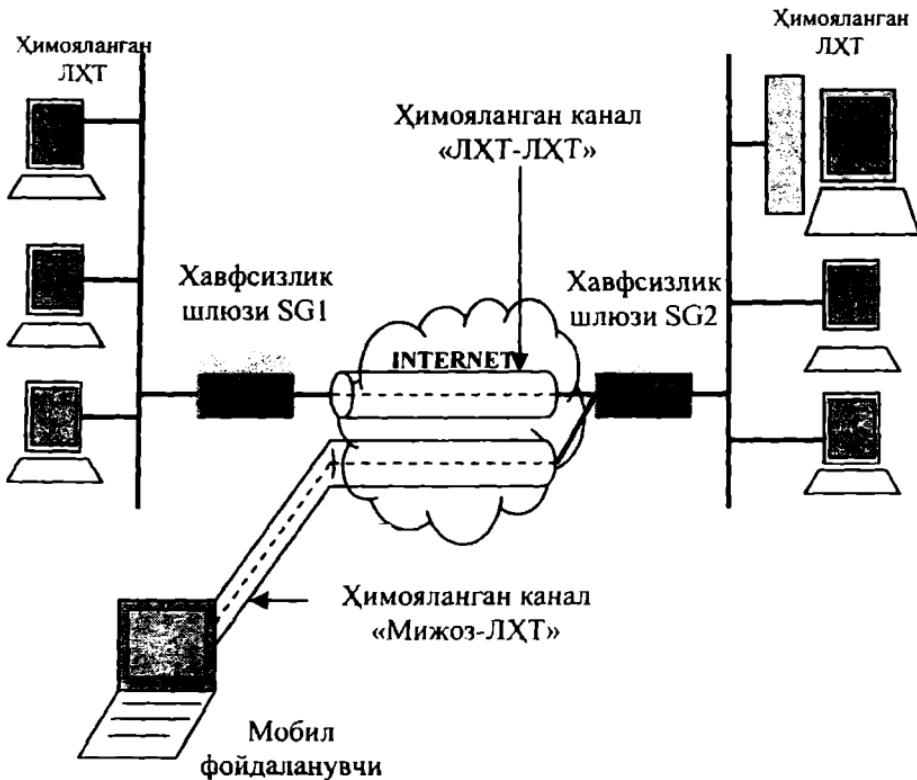
Туннеллаш механизми химояланувчи канални шакллантирувчи турли протоколларда кенг қўлланилади. Одатда, туннел факат маълумотларнинг конфиденциаллиги ва яхлитлигининг бузилиши хавфи мавжуд бўлган очик тармок кисмida, масалан, очик Internet ва корпоратив тармок кириш нуқталари орасида, яратилади. Бунда ташки пакетлар учун ушбу икки нуктада ўрнатилган чегара маршрутизаторларининг манзилларидан фойдаланилса, охирги узелларнинг ички манзиллари ички дастлабки пакетларда химояланган ҳолда сакланади. Таъкидлаш лозимки, туннеллаш механизмининг ўзи қандай мақсадларда туннеллаш қўлланилаётганига боғлик эмас. Туннеллаш нафакат узатилаётган барча маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлашда, балки турли протоколи (масалан, IPv4 ва IPv6) тармоклар орасида ўтишни ташкил этишда ҳам қўлланилади. Туннеллаш бир протокол пакетини бошқа протоколдан фойдаланувчи мантикий мухитда узатишни ташкил этишга имкон беради. Натижада, бир неча турли хил тармокларнинг ўзаро алокалари 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 тармокларида маълумотларни ташувчи транспорт протоколи IPX ишлатилиши мумкин. Элтувчи протоколнинг энг кўп тарқалган варианти Ipsec тармогининг IP-протоколи хисобланади. Туннеллаш протоколи сифагида канал сатҳи протоколари PPTP ва L2TP,

хамда тармоқ сатхи протоколи IPSec ишлатилиши мумкин. Туннеллаш туфайли Internet инфратузилмасини VPN-иловалардан беркитиш 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 химояланаш учун ишлатиш максадга мувофиқ бўлса, VPN-серверлар ва VPN-мижозлардан масофадаги ва мобил фойдаланувчиларни Internet оркали корпоратив тармоқ билан химояланган уланишини ташкил этишда фойдаланилади.

**Виртуал химояланган каналларни қуриш вариантилари.** VPN ни лойихалашда одатда, иккита асосий схема қўрилади (7.3-расм):



7.3-расм. «ЛХТ-ЛХТ» ва «Мижоз-ЛХТ» хилидаги виртуал химояланган каналлар

- локал тармоклар орасидаги виртуал химояланган канал («ЛХТ-ЛХТ» канал);
- узел ва локал тармок орасидаги виртуал химояланган канал («мижоз-ЛХТ» канали).

Уланишнинг биринчи схемаси алоҳида оғислар орасидаги кимматли ажратилган линиялар ўрнига ўтади ва улар орасида доимо фойдаланувчан, химояланган каналларни яратади. Бу ҳолда хавфсизлик шлюзи туннел ва локал тармок орасида интерфейс вазифасини ўтайди ва локал тармок фойдаланувчилари бир-бирлари билан мулоқот килишда туннелдан фойдаланадилар. Аксарият компаниялар VPNнинг бу хилидан глобал тармокнинг мавжуд Frame Relay каби уланишларни алмаштириш учун ёки уларга кўшимча сифатида фойдаланадилар.

VPN химояланган каналнинг иккинчи схемаси масофадаги ёки мобил фойдаланувчилар билан уланишни ўрнатишга аталган. Туннелни яратишни мижоз (масофадан фойдаланувчи) бошлаб беради. Масофадаги тармокни химояловчи шлюз билан боғланиш учун у ўзининг компьютерида маҳсус мижоз дастурий таъминотини ишга туширади. VPNнинг бу тури коммутацияланувчи уланишларни ўрнига ўтади ва масофадан фойдаланишнинг анъанавий усуллари билан бир каторда ишлатилиши мумкин.

Виртуал химояланган каналларнинг катор вариантлари мавжуд. Умуман, орасида виртуал химояланган канал шакллантирилувчи корпоратив тармокнинг ҳар кандай иккита узели химояланувчи ахборот оқимининг охирги ва оралик нуктасига таалукли бўлиши мумкин. Ахборот хавфсизлиги нуктаи назаридан химояланган туннел охирги нукталарининг химояланувчи ахборот оқимининг охирги нукталарига мос келиши варианти маъкул 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 тармокдаги локал тармок ичida графикни химоялаш талаб этилмаса, химояланган туннелнинг охирги нуктаси сифатида ушбу локал тармокнинг тармокларапо экрани ёки чегара маршрутизатори танланиши мумкин. Агар локал тармок ичидаги ахборот оқими химояланиши шарт бўлса, бу тармок охирги нуктаси вазифасини химояланган алокада иштирок этувчи компьютер бажаради.

Локал тармоқдан масофадан фойдаланилганида фойдаланувчи компьютери виртуал химояланган каналнинг охирги нуктаси бўлиши шарт. Факат пакетларни коммутациялашти очик тармоқ, масалан Internet ичидаги ўтказилувчи химояланган туннел варианти етарижа кенг таркалган. Ушбу вариант ишлатилиши кулиялиги билан ажралиб турсада, нисбатан паст хавфсизликка эга. Бундай туннелнинг охирги нукталари вазифасини одатда, Internet провайдерлари ёки локал тармоқ чегара маршрутизаторлари (тармоқлараро экранлар) бажаради.

Локал тармоқлар бирлаштирилганида туннел факат 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 мижоз компьютерлари ва серверлари учун тўла шаффофф хисобланади. Ушбу узелларнинг дастурий таъминоти ўзгармайди. Аммо бу вариант ахборот алоқасининг нисбатан паст хавфсизлиги билан характерланади, чунки трафик кисман очик алоқа канали бўйича химояланмаган ҳолда ўтади. Агар шундай VPNни яратиш ва эксплуатация килишни провайдер ISP ўз зиммасига олса, барча виртуал хусусий тармоқ унинг шлюзларида, локал тармоқлар ва корхоналарнинг масофадаги фойдаланувчилари учун шаффофф 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 кабул килинган.

*Туннел инициатори* дастлабки пакетни янги пакетга, жўнатувчи ва кабул килувчи 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

хисобланади. Туннелнинг инициатори ва терминатори орасидаги маршрутни одатда, Internetдан фарқланиши мумкин бўлган, оддий маршрутланувчи тармоқ IP аниклади.

Туннелни инициаллаш ва узиш турли тармоқ курилмалари ва дастурий таъминот ёрдамида амалга оширилиши мумкин. Масалан, туннел масофадан фойдаланиш учун улашни таъминловчи модем ва мос дастурий таъминот билан жихозланган мобил фойдаланувчинг ноутбуки томонидан инициалланиши мумкин. Инициатор вазифасини мос функционал имкониятларга эга бўлган локал тармоқ маршрутизатори хам бажариши мумкин. Туннел одатда, тармоқ коммутатори ёки хизматлар провайдери шлюзи билан туғалланади.

*Туннел терминатори инкапсуляциялаш жараёнига тескари жараённи бажаради. Терминатор янги янги сарлавҳаларни олиб ташлаб, хар бир дастлабки пакетни локал тармоқдаги манзилга йўллади.*

Инкапсуляцияланувчи пакетларнинг конфиденциаллиги уларни шифрлаш, яхлитлиги ва ҳакиқийлиги эса электрон ракамли имзони шакллантириш йўли билан таъминланади. Маълумотларни криптографик химоялашнинг жўда қўп усуллари ва алгоритмлари мавжуд бўлганлиги сабабли, туннел инициатори ва терминатори химоянинг бир хил усулларидан фойдаланишга ўз вактида келишиб олишлари максадга мувофик хисобланади. Маълумотларни расшифровка килиш ва ракамли имзони текшириш имкониятини таъминлаш учун туннел инициатори ва терминатори катитларни хавфсиз алмашиш вазифасини хам мададлашлари зарур. Ундан ташкари, VPN туннеларини ваколатли фойдаланувчилар гомонидан яратилишини кафолатлаш максадида ахборот алоқасининг асосий тарафлари аутентификациялашдан ўтишлари лозим. Корпорациянинг мавжуд тармоқ инфратузилмалари VPNдан фойдаланишга хам дастурий, хам аппарат таъминот ёрдамида тайёрланишлари мумкин.

## 7.2. Химояланган виртуал хусусий тармоқларнинг туркумланиши

Химояланган виртуал хусусий тармоқлар VPNни туркумлашни турли варианtlари мавжуд. Кўпинча туркумлашнинг куйидаги учта аломати ишлатилади:

- OSI моделининг иш сатхи;
- VPN техник ечимиининг архитектураси;
- VPNни техник амалга ошириш усули.

### ***OSI моделининг иш сатҳи бўйича VPNнинг туркумланиши.***

Ушбу туркумлаш анчагина кизикиш тўғдиради, чунки амалга оширилувчи VPNнинг функционаллиги ва унинг корпоратив ахборот тизимлари иловалари ҳамда химоянинг бошка воситалари билан биргаликда ишлатилиши кўп холларда танланган OSI сатхига боғлик 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 курилади. Бунинг сабаби шуки, химояланган канал воситалари қанчалик пастки сатҳда амалга оширилса, уларни иловаларга ва татбиқий протоколларга шунчалик шаффоф килиш соддалашади. Тармоқ ва канал сатҳларида иловаларнинг химоя протоколларига боғликлиги умуман йўқолади. Шу сабабли, фойдаланувчилар учун универсал ва шаффоф химояни фақат OSI моделининг пастки сатҳларида куриш мумкин. Аммо, бунда биз бошқа муаммога химоя протоколининг муайян тармоқ технологиясига боғликлиги муаммосига дуч келамиз.

***Каналь сатҳидаги VPN.*** OSI моделининг канал сатҳида ишлатилувчи VPN воситалари учинчи (ва юкорироқ) сатхнинг турли хил трафигини инкапсуляциялашни таъминлашга ва «нукта-нукта» тилидаги виртуал туннелларни (маршрутизатордан маршрутизаторга ёки шахсий компьютердан локал хисоблаш тармоғининг шлюзи-гача) куришга имкон беради. Бу гурухга L2F (Layer 2 Forwarding) ва PPTP (Point-to-Point Tunneling Protocol) протоколлари ҳамда Cisco Systems и MicroSoft фирмаларининг бирга ишлаб чиккан L2TP(Layer 2 Tunneling Protocol) стандартидан фойдаланувчи VPN-маҳсулотлар тааллукли.

Химояланган каналнинг протоколи PPTP «нукта-нукта» уланишларида, масалан, ажратилган линияларда ишлаганда кенг кўлланилувчи PPP протоколига асосланган. PPTP протоколи иловалари ва татбиқий сатҳ хизматлари учун химоя воситаларининг шаффоғлигини таъминлайди ва тармоқ сатҳида ишлатилувчи протоколга боғлик эмас. Хусусан, PPTP протоколи ҳам IP тармоқларида, ҳам IPX, DECnet ёки NetBEUL протоколлари асосида ишловчи тармоқларда пакетларни ташиши мумкин. Аммо, PPP

протоколи хамма тармокларда хам ишлатылmasлиги сабабли (аксарият локал тармокларида канал сатхида Ethernet протоколи ишласа, глобал тармокларда ATM, Frame Relay протоколлари ишлайди), уни универсал восита деб бўлмайди. Йирик бирикма тармокнинг турли кисмларида, умуман айтганда, турли канал протоколлари ишлатилади. Шу сабабли бу гетероген мухит орқали канал сатхининг ягона протоколи ёрдамида химояланган канални ўтказиш мумкин эмас.

L2TP протоколи, эҳтимол, локал хисоблаш тармокларидан фойдаланишни ташкил этишда устунлик килувчи ечим бўлиб колиши мумкин (чунки у, асосан, Windows операцион тизимига таянади.)

*Тармоқ сатхидаги VPN.* Тармоқ сатхидаги VPN-маҳсулотлар IPни IPга инкапсуляциялашни бажаради. Бу сатхдаги кенг таркалган протоколлардан бири SKIP протоколидир. Аммо бу протоколни аутентификациялаш, туннеллаш ва IP-пакетларни шифрлаш учун аталган IPSec(IPSecurity) протоколи аста-секин сўриб чиқармоқда.

Тармоқ сатхидаги IPSec протоколи муросага асосланган вариант хисобланади. Бир томондан у иловалар учун шаффоф, иккинчи томондан кенг таркалган IP протоколига асосланганлиги сабабли барча тармокларда ишлаши мумкин. Шу орада эсдан чиқармаслик лозимки, IPSecнинг спецификацияси IPга мўлжалланганлиги сабабли у тармоқ сатхининг бошқа протоколлари трафиги учун тўғри келмайди. IPSec протоколи L2TP протоколи билан биргалиқда ишлаши мумкин. Натижада, бу икки протокол ишончли идентификациялашни, стандартланган шифрлашни ва маълумотлар яхлитлигини таъминлайди. Иккита локал тармоқ орасидаги IPSec туннели маълумотлар узатувчи якка тармоклар тўпламини мададлаши мумкин. Натижада, бу хилдаги иловалар масштабланиш нуктаи назаридан иккинчи сатҳ технологияларига нисбатан устунликка эга бўлади.

IPSec протоколи билан масофадаги курилмалар орасида криптографик калитларни хавфсиз бошқариш ва алмашиб масалаларини ечувчи IKE (Internet Key Exchange) протоколи боғланган. IKE протоколи калитларни алмашибни автоматлаштиради ва химояланган уланишни ўранатади, IPSec эса пакетларни кодлайди ва «имзо чекади». Ундан ташкари, IKE ўрнатилган уланиш учун

калитни ўзгартериш имкониятіга зәғін. Бу узатилувчи ахборотнинг конфиденциаллигини оширади.

*Сеанс сатхидаги VPN.* Баъзи VPNлар «канал воситачилари» (circuit proxy) деб аталувчи усулдан фойдаланади. Бу усул транспорт сатхи устида ишлайди ва ҳар бир сокет учун алохіда трафикни химояланган тармокдан умумфойдаланувчи Internet тармоғига ретрансляциялади. (IP сокети TCP-уланишнинг ва муайян порт ёки берилған порт UDP комбинацияси орқали идентификацияланади. TCP/IP стекида бешинчи-сеанс сатхи бўлмайди, аммо сокетларга мўлжалланган амалларни кўпинча сеанс сатхи амаллари деб юритишади.)

Туннелнинг инициатори ва терминатори орасида узатилувчи ахборотни шифрлаш транспорт сатхи TLS(Transport Layer Security) ёрдамида амалга оширилади. Тармоклараро экран орқали аутентификацияланган ўтишни стандартлаш учун SOCKS деб аталувчи протокол аникланган 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-тармоклараро экран орқали боғланишнинг ягона усули. Воситачи, ўз навбатида, мижоз томонидан сўралған ҳар кандай амални бажаради. Воситачига сокет сатхидаги трафик маълумлиги сабабли, у синчиклаб назорат килиши, масалан, муайян иловаларни, агар улар зарурый ва колатларга зәғін бўлмаса, блокировка килиши мумкин.

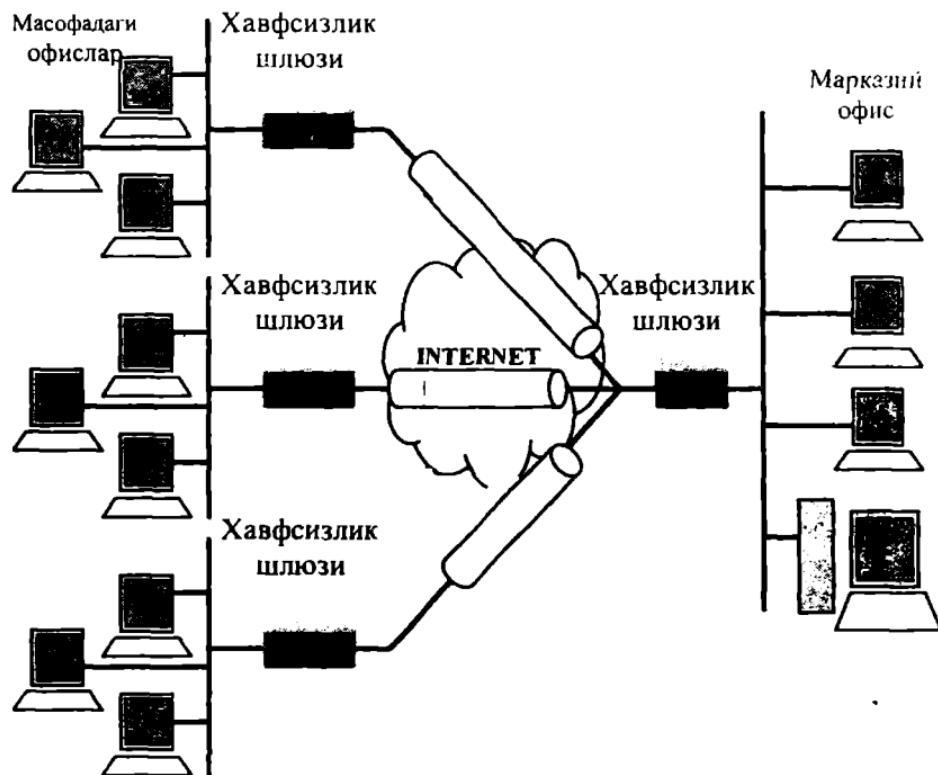
Агар IPSec протоколи мохияти бўйича, IP тармокни химояланган туннелга тарқатса, SOCKS протоколи асосидаги маҳсулотлар уни алохіда ҳар бир илова ва ҳар бир сокетга кенгайтиради. Иккинчи ва учинчи сатхнинг яратилған туннеллари иккала йўналишда бирдай ишласа, 5 сатхнинг VPN тармоғи ҳар бир йўналишда узатишни мустакил бошқаришга рухсат беради. IPSec протоколга ва иккинчи сатх протоколларига ўхшаб 5 сатхнинг VPN тармоклари виртуал хусусий тармокларнинг бошқа турлари билан бирга ишлатилиши мумкин, чунки бу технологиялар бир-бирини инкор кильмайди.

*Техник ечимининг архитектураси бўйича VPNнинг туркумланиши.* Ушбу туркумлаш бўйича виргуал хусусий тармоклар қўйидаги уч турга бўлинади:

- корпорация ичидаги VPN тармок;

- масофадан фойдаланилувчи VPN гармок;
- корпорацияларо VPN тармок.

**Корпорация ичидаги VPN тармок.** Корпорация ичидаги VPN тармоклар (Intranet VPN) корхона ичидаги бўлинмалар ёки алоканинг корпорация тармоклари (шу жумладан, ажратилган линиялар) ёрдамида бирлаштирилган корхоналар гурухи орасида химояланган алокани ташкил этиш учун ишлатилади. Ўзининг филиаллари ва бўлимлари учун ахборотнинг марказлаштирилган омборидан фойдаланишга эхтиёж сезган компаниялар масофадаги узелларни ажратилган линиялар ёки frame relay технологияси ёрдамида улайдилар. Аммо ажратилган линияларнинг ишлатилиши эгалланадиган ўтказиш полосасининг ва объектлар орасидаги ма-софанинг катталашгани сари жорий сарф-харажатларнинг ошишига сабаб бўлади. Буларни камайтириш учун компания узелларини виртуал хусусий тармок ёрдамида улаши мумкин (7.4-расм).



7.4-расм. VPN intranet технологияси ёрдамида тармок узелларини улаш.

Intranet VPN тармоқлар Internetдан ёки сервис-провайдерлар томонидан тақдим этилувчи бўлинувчи тармок инфратузилмаларидан фойдаланган холда курилади. Компания нархи киммат ажратилган линиялардан воз кечиб, уларни арzonрок Internet орқали алоқа билан алмаштиради. Бу ўтказиш полосасидан фойдаланишдаги сарф-харажатни жиддий камайтиради, чунки Internetда масофа уланиш нархига хеч таъсир этмайди.

Intranet VPN учун куйидаги афзаликлар ҳарактерли:

- конфиденциал ахборотни химоялаш учун шифрлашнинг кучли криптографик протоколларидан фойдаланиш;
- автоматглаштирилган савдо тизими ва маълумотлар базасини бошқариш тизими каби жиддий иловаларни бажаришда ишлишнинг ишончлилиги;
- сони тез ўсаёғган фойдаланувчилар, янги оғислар ва янги дастурий иловаларни самаралироқ жойлаштириш учун бошқаришнинг мослашувчанлиги.

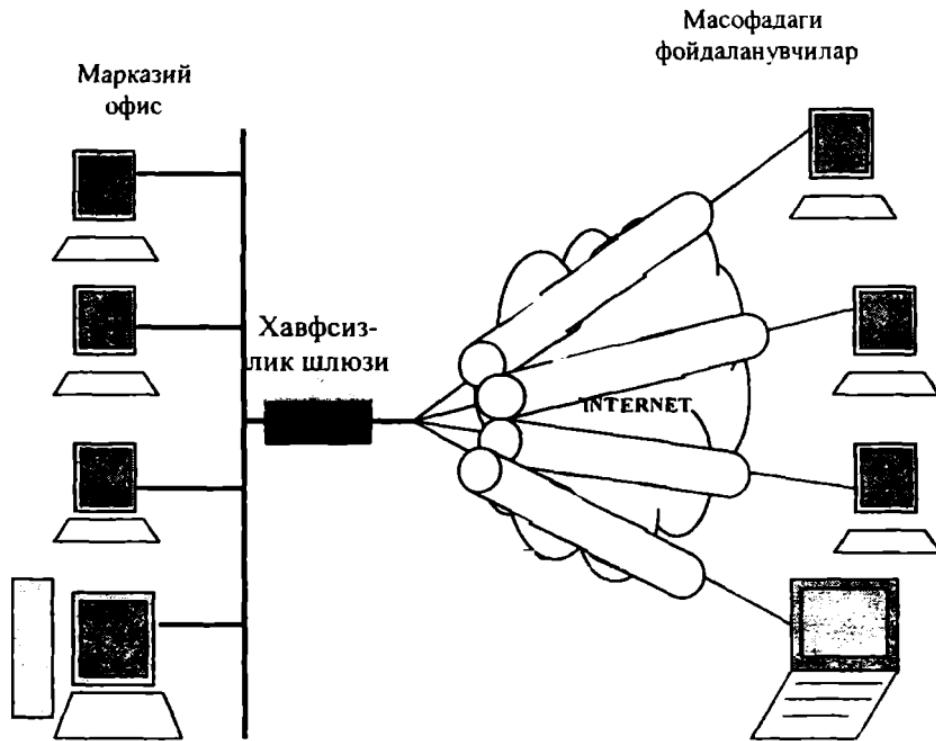
Internetдан фойдаланиб Intranet VPNни куриш VPN-технологияни амалга оширувчи энг рентабел усули хисобланади. Аммо Internetда сервис даражаси умуман кафолатланмайди. Кафолатланган сервис даражасини хохловчи компаниялар ўзларининг VPNларини сервер-провайдерлари томонидан тақдим этилувчи бўлинувчи тармок инфтузилмаларидан фойдаланиб сафлаш имкониятларини кўришлари шарт.

*Масофадан фойдаланилувчи VPN тармоқ.* Масофадан фойдаланилувчи виртуал хусусий тармоқлар VPN (Remote Access VPN) корпорациянинг мобил ёки масофадаги ходимларига (компания раҳбарияти, меҳнат сафаридаги ходимлар, касаначилар ва х.) корхона ахборот ресурсларидан химояланган 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 нуктаси билан уланишларни ўрнатади. Сўнгра уларнинг сўровлари Internet орқали туннелланади. Бу шаҳарлараро ва ҳалкаро алоқа учун тўловдан кутилишга имкон беради. Ундан кейин барча сўровлар мос узелларда тўпланади ва корпорация тармоқларига узатилади.

Хусусий бошкарилувчи тармоқлардан (dial networks) масофадан фойдаланилувчи VPN тармоқларга (Remote Acces VPN) ўтиш қуидаги афзалликларни беради:

- шаҳарлараро ракамлар ўрнига маҳаллий ракамлардан фойдаланиши имконияти шаҳарлараро телекоммуникацияга сарф-харажатларни анчагина камайтиради;
- аутентификациялаш жараёнини ишончли ўтказишни таъминловчи масофадаги ва мобил фойдаланувчилар ҳакицийлигини аниклаш тизимининг самарадорлиги;



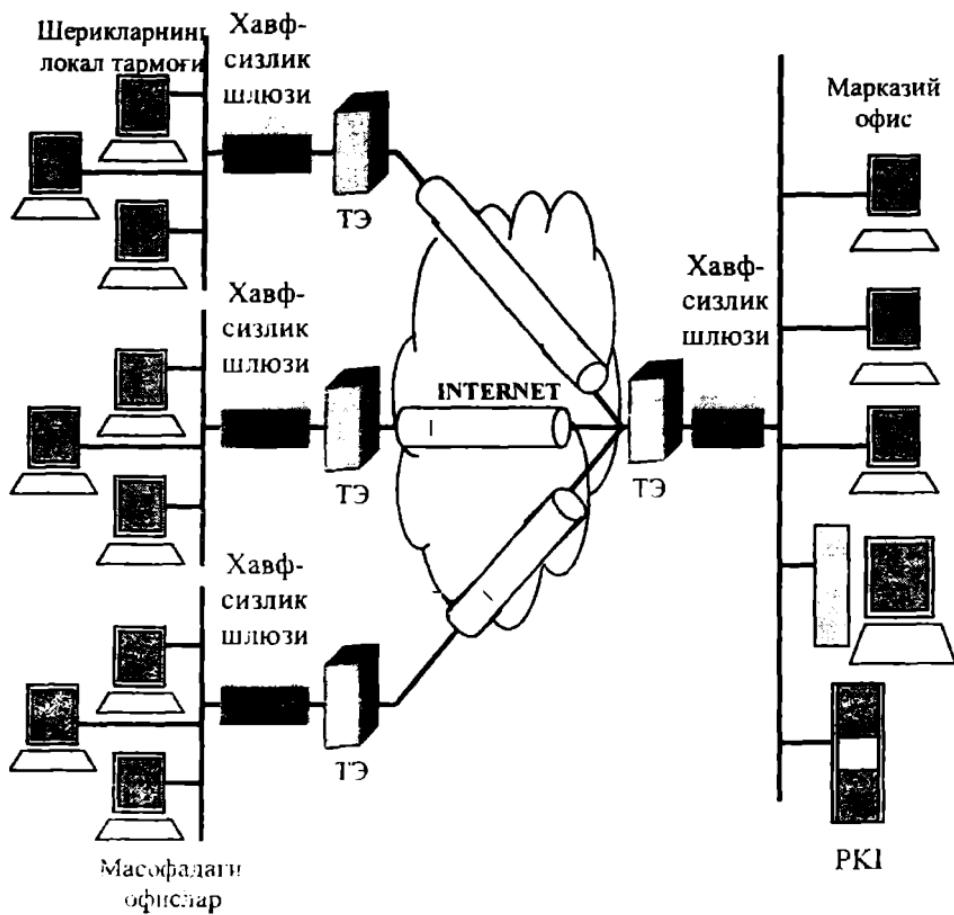
7.5-расм. Масофадан фойдаланишли виртуаль хусусий тармок.

- масштабланишнинг янада юкорилиги ва тармокка қўшилувчи янги фойдаланувчилар сафланишининг оддийлиги;
- компания эътиборини тармок ишлаши муаммолари ўрнига корпорациянинг асосий бизнес-максадларига қаратиш.

Таъкидлаш лозимки, сезувчан корпорация трафигини ташишда очик тармок 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 тармоклардан (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 алока ишончлилигини оширишга имкон берувчи технологиядир.



7-расм Корпорациялараро extranet VPN тармоғи.

Extranet VPN тармоқтары умуман корпорация ичидаги виртуал хусусий тармоқтарға үхшаш, фарқи шундаки, корпорациялараро виртуал хусусий тармоқтар учун ахборот химояси муаммоси кескинроқтады. Extranet VPN үчүн ишбилиармен шериклар ўзларининг тармоқтарыда кўллашлари мумкин бўлган турли VPN ечимлар билан алоқа килиш имкониятларини кафолатловчи стандартгластирилган VPN-максулотлардан фойдаланиш характерлидир.

Бир неча компаниялар бирга ишлашга келишиб, бир-бирларига тармоқтарини очишганида, улар янги шерикларининг факат маълум ахборотдан фойдаланишларига йўл кўйишлари лозим. Бунда конфиденциал ахборот рухсатсиз фойдаланишдан ишончли химояланиши зарур. Айнан, шу сабабли корпорациялараро тармоқларда очик тармок томонидан тармоқлараро экран (бранд-маузер) ёрдамида назоратга катта ахамият берилади. Ахборотдан ҳакикий фойдаланувчининг фойдаланишини кафолатловчи аутентификациялаш хам муҳим ҳисобланади. Шу билан бир каторда рухсатсиз фойдаланишдан химоялашнинг сафланган тизими ўзига эътиборни жалб килмаслиги 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 боғлик.

Баъзида VPN тармоғининг локал варианти (Localnet VPN) алоҳида гурухга ажратилади. Localnet VPN локал тармоғи компания локал тармоғи ичидаги (одагда, марказий офис) айланувчи ахборотлар оқимидан компаниядан ишловчи «ортикча кизиқувчи» ходимларнинг рухсатсиз фойдаланишидан химоялашни гаъминлайди. Таъкидлаш лозимки, хозирда VPNни амалга оширувчи турли усулларнинг конвергенцияси гояси кўзга ташланмоқда.

**Техник амалга ошириш бўйича VPNнинг туркумланиши.** Виртуал хусусий тармоқнинг конфигурацияси ва характеристикалари кўп жихатдан ишлатиладиган VPN-курилмаларининг турига боғлик.

Техник амалга ошириш бўйича VPNнинг куйидаги гурухлари фарқланади:

- маршрутизаторлар асосидаги VPN;
- тармоқлараро экранлар асосидаги VPN;

- дастурий таъминот асосидаги VPN;
- ихтисослаштирилган аппарат воситалари асосидаги VPN.

*Маршрутизаторлар асосидаги VPN.* VPN қуришнинг ушбу усуги биноан химояланган каналларни яратишда маршрутизаторлардан фойдаланилади. Локал тармоқдан чиқувчи барча ахборот маршрутизатор орқали ўтганлиги сабабли, унга шифрлаш вазифасини юклаш табиий. Маршрутизатор асосидаги VPN асбобускуналарига мисол тарикасида Cisco-Systems компаниясининг курилмаларини кўрсатиш мумкин.

*Тармоқлараро экранлар асосидаги VPN.* Аксарият ишласчикарувчиларнинг тармоқлараро экрани туннеллаш ва маълумотларни шифрлаш вазифаларини маддлайди. Тармоқлараро экранлар асосидаги ечимга мисол тарикасида Check Point Software Technologies компаниясининг Fire Wall-1 маҳсулотини кўрсатиш мумкин Шахсий компьютер асосидаги тармоқлараро экранлар факат узати лувчи ахборот ҳажми нисбатан кичик бўлган тармоқларда кўлланилади. Ушбу усулнинг камчилиги – битта ишчи ўрнига хисобланганда ечим нархининг юқорилиги ва унумдорликнин тармоқлараро экран иштайдиган аппарат таъминотига боғликлиги.

*Дастурий таъминот асосидаги VPN.* Дастурий усул бўйича амалга оширилган VPN маҳсулотлар унумдорлик нуткаи назаридан ихтисослаштирилган курилмадан колишисада, VPN-тармоқларни амалга оширилишида етарли кувватга эга. Таъкидлаш лозимки, масофадан фойдаланишда зарурӣ ўтказиш полосасига талаблар катта эмас. Шу сабабли, дастурий маҳсулотларнинг ўзи масофадан фойдаланиш учун етарли унумдорликни таъминлайди. Дастурий маҳсулотларнинг шубҳасиз афзаллиги-кўлланилишининг мославинувчанилиги ва қулайлиги хамда нархининг нисбатан юкори эмаслиги.

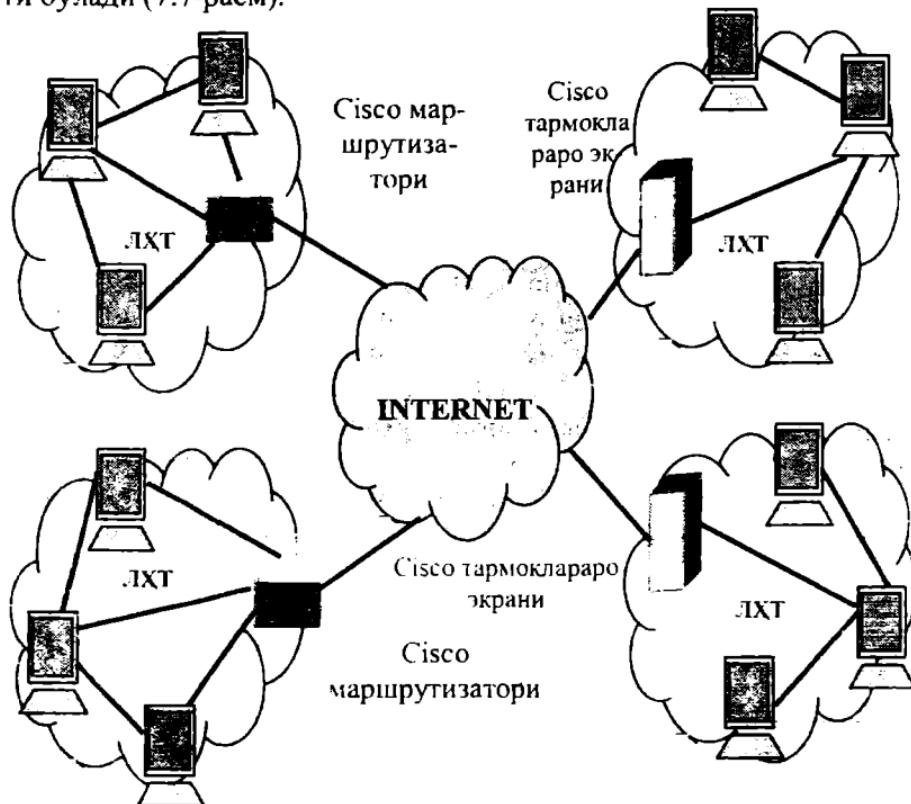
*Ихтисослаштирилган аппарат воситалари асосидаги VPN* Ихтисослаштирилган аппарат воситалари асосидаги VPNларнинг энси мухим афзаллиги унумдорлигининг юқорилигидир. Ихтисослаштирилган аппарат воситалари асосидаги VPN тизимларда шифрлашнинг микросхемаларда амалга оширилиши тезкорликнин таъминланишига сабаб бўлади. Ихтисослаштирилган VPN-курилмалар хавфсизликнин юкори даражасини таъминлайди, аммо уларнинг нархи анчагина юкори.

## **7.3. Химояланган корпоратив тармоқларни қуриш учун VPN ечимлар**

**Маршрутизаторлар асосидаги VPN.** Ташки дунё билан локал тармоқ алмашадиган барча ахборо машрутизатор оркали ўтади. Бу маршрутизаторларни чикувчи пакетларни шифрловчи ва киравчы пакетларни расшифровка килувчи габий платформага айлантиради. Бошкача 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 факат ҳам тармоқдан фойдаланиш бўйича, ҳам узатиладиган трафикни шифрлаш бўйича химоялаш вазифаларини биргаликда ҳал этувчи маршрутизатор ёрдамида ташкил этган ҳолларда маршрутизаторларни VPNни мададлашда ишлиатилиши айникса фойдалидир. Ушбу ечимнинг камчилиги маршрутлаш бўйича асосий амалларнинг кўп меҳнат сарфини талаб этувчи трафикни шифрлаш ва аутентификациялаш амаллари билан бирга олиб бориши натижасида маршрутизатор унумдорлигига кўйиладиган талабларнинг ошиши билан боғлик. Маршрутизаторларнинг унумдорлигини оширишга шифрлаш вазифаларини аппарат мададлаш оркали эришилади. Ҳозирда барча маршрутизатор ва бошка тармоқ курилмаларини етакчи ишлаб чиқарувчилари ўзларининг маҳсулотларида турли VPN-протоколларини мададлайдилар. Бу соҳада Cisco Systems ва 3Com компаниялари лидер хисобланадилар. Cisco Systems компанияси ўзлари ишлаб чиқкан маршрутизаторларга энг кенг таркалган стандартлар асосида VPNларни куришга имкон берувчи канал сатхи протоколини мададловчи IOS 11.3(Internetwork Operation System 11.3) ва тармоқ сатхи протоколи IPSесни киритди. L2F протоколи аввалтрок IOS операцион тизимнинг компонентига айланди ва Cisco ишлаб чиқарадиган барча тармоқлараро алоқа ва масофадан фойдаланиш курилматаридан маддланади.

Cisco маршрутизаторларида VPN вазифалари бутунлай ҳастурй йўл билан ёки шифрлаш сопроцессори бўлган маҳсус кенгайтириш платасидан фойдаланилган ҳолда амалга оширилиши мумкин. Охирги вариант VPN амалларида маршрутизатор унумдорлинин анчагина оширади. Cisco Systems компанияси томонидан иш-

лаб чиқилған VPN қуриш технологияси юкори унумдорлығи ва мосланувчанлиғи билан ажралиб туради. Үнда «тоза» ёки инкапсуляция килингандың күринишінде узатылувчи ҳар қандай IP-оким учун шифрлаш билан туннеллаш таъминланади. Cisco компаниясының маршрутизаторлари ассоциацияда VPN-каналларини қуриш операцион гизимининг воситалари ёрдамида Cisco IOS 12.x. версиясидан бош лаб амалга оширилади. Агар мазкур операцион тизим компания нинг бошқа бўлимларидаги Cisco чегара маршрутизаторларидан ўрнатилган бўлса, бир маршрутизатордан иккинчисига «сунгат нукта» туридаги виртуал химояланган туннеллар мажмуасида иборат бўлган корпоратив VPN тармокни шакллантириш имконияти бўлади (7.7-расм).



Маршрутлизаторлар асосида VPNларни куришда эсда тутиш лозимки, бундай ёндашишнинг ўзи компаниянинг умумий ахборот хавфсизлигини гаъминлаш муаммолини ҳал этмайди, чунки барча ички ахборот ресурслар барибир ташкаридан хужум қилиш учун очик қолади. Бу ресурсларни химоялаш учун, одатда, чегара маршрутлизаторларидан кейин жойлашган тармоқлараро экранлардан фойдаланилади.

Cisco 1720 VPN Access Router маршрутлизатори катта бўлмаган ва ўртacha корхоналарда химояланган фойдаланишини ташкил этишга аталган. Бу маршрутлизатор Internet ва интрапармоклардан фойдаланишини ташкил этишга зарур бўлган имкониятларни таъминлайди ва Cisco IOS дастурий таъминот асосидаги виртуал хусусий тармоқларни ташкил этиш вазифаларини мададлайди. Cisco IOS операцион тизими маълумотларни химоялаш, хизмат сифагини бошқариш ва юкори ишончилиликни таъминлаш бўйича VPN вазифаларининг жуда кенг тўпламини таъминлайди.

Cisco 1720 маршрутлизатори маълумотлар химоясинини куйидаги вазифаларини бажаради:

- *тармоқлараро экранлаш*. Cisco IOS Firewall компонента локал тармоқларни хужумлардан химоялайди. *Фойдаланишининг контексти назорати* CBAC (Context-based access control) функцияси маълумотларни динамик ёки холатларга асосланган, иловалар бўйича дифференциалланган фильтрлашни бажаради. Бу функция самарали тармоқлараро экранлаш учун жуда муҳим хисобланади. Cisco IOS Firewall компонента катор бошка фойдали вазифаларни ҳам, хусусан, «хизмат қилишдан воз кечиш» каби хужумларни аниклаш ва олдини олиш, Javaни блокировка этиш, аудит ва вактнинг реал масштабида огоҳлантиришларни тарқатиш вазифаларини бажаради;

- *шифрлаш*. IPSec протоколидаги DES ва Triple DES шифрлаш алгоритмларини мададлаш маълумотларни конфиденциаллиги ва яхлилтигини ва маълумотлар манбанин аутентификациялашни (маълумотлар глобал тармоқдан ўтганидан сўнг) таъминлаш максадида ишончли ва стандарт шифрлайди;

- *туннеллаш*. Туннеллашнинг IPSec, GRE (Generic Routing Encapsulation), L2F ва L2TP стандартлари ишлатилади. L2F ва L2TP стандартлари масофадаги фойдаланувчиларнинг корхона локал гармоғида ўрнатилган Cisco 1720 маршрутлизаторигача виртуал туннел ўтказгандарига ишлатилади. Бундай кўлланишда корхонада

масофадан фойдаланиши сертификацияга энгеж көлмайди ва шахарлараро ёки халқаро күнгироллар учун гүлови төсалади;

– курилмаларни аутентификациялаши ва калитларни бошкариши. IPSec катта тармоқларда маълумотлар ва курилмаларни масштабланувчи аутентификацияланни таъминловчи калитларни бошкариш протоколи IKE, ракамли сертификатлар X.509 версия 3. сертификатларни бошкарувчи протокол СЕР, хамда Verisign ва Entrust компанияи сертификат сервасрлари мададланади;

– *VPNning* шикоз дастурини таъминоти. IPSec ва L2TP протоколарининг стандарт версиялари билан ишловчи хар қандай миҷоз Cisco IOS билан ўзаро алоқа килиши мумкин;

– фойдаланувчиларни аутентификациялаши. Бунинг учун PAP, CHAP протоколлари, TACACS<sup>+</sup> ва RADIUS тизимлари, фойдаланиши токенлари каби воситалардан фойдаланилади.

Виртуал химояланган тармоқлар нафақат маълумотларни химоялаш, балки химоялашининг юқори савииси QoSни (Quality of Service) таъминлаши лозим. Cisco 1720 маршрутизатори QoSни куйидаги бошкариш механизмиларни мададлайди:

– фойдаланишининг келинисиган тезиги CAR (Committed Access Rate) иловалар ёки фойдаланувчилар базисида куйидаги учта муҳим вазифани бахаради:

- трафик турини туркумлайди;
- берилган иловага ружсат этилган ўтказиш қобилиятигини максимал даражасини ўрнатади;
- трафикнинг хар бир турни устуворлигини белгилайди;

– сиёсат асосида маршрутизация (Policy Routing) хам трафикни туркумлайди ва устуворлайди хамда трафикнинг қайси турини маршрутизаторнинг мос чиқиш йўли портига жўнатиш лозимлигини ҳал этади;

– цулоҳазали одилона наебат WFQ (Weighted Fair Queueing) трафикни хисобга олган ҳолда макбул жавоб вактини таъминлайди:

протокол RSVP иловаларга йўлнинг бошидан охиригача кафолатланган ўтказиш қобилиятини резервлашга имкон беради.

Маршрутизаторнинг мослашувчанини модулли конструкция ва иккита слотда ўрнатилувчи интерфейс WAN-карталари гўпчами оркали таъминланади. Cisco 1720 моделида Cisco 1600, 2800, ва 3600 моделларда ишлатиладиган WAN-карталардан фойдаланилади.

Компания 3Com VPN технологияны амалга ошырыпшида бошындан стандартларни күзгө туттган эдди VPN ни мададлаш учининг NetBuilder II, Super Stack II NetBuilder маршрутизаторларига Office Connect Net Builder Platform платформасында үрнатылған.

3Com компаниясы PPTP ва L2TP протоколдарни мададловчы масоғадан фойдаланытувчи концентраторларни йирик ишлаб чиқарувчиларидан биридир. 3Com компаниясининг VPN тармоклари IPSec билан биргә ишләтилади жаңы каталоглар, жумладан, Novell NDS ва Windows NT Directory Servicesлар билан ўзаро алоқа килиш учун ишлаб чиқылған.

Компания Web-технологияга асосланған ва VPN юкландырылған назоратлашга хамда юз берувчи ходисалар асосида статистика ва ахборотни йиғишига аталған дастурный илова Transcend Ware Secure VPN Manager ни хам ишлаб чысади. Ундан ташкари, 3Com криптохимояланған туннелларни осонгина яратышга имкон берувчи Web асосидаги инструментарийни ишлаб чиқаради.

Internet Devices компаниясининг Fort Knox маршрутизаторларыда тезлик ва күвват үйғунашылған. Үндагы тармокни химоялашни таъминлашта үйналтирилған IP-трафикни ишлеш вазифалари рўйхатининг кенглиги учининг афзаллигидир. Fort Knox маршрутизатори тармоклараро экран режимида ишләши, NAT стандарти бўйича манзилларни трансляциялаши, хавфсизлик сиёсатини бошқариши, Web-саҳифалар ва DNS жадвал ёзувларини көшлаши, аудитни баҗариши мумкин. Одатда, Fort Knox корпоратив тармок чегарасида, корпоратив тармокни глобал тармок билан уловчи маршрутизатордан кейин үрнатылади. Демак, у бошқа локал тармоклар билан VPN-алокани үрнатиш ва тармоклараро экранлар каби фойдаланишни назоратлашни турти қоидаларини шакллантириши мумкин. Fort Kloхда NAT манзилларини трансляциялаш функцияси мавжудлиги, унга ички IP-манзилларни беркитиш ва маршрутизаторлар трафигини кайта үйналтириш имконини беради. Бу корпоратив тармок маъмурларини VPNни куришда маршрутизаторларни янгидан конфигурациялашдан озод этади. Fort Kloх функциялари тўпламининг кенглигига карамай учининг нархи оддий маршрутизатор нархига генг.

**Тармоклараро экранлар асосидаги VPN.** Локал тармокнинг тармоклараро экранни орқали, худди маршрутизатордагидек, бутун трафик ўтади. Шу сабабли, тармоклараро экран хам чиқувчи трафикни шифрлаш, киравчы графикни расшифровка килиш вазифа-

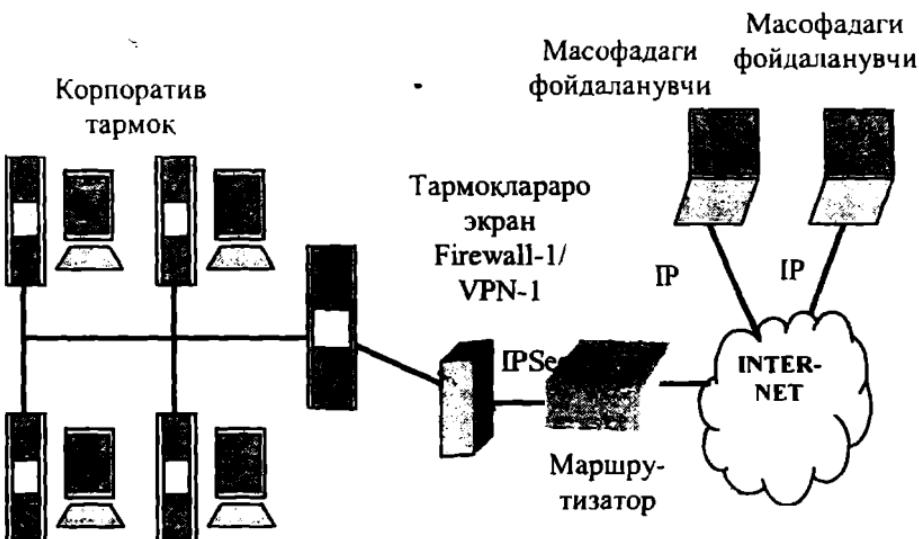
сини бажариши мумкин. Ҳозирди қатор VPN-ечимлар тармоклараро экранларни VPNнинг кўшимча мадад функциялари билан тўлдирилишига таянади. Бу Internet оркали бошка тармоклараро экранлар билан шифрланган уланишни ўрнатишга имкон беради. Ахборот хавфсизлиги бўйича қатор мутахассисларнинг фикрича VPNни тармоклараро экранлар асосида куриш, корпоратив тармокларни очик тармоклар ҳужумларидан комплекс химоялаш нуктаи назаридан, тўла асосланган ечимдир. Ҳакикатан тармоклараро экран ва VPN-шлюз функциялари бир нуктада, ягона бошқариш ва аудит тизими назоратида бирлаштирилса, корпоратив тармокни химоялаш функциялари битта курилмада тўпланади. На тижада, химоя воситаларини маъмурлаш сифати ошади.

Аммо, химоялаш воситаларининг бундай универсаллаштирилиши, хисоблаш воситаларининг мавжуд имкониятлари даражаси да нафақат ижобий, балки салбий томонига ҳам эга. Шифрлаш ва аутентификациянш амалларини хисоблаш мураккаблиги тармоклараро экран учун анъанавий бўлган пакетларни фильтраш амалларига нисбаган анча юкори. Шу сабабли, VPNнинг кўшимча ва-зифаларини амалга оширишда мураккаблиги катта бўлмаган амалларни бажаришга мўлжалланган тармоклараро экран кўпинча се-ракли унумдорликни таъминламайди. Корпоратив тармок тезкоғи-канал оркали очик тармокка уланганида сифатли химояни таъминлаш учун алоҳида аппарат, дастурний ёки комбинациянланган курияма кўринишидаги VPN-шлюздан фойдаланиш лозим.

Аксарият тармоклараро экранлар сервер дастурий таъминоти дан иборат, шу сабабли унумдорликни ошириш муаммоси юкори унумдорликка эга бўлган компьютер платформасидан фойдаланиш эвазига ечилиши мумкин.

Check Point Software Technologies компанияси Internet билан ишлаганда ахборот хавфсизлгини комплексе таъминлаш маҳсулотларини ишлаб чиқариш соҳасидаги стакчилардан бири хисобланади. Check Point Fire Wall-1 тармоклараро экран корпоратив ахборот ресурслари учун ягона комплекс доирасида химоянинг чукур эшелонланган чегарасини куришга имкон беради. Бундай комплекс гаркибига Check Point FW-1 нинг ўзи ва корпоратив VPN тармок (химояланган туннелларни шакллантирувчи кисм тизим) куриш учун маҳсулотлар тўплами Check Point VPN-1 ҳамда сукилиб киришни пайкаш воситалари Flood Gate ва x. киради.

Дастурий таъминотлар Check Point Fire Wall-1/VPN-1 асосида корпоратив тармок 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 кисм тизим таркибидаги барча маҳсулотлар хам ўзаро, хам оммавий брандмауэр Fire Wall-1 билан узвий интегрияланган. Check Point компанияси «тармок-тармок» (VPN-1 Gateway) ва «тармок-масофадаги фойдаланувчи» (VPN-1 Gateway+VPN-1 Secu Remote) типидаги химояланган тармоқларни ташкил этиш учун воситаларни тақдим этади.

Check Point VPN-1 маҳсулотлари очик стандартлар (IPSec) асосида амалга оширилган, фойдаланувчиларни аутентификациялашнинг ривожланган тизимиға эга, очик калитларни (PKI) тақсимлашнинг ташки тизимлари билан ўзаро алоқани мададлайди, бошқариш ва аудитнинг марказлаштирилган тизимини куришга имкон беради ва ҳ.

Check Point Fire Wall-1/VPN-1 нафакат очик, балки криптохимояланган трафикни хам назоратлайди. Тармоқлараро экран FW-1га келган маълумотлар VP-1 воситалари ёрдамида расшифровка килинади, сўнгра ахборотлар пакети яна шифрланади ва ўтказиб юборилади.

VPN-1 қисм тизими трафикни нафакат криптографик беркитади, балки ахборотлар пакетини аутентификациялади ҳам. Check Point Fire Wall-1/VPN-1 каналларида трафикни шифрлашда машхур DES, 3-Des, CAST, IDEA, FWZ1 ва х. критоалгоритмлардан 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 тармоқларо экран Fire Wall – 1 билан узвий интеграцияланган. Бу маҳсулот корхонага узатилувчи маълумотларнинг тўла конфиденциаллигини, аутентификацияланганлиги ва яхлитлигини кафолатлаган ҳолда Internet орқали алоқа каналларини куришга имкон беради. VPN функциялари корхонанинг умумий ҳавфсизлик сиёсатига тўла интеграцияланганлиги сабабли, брандмаузер ва VPN-маҳсулотларни алоҳида бошқаришга эҳтиёж колмайди.

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 оркасидаги оддий хостлар груҳи бўлиши мумкин. Бу маълумотлар тармоқнинг оммавий қисми бўйича шифрланган кўринишда узатилади, ички тармоқ бўйича узатилганда шифрланмайди. VPN-амалларининг барчаси охирги фойдаланувчи ва барча иловалар учун шаффоғдир.

VPN-1 Gateway шлюзи шифрлашнинг бир неча алгоритмини ва бир неча калитларни бошқариш протоколини мададлайди. Бу шлюз IKE (Internet Key Exchange) каби индустрисал стандарт VPN-протоколларни мададлаши сабабли, экстратармоқларни ташкил этишда қўллаш қуляй хисобланади. Экстратармоқларда VPN бизнес-шериклар орасида ҳавфсиз алоқани таъминлайди. Check Point компаниясининг VPN-маҳсулотлари IKE стандартига амал килади. Шу сабабли улар карши томон билан музокараплар жараёнида автоматик тарзда шифрлашнинг энг криптобардош алгоритмини (DES ва Triple DES) ва аутентификациялашнинг энг катъий алгоритмини (SHA-1 ва MD5) танлайди. Ундан ташқари, шифрлашнинг маҳфий калитлари, максимал химояланишни кафолатлаган ҳолда, тез-тез янгиланади.

VPN-1 Gateway шлюзи виртуал хусусий тармокдаги иккита охирги узелларга ҳам шифрланган, ҳам шифрланмаган маълумотларни алмашишга имкон берувчи шифрлашнинг танлов режимини мададлайди. Бунинг учун тармок маъмури трафиги учун химояланганинг 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 қалитларни бошқаришнинг қуидаги механизмларини мададлайди: IPSec учун стандарт бўлган IKE, қалитларни бошқаришнинг саноат стандарти FWZ, оммавий протокол SKIP ва қалитларни кўл билан тарқатиладиган усули. У X.509 сертификатлари ва Entrus Technologies компаниясининг сертификатлар серверлари технологияси асосида очик PKI қалитларни бошқариш инфратузилмасини мададлайди.

VPN-1 Secu Remote мижоз дастурий таъминоти VPN-1 Gateway Шлюзи ёрдамида «тармок-масофадаги фойдаланувчи» хилидаги химояланган уланишларни ташкил этишда ишлатилади. Windows 98/XP/NT/2000 бошқарувида ишловчи масофадаги компьютерларга VPN-1 Secu Remotенинг ўрнатилиши мобил ходимларнинг ёки телекомпьютерларнинг корхона бош тармоғи билан Internet орқали химояланган боғланишини таъминлайди. VPN-1 Secu Remotенинг маълумотларни OSI моделининг тармок сатҳида шифрлаши ва расшифровка килиши ушбу амалларнинг барча иловалар учун шаффоғлигини, мавжуд иловаларга ўзгартириш киритишни талаб қилмаган холда, таъминлайди. SecuRemote фойдаланувчиларга VPN-воситалар ўрнатилган бир неча турли тармоқлар билан боғланишига имкон беради.

VPN-1 Accelerator Card қурилмаси Chrysalis-ITS компанияси томонидан иштаб чиқилган аппарат криптографик теззлатгичdir. VPNнинг химояланган каналларида трафикни шифрлаш ва қалитларни генсерацияловчи амаллар анчагина хисоблаш мураккаблигига эга ва VPN орқали узатилувчи трафикнинг ҳажми ошган сари компьютернинг процессори ва хотирасининг хаддан ортиқ юкланиши рўй бериши мумкин. VPN-1 Accelerator маҳсулоти бу муаммони хал этиши мумкин.

VPN-1 Accelerator Card теззлатгичи VPN-1 Gateway шлюзи билан биргаликда ишлашга аталган ва IKE ва IPSeclар талаб этадиган

барча криптографик амалларни бажаради. VPN-1 Accelerator Card бевосита шлюз орқали маъмурланади.

VPN функциялари ўрнатилган SecureZone тармоклараро экранни Secure Computing компанияси томонидан ишлаб чиқилган ва асосий характеристикалари куйидаги:

- VPNни мададлаш функциялари – IPSec стандартги, DES ва Triple DES, PKI бошқариш ва Netscape, Entrust ва Verisign компаниялардан X.509 сертификатлари;

- ихтисослаштирилган операцион тизими Secure OS (Unixнинг химояланган варианти) бошкарувида ишлайди;

- куйидагиларни каноатлантирувчи аппарат платформалар: процессор Intel Pentium, Pentium Pro, ёки Pentium II; RAM-камида 64Мбайт; ташки курилмалар қаттиқ диск 4 Гбайт SCSI-2, кайишкок дисклар 3,5, CO KOM, стриммер DAT; SVGA video, PS/2- билан бирга ишлай олувчи сичкон;

- стандарт тармок интерфейслари: 2-4 Ethernet, FAST Ethernet, Token Ring ёки FDDI;

- бузилишга бардошлик хоссасига эга.

Secure Computing компанияси MicroSoft Windows мухитида ишловчи, алохидা 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 тармоклараро экранни Axent Technologies компанияси томонидан ишлаб чиқилган ва Eagle Firewallнинг модификацияланган маҳсулоти хисобланади. Бу тармоклараро экраннинг характеристикалари куйидаги:

- VPN мадади тармоклараро экранга ўрнатилган;

- IPSec стандарти мададланади, дастурий шифрлаш IP (текин таркатилувчи шифрлаш усули swIPe);

- хавфсизликнинг умумий сиёсати тармоклараро экран функцияларига ва VPN функцияси ёрдамида туннелланувчи трафикка гааллукли;

- Windows NT/2000 ва Solaris операцион тизимлар бошкарувида ишлайди.

Axent компанияси масофадаги фойдаланувчилар учун VPNнинг мижоз дастурий таъминотини ҳам такдим 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 экранни учун, ушбу тармоклараро экран мухитида узвий интеграцияланувчи, кўшимча дастурий маҳсулот хисобланади.

IPSec протоколига асосланган Gauntlet Global VPN кисм тизими трафикни криптографик химоялашнинг куйидаги иккита режимини мададлайди:

- Smart Gate шлюзлари ёрдамида амалга оширилувчи тармоклараро экрандан тармоклараро экрангача;
- масофадаги мижоз дастурий таъминоти Gauntlet PC Extender ёрдамида амалга оширилувчи тармоклараро экрандан масофадаги фойдаланувчи компььютеригача.

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 ракамли сертификатларни генерациялаши ва текшириши мумкин.

VPN куриш функциясини мададловчи BorderManager тармоклараро экранни Novell компаниясининг маҳсулоти бўлиб, нафака! VPN куриш имкониятини, балки фойдаланишни чегаралашни, пакетларни фильтрлаш ва тармок манзилларини трансляциялашни таъминлайди, воситачи HTTPнинг хизматларини тавсия этади, Web сахифаларини кешилайди, 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 таксимоти RSA криптотизими ва Диффи-Хелман алгоритми бўйича амалга оширилади. Ахборот пакетларини криптографик беркитиш ва аутентификациялаша RC2 ва RSA криптотизимлардан фойдаланиллади. Border Managerнинг бир версиясида IPSec протоколи мададланади. Border Manager тармоклараро экран асосида қурилган химояланган виртуал тармокларда браузерлардан бирининг асосий бўлиши, бошқариш маркази ролини бажариши лозим.

## *Ихтисослаштирилган дастурий таъминот асосидаги VPN.*

VPN куришда ихтисослаштирилган дастурий воситалар кенг кўлланилади. VPN куришнинг дастурий воситалари химояланган туннелларни факат дастурий шакллантиришга имкон беради ва улар ишлайдиган компьютерни TCP/IP маршрутизаторига айлантиради. Бу маршрутизатор шифрланган пакетларни қабул килади, расшифровка килади ва локал тармок оркали тайинланган нуктага узатади. Охирги вактда 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 қурилмалардан колишсада, дастурий маҳсулотлар масофадаги фойдаланувчиларга етарли унумдорликни осонгина таъминлайди. Дастурий маҳсулотларнинг шубҳасиз афзалиги ишлатилишида мосланувчанилиги ва кулагилиги ҳамда нисбатан юкори бўлмаган нархидир. Аппарат шлюзларни ишлаб чиқарувчи кўпгина компанииялар (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 варианти-химояланган канал протоколи PPTPни (Point-to-Point Tunneling Protocol) ўрнатилиши эвазига VPN технологияни мададлайди. Трафикни туннеллаш очик IP-тармок бўйича узатиладиган стандарт PPP- фреймларни IP-датаграммаларга инкапсуляциялаш ва кейин шифрлаш оркали амалга оширилади.

RASнинг асосий афзалиги – тежамлилиги, камчилиги – унумдорлигининг пастилиги. Ҳозирда бу маҳсулотнинг такомиллаштирилган версияси – RRAS (Routing and Remote Acces Service) пайдо бўлди. RRAS таркибидаги такомиллаштирилган дастурий кўп протоколи маршрутизатор маршрутлашнинг RIP (Routing Information Protocol) ва OSPF (Open Shortest Path First) протоколларини мададлайди. RRASнинг бу хусусиятлари ундан VPN шлюзи каби «тармок-тармок» 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 тармоклар 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 халкаро версияси RC4 алгоритми бўйича шифрлашда 56 ёки 40 битли калитлардан фойдаланади. Маълумотларни аутентификациялаш ва яхлитлигини таъминлаш учун MD5 ҳэш-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 мухитда Alta Vista Tunnel Server маҳсулоти бир вактнинг ўзида 200 туннел уланишларини, UNIX операцион мухитда эса 2000 гача туннел уланишларни мададлайди.

***Ихтисослаштирилган аппарат воситалари асосидаги VPN.*** Ихтисослаштирилган аппарат курилмалари асосидаги VPN-воситаларнинг асосий афзаллиги-юкори унумдорлиги. VPN-пакетларни ишлашда керакли хисоблашлар хажми оддий пакетларни ишлашдагига нисбатан 50–100 марта ошади. Аппарат воситалари асосидаги VPNларда юкори тезликка уларда шифрлашнинг ихтисослаштирилган микросхемаларда амалга оширилиши эвазига эришиллади. Бундай VPN-воситалар кўпинча IPSec протоколи билан

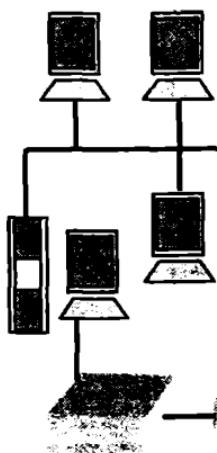
бирга ишлай олади ва локал тармоқлар орасида криптохимояланган туннелларни шакллантиришда ишлатилади. Баъзи ишлаб чикарувчиларнинг VPNни шакллантирувчи асбоб-ускуналари бир вактнинг ўзида «масофадаги компьютер-локал тармок» режимида химояланган боғланишни ҳам мададлайди.

Аппарат VPN-шлюзлар алоҳида аппарат курилмаси кўринишида бўлади. Уларнинг асосий вазифаси -- трафикни юқори унумдорлик билан шифрлаш. Бу VPN-шлюзлар X.509 ракамли сертификатлари PKI очик қалитларни бошқариш инфратузилмалари билан ишлайди, LDAP бўйича маълумот берадиган хизматлар билан ишлашни мададлайди.

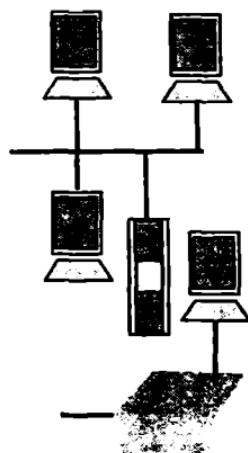
Аппарат химояланган туннел ишлашининг энг оддий варианти - аппарат шифрлашдан фойдаланиб уланишларни яратиш. Туннеллашнинг аппарат воситалари одатда, локал ва глобал тармоқларнинг туташган жойида, маршрутизатордан кейин ўрнатилади (7.9-расм) ва автоматик тарзда берилган трафикни шифрлайди. Бундай ёндашишнинг асосий афзаллиги шундаки, ишчи станциялар ва маршрутизаторларнинг шакллантирилувчи криптотуннеллар билан хеч қандай боғликлиги йўқ, VPN ўрнатилганида уларни конфигурациясини ўзгартириш талаб этилмайди.

Аппарат шлюзларни инсталляциялаш дастурий шлюзлар ва маршрутизаторлар ва брандмауэрлар асосидаги шлюзларга нисбатан жуда осон амалга оширилади. Бундай курилмаларни бошқариш иккита асосий масалани ечишини талаб этади: сертификация маркази орқали қалинларни бошқаруви ва хамонаден туннеллашни бошқарини. Аксёрнинг аниқларни туннелларни язарича сертификация марказлари Windowsла московланадиган турли клиентларни. Аппарат туннелларини марказлашган холда битта иш жойида туриб бошқариш мумкин. Бошқарувчи дастурлар туннелнинг асосий химоялаш функцияларининг бажарилишини ва хатоликларни ишлашни таъминлайди.

Локал тармок



Локал тармок



Маршрутизатор

INTERNET

Криптотуннель

Туннеллашнинг  
аппарат  
воситалари

Маршрутизатор

7.9-расм. Ихтисослаштирилган аппарат воситалар асосида туннеллаш схемаси.

Ихтисослаштирилган аппарат VPN-воситалар нархидан ташкари барча бўлиши мумкин бўлган кўрсаткичлари бўйича етакчи хисобланади.

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 интрапартмок ва экстрапартмокларни қуриш учун тўлиқ счим хисобланади. PERMIT Enterprise мавжуд тармокларда тармок ва охирги фойдаланувчи унумдорлигига жиддий тъйсир килмаган холда, осонгина сафланади, унинг масштабланувчи архитектураси бирнеча VPNларни яратиш ва уларни бошқариш имкониятини беради.

Компания томонидан шлюзнинг қуидаги тўртта модификацияси тақдим этилади:

– PERMIT/Gate 1520 нархи қиммат бўлмаган автоном курилма бўлиб, қувватли телекомпьютерлар ёки SOHO синфидағи катта бўлмаган масофадаги оғислар учун ишлатилади;

– PERMIT/Gate 2520 ва PERMIT/Gate 4520 ўтказиш қобилияти, мос холда 4 ва 1- Мбит/с, бўлинмалар оғислари ва кичик локал хисоблаш тармоқларига мўлжалланган, масофадаги юзлаб фойдаланувчиларни мададлайди;

– PERMIT/Gate 7520 (70 Мбит/с) ички локал хисоблаш тармоқларида ишлатилади ва масофадаги минглаб фойдаланувчиларни мададлайди.

PERMIT/Gate шлюзларининг муҳим афзаллиги – трафик ишланишининг юкори унумдорлигини таъминлш максадида DES ва 3-DES шифрлаш алгоритмининг аппарат амалга оширилиши.

PERMIT/Gate7520 шлюзи IPSecнинг амалга оширилишининг аппарат воситаси билан ҳам жихозланганлиги, унумдорликка таъсир қилмаган холда минглаб VPN уланишларни мададлашга имкон беради. Бу, зарурят 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. бошкарувида ишловчи алоҳида ишчи станция томонидан манзилланган тармоқ трафигини химоялади.

PERMIT/Gate шлюзларининг ҳар бири дастурли утилита PERMIT/Config билан бирга тақдим этилади. Бу дастурли утилита виртуал хусусий тармоқнинг ҳар кандай нуктасидан бир неча шлюзларнинг дастурий таъминотини масофадан конфигурациялаш, бошқариш ва модификациялашга имкон яратади.

VPNNet компанияси VPN куриш учун дастлабки интеграцияланган счимлардан бири – VPNwareни таклиф этди. Бу ечим ўз ичига куйндаги маҳсулотларни олади:

– учта VPN-шлюз: штаб қароргоҳи ва йирик локал тармоқлар учун VSU-1100, бўлинмалар учун VSU-1010 ва катта бўлмаган оғислар учун VSU-10;

– iPass компаниясидан дастурний сервер RoamServer;

– мижоз дастурний таъминоти VPNremote;

– бошқаришнинг дастурний тизими VPNmanager.

VPNNet асбоб-ускуналари, «тармок-тармок» ва «тармок – масофадаги фойдаланувчи» хилидаги уланишларга мўлжалланган VPNни мададлайди. Ишлатиладиган маҳсулотларга боғлик холда VPNware тизими IPSecнинг стандарт амалга оширилиши ёрдамида оммавий IP тармок орқали узатилаётган маълумотларни химоялаш билан 25дан 5000тacha фойдаланувчиларни мададлаши мумкин. Бу тизим турли масштабли тармокларда 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 кодисаларни кайдлашга имкон беради. Хар хил VPNларни бошқаришни марказлаштириш эвазига химояни бошқаришнинг бошка функцияларини соддалаштириш ва марказлаштириш, масалан, корпоратив брданмауэр яхлитлигини бузилишини назоратини таъминлаш мумкин. VPNei маҳсулотларининг афзаллиги-мавжуд тармок билан интеграцияланишининг соддалиги, унумдорлигининг нисбатан юкорилиги ва IPSecнинг тўла амалга оширилиши.

Мижоз дастурий таъминоти VPNremote IPSec протоколини мададлайди ва Windows NT мухитида хамда телефон тармоклари орқали фойдаланилганда масофадаги ва мобил фойдаланувчилар, телекомпьютерлар ва бизнес-шерикларнинг маълумотларини химоялашда Windows95/98/XP мухитида ишлайди.

Бошқарув тизими VPNmanager виртуал хусусий тармокларни яратиш, конфигурациялаш ва бошқариш учун маҳсус ишлаб чиқилган. Тармок маъмури ушбу тизим ёрдамида, график интерфейсни ишлатиб масофадаги фойдаланувчиларни ва бизнес-шерикларни VPNга осонгина кўшиши мумкин. VPN мижозларини масофадан маъмурлашга Dyna-Policy функцияси атаган.

LanRover VPN Gateway шлюзи Shiva компанияси томонидан тақдим этилган бўлиб, ICSA томонидан сертификацияланган. Бу шлюз очик тармок орқали узатиладиган маълумотларни химоялаш технологияларининг кенг тўпламини мададлайди. Яхлитликни ва конфиденциалликни таъминлаш, фойдаланишининг 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 иктинослаштирилган интеграл схемаларнинг тезкорлиги ва реал вактнинг кўп вазифали операцион тизим реактивлигининг ноёб бирикмасидан фойдаланади. Бу шлюзлар ишлатишда кулай ва уларнинг ишлаши охирги фойдаланувчилар учун шаффоф. Бу шлюзлар билан ишлаш кулагигини таъминлаш максадида график фойдаланувчи интерфейсли утилита VPN manager тақдим этилади. Бу утилита маъмурга ҳар кандай Windows 95/NT тизимидан бирданига бир неча шлюзларни бошкаришни таъминлайди.

#### **7.4. Канал ва сеанс сатҳларда ҳимояланган виртуал каналларни куриш**

*Канал сатҳида ҳимояланган виртуал каналларни шакллантириши протоколлари.*

PPTP, L2F ва L2TP протоколлар OSI модели канал сатхининг туннеллаш протоколлари хисобланади. Ушбу протоколларнинг умумий ҳусусияти шундан иборатки, улар очик тармоқ, масалан, Internet оркали корпоратив тармоқ ресурсларидан ҳимояланган кўп протоколли масофадан фойдаланишни ташкил этишда ишлатилади. Учала протоколни, одатда, ҳимояланган канални шакллантириш протоколларига мансуб деб хисоблайдилар. Аммо бу таърифга узатиладиган маълумотларни туннеллашни ва шифрлашни таъминловчи факат PPTP протоколи аник мос келади, чунки L2F ва L2TP протоколлар факат туннеллаш функцияларини мададлайди. Туннелланган маълумотларни ҳимоялаш (шифрлаш, яхлитлик, аутентификация) учун бу протоколларда қўшимча, протокол, ҳусусан, IPSec протоколи ишлатилади.

PPTP протоколи маълумотларни IP, IPX ва NetBEUI протоколлари бўйича алмашиш учун ҳимояланган каналларни яратишга имкон беради. Ушбу протоколлар маълумотлари PPP кадрларига жойланади ва сўнгра PPTP протоколи воситасида IP протоколининг пакетларига инкапсуляцияланади ва шу протокол ёрдамида шифрланган кўринишида ҳар кандай TCP/IP тармоғи оркали ташилади.

PPP сессияси доирасида узатилувчи пакетлар күйидаги тузилмага эга (7.10-расм):

- Internet ичидә ишлатилувчи канал сатхининг сарлавҳаси, ма-салан, Ethernet кадрининг сарлавҳаси;
- таркибида пакетни жўнатувчи ва кабул килувчи манзиллари бўлган IP сарлавҳаси;
- маршрутлаш учун инкапсуляциялашнинг умумий усулининг сарлавҳаси GRE(Generic Routing Encapsulation);
- таркибида IP, IPX ёки NetBEUI пакетлари бўлган дастлабки пакет PPP.

Узатила- диган кадр сар- лавҳаси	IP – сар- лавҳа	GRE – сар- лавҳа	PPP – сар- лавҳа	Шифрлан- ган маълу- мотлар PPP	Узати- ладиган кадр охири
---	-----------------------	------------------------	------------------------	--------------------------------------	------------------------------------

7.10-расм. PPTP туннели бўйича жўнатилади пакет тузилмаси.

Тармоқнинг кабул килувчи 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 таалуқли), уларнинг янада юкорирок сатхнинг химояланган канал протоколларидан афзалигидир. Масалан, агар корпоратив тармоқда IPX ёки NetBEUI ишлатилса, IPSec ёки SSL протоколларини ишлатиб бўлмайди, чунки улар IP тармоқ сатхининг факат битта протоколига мўлжалланган.

Инкапсуляциялашнинг мазкур усули OSI моделининг тармоқ сатҳи протоколларига боғлик бўлмасликни таъминлайди ва очик IP-тармоқлар орқали ҳар кандай 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 фойдаланувчани аутентификациациялашда PPP учун кўлланиладиган турли протоколлардан фойдаланиш мумкин. Microsoft компанияси томонидан Windows 98/XP/NT/2000 га киритилган PPTРнинг амалга оширилишида аутентификациациялашнинг кўйидаги протоколлари мададланади: парол бўйича аниклаш протоколи PAP(Pasword Authentication Protocol), кўл беришиша аниклаш протоколи MSCHAP (Microsoft Challenge – Handshaking Authentication Protocols) ва аниклаш протоколи EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). PAP протоколидан фойдаланилганда идентификаторлар ва пароллар алокা линиялари оркали шифрланмаган кўринишда узатилади, бунда аутентификациациялашни факат сервер ўтказади. MSCHAP ва EAP-TLS протоколларидан фойдаланилганда нияти бузук одамнинг ушлаб колинган шифрланган паролли пакетдан кайта фойдаланишидан химоялаш ва мижоз ва VPN-серверни аутентификациациялаш таъминланади.

PPTP ёрдамида шифрлаш Internet оркали жўнатишда маълумотлардан хеч ким фойдалана олмаслигини кафолатлайди. Шифрлаш протоколи MPPE (Microsoft Point-to-Point Encryption) факат 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 қийматини ўзгартиради. MMPE протоколи «нукта-нукта» хипидаги алока каналлари учун ишлаб чиқилган бўлиб, бу алока ка-

налларида пакетлар кетма-кет узатилади ва маълумотлар йўқотилиши жуда кам. Бу вазиятда навбатдаги пакет учун калит киймати олдинги пакетнинг расшифровкаси натижасига боғлик. Умумфойдаланувчи тармок орқали виртуал тармок куришда бу шартларга риоя килиш мумкин эмас, чунки маълумотлар пакети кўпинча кабул килувчига жўнатилган кетма-кетликда келмайди. Шунинг учун PPTP шифрлаш калитини ўзгартиришда пакетларнинг тартиб ракамидан фойдаланади. Бу расшифровка килишни олдинги кабул килинган пакетларга боғлик бўлмаган ҳолда амалга оширишга имкон беради.

PPTP протоколи учун қўллашнинг кўйидаги 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.

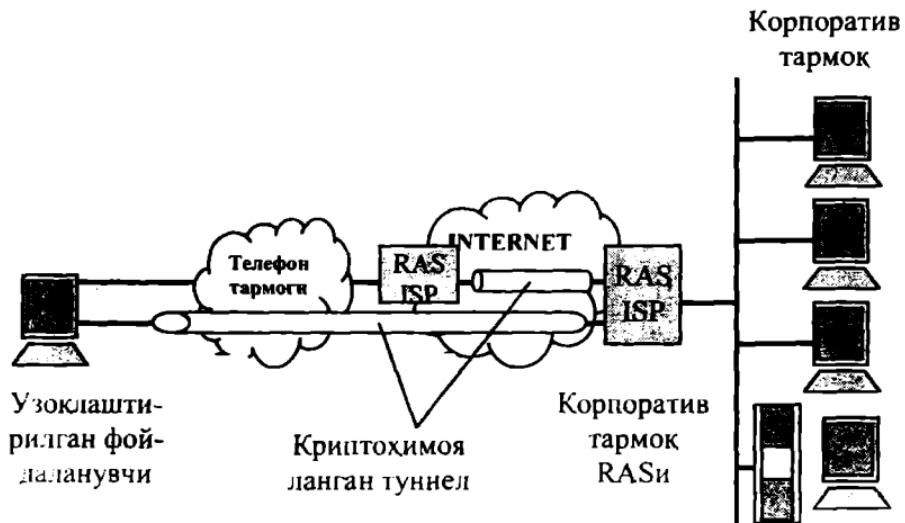
Туннеллашнинг биринчи схемаси амалга оширилганида (7.12-расм) масофадан фойдаланувчи Windows 98/XP/NT таркибидағи масофадан фойдаланиш сервиси RAS (Remote Access Service)нинг мижоз кисми ёрдамида локал тармок билан масофавий боғланишни ўрнатади. Сўнгра фойдаланувчи локал тармоқдан масофадан фойдаланиш серверига, унинг IP манзилини кўрсатиб мурожаат этади ва у билан PPTP 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 компьютерида Windows 98/XP/NT таркибидағи RAS сервернинг мижоз кисми ва PPTPнинг драйвери, масофадан фойдаланувчи локал тармоғининг серверида эса Windows NT Server таркибидағи RAS сервери ва PPTP драйвери ўрнатилиши шарт. PPTP протоколи ўзаро алоқадаги томонлар алмашадиган бир нечта хизматчи хабарни аниклади. Хизматчи хабарлар TCP протоколи бўйича узатилади. Муваффакиятли аутентификациялашдан сўнг химояланган алмашиб жараёни бошланади. Локал тармоқнинг ички серверлари PPTP протоколини мададламаслиги мумкин, чунки чегара маршрутизатор IP пакетлардан PPP кадрларини чиқариб олиб уларни локал тармоқ оркали керакли IP, IPX ёки NetBIOS форматида жўнатади.

Масофадаги компьютерни Internetra телефон линияси бўйича провайдер ISP (Internet Service Provider) оркали улашда туннеллаш схемасининг иккита варианти бўлиши мумкин (7.13-расм).



7.13-расм. Масофадан фойдаланувчи компьютерини ISP провайдери оркали телефон линиясидан фойдаланиб Internetra уланишини туннеллаш схемасининг иккита варианти.

Схеманинг биринчи вариангининг қурилиши протокол PPTPнинг провайдер ISPнинг масофадан фойдаланиш сервери ва чегара корпоратив маршрутизатор оркали мададланиши таҳминига

асосланган. Сервер одатда, фойдаланувчиларнинг уланишини таъминловчи кўп сонли тезкорлиги наст портларга эга. Провайдер ISPнинг сервери RAS ва маршрутизатор орасида химояланган канал ҳосил бўлади. Моҳияти бўйича бу - «шлюз-шлюз» хилидаги химояланган канал варианти.

Бу вариантда масофадан фойдаланувчининг компьютери 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 хисоб маълумотлари базасидан маршрутизаторнинг IP-манзилини топади. Бу маршрутизатор чегара маршрутизатори ва ушбу фойдаланувчининг локал тармоқдан масофадан фойдаланиш сервери хисобланади. Бу маршрутизатор билан провайдер сервери RAS IntreNet орқали PPTP протоколи бўйича сессия ўтказади. Провайдернинг сервери RAS локал гармоқдан масофадан фойдаланиш серверига фойдаланувчининг идентификаторини ва бошқа маълумотларни узатади. Улар асосида бу сервер CHAP протоколи бўйича фойдаланувчини яна аутентификациялаиди. Агар фойдаланувчи иккинчи аутентификациялашдан (бу унинг учун шаффоф бўлади) муваффакиятли ўтса, провайдернинг RASи бу тўғрида фойдаланувчини PPP протокол бўйича огохлантиради ва сўнгра, провайдернинг масофадан фойдаланувчи сервери ва локал тармоқ орасида химояланган виртуал канал шакланади.

Масофадан фойдаланувчининг компьютери локал тармок IP, IPX, ёки NetBIOS билан ўзаро алока пакетларини PPP кадрларига жойлаб провайдернинг масофадан фойдаланувчи сервери RASiga узатади. Провайдернинг RASи аталган манзил сифатида чегара маршрутизатори манзилини, манба манзили сифатида ўзининг шахсий IP-манзилини кўрсатган холда PPP кадрларининг IP пакетларга инкапсуляциясини амалга оширади. Провайдернинг масофадан фойдаланувчи сервери ва локал тармок орасида узатишга аталган PPP пакетлари симметрик шифрда шифрланади. Бунда симметрик маҳфий калит сифатида CHAP прогоколи бўйича аутентификациялаш учун провайдер RASининг хисоб маълумотлари базасида сакланувчи фойдаланувчи паролининг дайджести ишлатилади. Симметрик шифрлаш алгоритмлари сифатида DES ёки RC-4 алгоритм ишлатилади.

Тавсиф этилган вариант кенг тарқалмади, чунки протокол PPTP, асосан, Microsoft компаниясининг маҳсулотларида – RAS Windows NT 4.0 нинг мижоз ва сервер кисмларида ҳамда RAS Windows 98/ХРнинг мижоз қисмида амалга оширилган. Провайдерлар масофадан фойдаланиш сервери сифатида одатда RAS Windows NTга нисбатан кувватлироқ воситалардан фойдаланади. Бунда протокол PPTP Internet провайдерларининг масофадан фойдаланиш серверлари RAS орқали доимо мададланмайди. Ундан ташкари, бу схемада маълумотлар фойдаланувчи компьютери ва Intrenet провайдери орасида химояланмаган ҳолда узатилади, натижада, унинг хавфсизлиги жиддий ёмонлашади.

Microsoft компанияси томонидан PPTP протоколини кўллашнинг яна бир бошқа схемаси тавсия этилган. Бу схемага биноан PPTP протоколининг провайдернинг масофадан фойдаланиш сервери томонидан мададланиши талаб этилмайди. Туннеллашнинг бу варианти (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 яратиш мумкин.

Ушбу схемага биноан фойдаланувчи икки марта масофадан уланишини ўрнатиши лозим. Биринчи марта фойдаланувчи провайдернинг масофадан фойдаланиш серверига модем бўйича қўнгирок килиб, PPP протоколи бўйича у билан алока ўрнатади ва провайдер ISP томонидан мададланувчи протоколларнинг бирига (PAP ёки CHAP) ёки терминал диалогига мувофик аутентификациядан ўтади. ISP провайдерида аутентификациядан муваффакиятли ўтганидан сўнг фойдаланувчи локал тармоқдан масофадан фойдаланиш сервери билан, унинг IP-манзилини кўрсатиб уланишини ўрнатади. Натижада, масофадаги компьютер ва локал тармоқ RAS орасида PPTP протоколи бўйича сессия ўрнагилади. Мижоз яна, инди ўзининг корпоратив тармоғи серверида аутентификацияланади. Масофадан фойдаланиш сервери фойдаланувчининг ҳакикийигини ўзининг хисоб маълумотлари базаси асосида текширади. Муваффакиятли 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, маддадлаш ва узиш учун аталган. Бошқарувчи хабарларни алмашиш мижоз ва PPTPнинг сервери орасида ўрнатилувчи TCP-уланиш бўйича амалга оширилади. Бу уланиш бўйича узатиладиган пакетларда канал сатҳи 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 моделлининг канал сатҳида химояланган виртуал тармок куриш учун, PPTP протоколига альтернатива сифатида ишлаб чиқилган. L2F протоколи турли тармок протоколлари томонидан маддадланиши билан ажralиб турди ва Internet провайдерлари учун фойдаланишда анча қулай. L2F протоколи масофадаги фойдаланувчи компьютери билан провайдер сервери алокасини ташкил этишда масофадан фойдаланишнинг турли протоколларини (PPP, SLIP ва х.) ишлатишга йўл қуяди. Туннел оркали пакетларни ташишда ишлатилувчи очик тармок IP протоколи асосида ва бошка, хусусан, X.25 протоколи асосида ишлаши мумкин.

L2F протоколи куйидаги хусусиятларга эга:

- ҳақиқийликни текширувчи муайян протоколга катьйи боғланмаганликни таҳминловчи аутентификациялаш муолажалининг мосланувчанлиги;
- охирги тизимлар учун шаффоғлиги, яъни локаль тармокнинг ишли станциялари ва масофадаги тизимга химоялаш серверидан фойдаланиш учун махсус дастурий таъминот талаб этилмайди;
- воситалар учун шаффоғлиги, яъни масофадаги фойдаланувчиларни авторизациялаш локал тармокнинг масофадан фойдаланиш серверига фойдаланувчиларни бевосита уланишига ўхшаб амалга оширилади;
- аудитнинг тўликлиги, яъни локал тармок серверидан фойдаланиш ҳодисасини кайдлаш нафакат масофадан фойдаланиш сервери тмонидан, балки провайдер сервери томонидан ҳам амалга оширилади.

L2F протоколининг спецификациясига мувофик химояланган туннелни ҳосил килишда куйидаги протоколлар ишлатилади:

- дастлабки инкапсуляцияланувчи протокол – бу протокол (IP, IPX, ёки NeBEUI) асосида локал тармок ишлайди;

– протокол – «йўловчи» – бу протоколга дастлабки протокол инкапсуляцияланади ва бу протоколнинг ўзи хам очик тармок оркали масофадан фойдаланганда инкапсуляцияланиши мумкин; PPP протоколи тавсия этилади;

– бошқарувчи (инкапсуляцияловчи) протокол, туннелни яратиша, 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 протоколидир.

Таъкидлаш лозимки, L2F технологиясидан фойдаланилганда провайдернинг масофадан фойдаланиш сервери фойдаланувчими аутентификациялашни факат виртуал канал яратилиши зарурлигини аниклаш ва исталган локал тармокнинг масофадан фойдаланиш сервери манзилини топишда ишлатади. Ҳакиқийликни якуний 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 охирги нуктлари орасида криптохимояланган туннел яратиш кўзда тутилмаган;

– виртуал химояланган канал факат провайдернинг масофадан фойдаланиш сервери ва локал тармокнинг чегара маршрутизатори орасида яратилиши мумкин, бунда масофадаги фойдаланувчи компьютери билан провайдер сервери орасидаги жой очик колади.

Хозирда L2F протоколи Internet стандарти лойихаси мақомига эга бўлган L2TP протоколига сингдирилган.

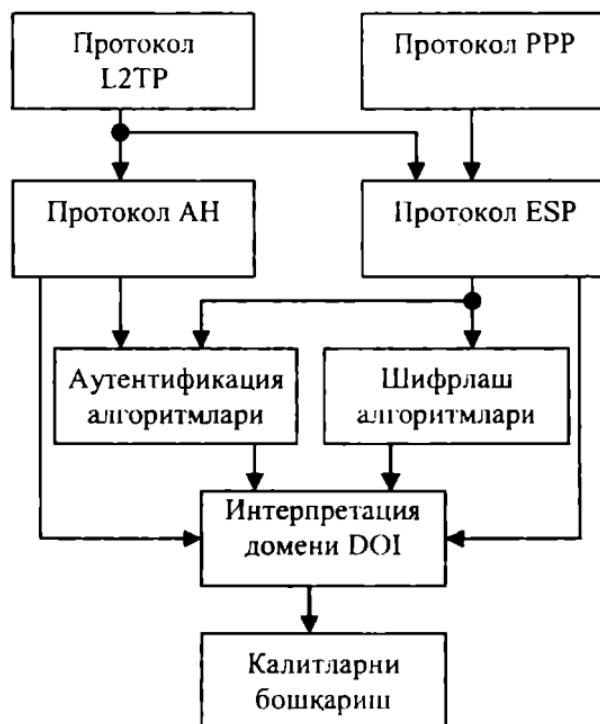
*L2TP* протоколи IETF ташкилотида Microsoft ва Cisco Systems компаниялари мададида ишлаб чикилган. L2TP протоколи ихтиёрий мухитли умуммаксад тармок оркали PPP-трафикни химояланган туннеллаш протоколи сифатида ишлаб чикилган.

PPTPдан фаркли холда L2TP протоколи IP протоколига боғланган эмас, шу сабабали ундан пакетларни коммутацияловчи гармокларда, масалан, ATM (Asynchronous Transfer Mode) ёки кадрларни ретрансляцияловчи (frame relay) тармокларда фойдаланиш мумкин.

L2TP протоколида PPTP ва L2F протоколларининг нафакат яхши хусусиятлари бирлаштирилган, балки янги функциялар, жум-

ладан, IPSec протоколлари стекининг AH ва ESP протоколлари билан ишлаш имконияти қўшилган.

L2TP протоколининг архитектураси 7.14-расмда келтирилган.



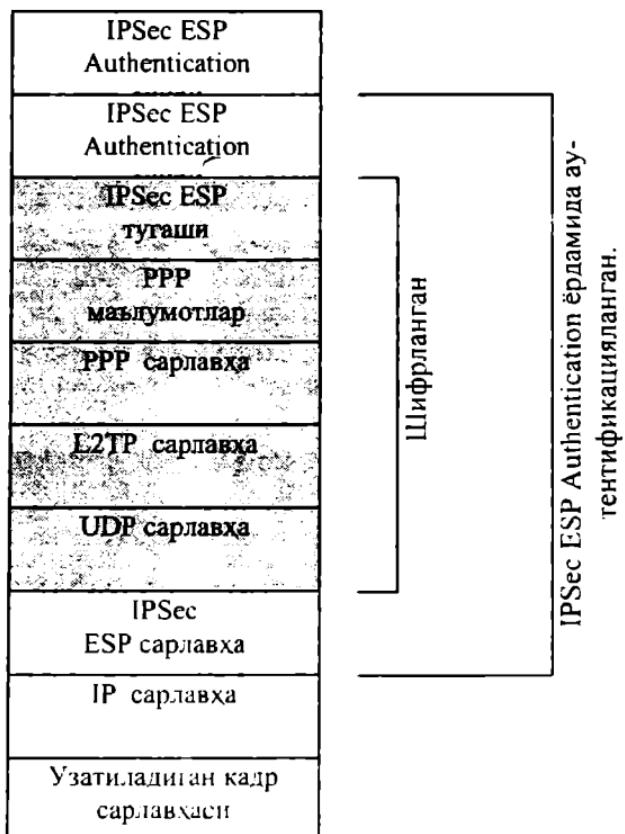
7.14 -расм. L2TP протоколинин архитектураси.

AH ва ESP протоколлари фойдаланувчиларнинг, келишилган ҳолда, шифрлаш ва аутентификациялашнинг турли криптографик алгоритмларини ишлатишларига йўл кўяди. Интерпретация домени DOT (Domain of Interpretation) ишлатилувчи протоколлар ва алгоритмларнинг бирга ишлашини таъминлайди.

Мохияти 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 туннелни бошқаришда ва маълумотларни ташишда хабарларнинг бир хил форматидан фойдаланади.

PPTP протоколидагидек, L2TP протоколи туннелга узатиш учун пакетни йиғишида аввал PPP ахборот маълумотлари майдонига PPP сарлавҳасини, сўнгра L2TP сарлавҳасини кўшади. Шу тариқа олингган пакет UDP протокол томонидан инкапсуляцияланади. L2TP протокол жўнатувчи ва кабул килувчи порти сифатида UDP-портдан фойдаланади. 7.15-расмда L2TP туннели бўйича жўнатилувчи пакет тузилмаси келтирилган.



7.15-расм. L2TP туннели бўйлаб жўнатилидиган пакет тузилмаси

IPSec протоколлар стеки хавфсизлиги сиёсатининг танланган хилига боғлик 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 килувчи манзиллари бўлган IP-сарлавҳа қўшилади. Охирида L2TP маълумотларни узатишга тайёрлаш учун иккинчи PPP-инкапсуляциялашни бажаради.

Компьютер – қабул килувчи маълумотларни қабул килади. 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 факат фойдали маълумотлар бўлади, улар ишланади ва кўрсатилган қабул килувчига юборилади.

L2TP протоколи «фойдаланувчи» ва «компьютер» сатҳларда аутентификациялашни таъминлайди ҳамда маълумотларни аутентификациялайди ва шифрлайди. Мижозларни ва VPN серверларини аутентификациялашнинг биринчи боскичида L2TP сертификация хизматидан олинган локал сертификатлардан фойдаланади. Мижоз ва сервер сертификатлар билан алмасишида ва ҳимояланган уланиш ESP SA (Security Association)ни яратишади.

L2TP компьютерни аутентификациялашни тутгатганидан сўнг, фойдаланувчи сатҳда аутентификациялашда фойдаланувчи исмини ва паролни очик кўринишда узатувчи ҳар қандай протокол, ҳатто PAP, ишлатилиши мумкин. Бу тамомила хавфсиз, чунки L2TP бутун сессияни шифрлайди. Аммо фойдаланувчини аутентификациялашни, компьютер ва фойдаланувчини аутентификациялашда турили калитлардан фойдаланувчи MSC НАР ёрдамида ўтказиш хавфсизликни ошириши мумкин.

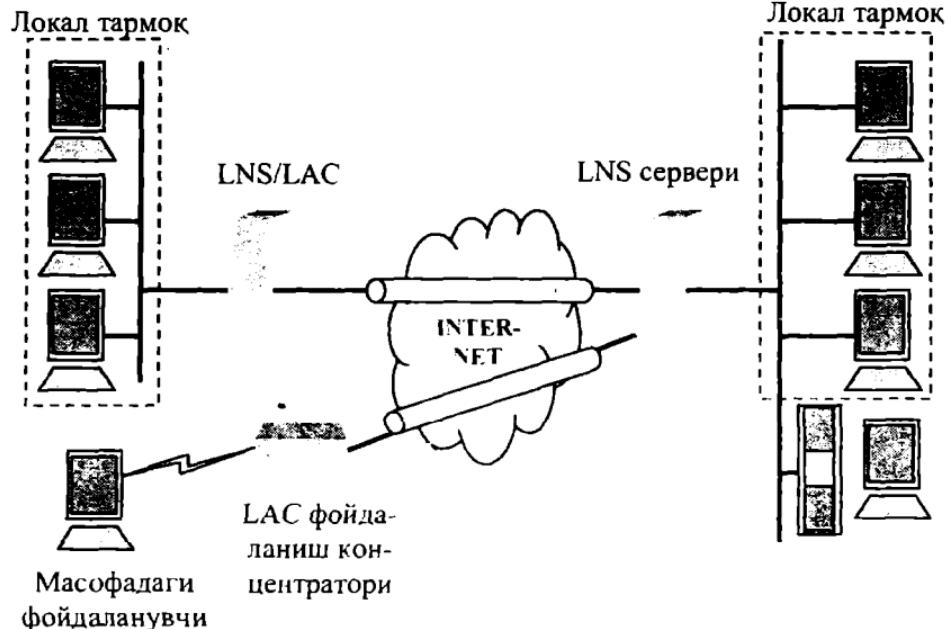
L2TP протоколининг таҳмини бўйича провайдернинг масофадан фойдаланиш сервери ва корпоратив тармок маршрутизатори орасида туннел ҳосил килувчи схемалардан фойдаланилади. Бу протокол олдингиларидан (PPTP ва L2F протоколларидан) фарқли ҳолда охирги абонентлар орасида, ҳар бири алоҳида иловага ажратилиши мумкин бўлган, бир неча туннелни бирданига очиш имко-

ниятини 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 оркали 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 боскичда 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 қиласи ва канал PPPни ўрнатади. Сўнгра фойдаланувчи концентратори LAC охирги узел ва унинг фойдаланувчисини кисман аутентификациялади. Провайдер ISP факат фойдаланувчининг исмидан фойдаланган ҳолда унга L2TP туннеллаш сервисининг кераклигини ҳал қиласи. Агар бундай сервис керак бўлса, фойдаланиш концентратори LAC туннелли уланиш ўрнатилиши лозим бўлган тармок сервери LNS манзилини аниклашга ўтади. Фойдаланувчи ва фойдаланувчи тармогига хизмат кўрсатувчи сервер LNS орасидаги мувофиқликни аниклашнинг қулиялигини таъминлаш максадида провайдер ISP томонидан ўзининг мижозлари учун мааддланувчи маълумотлар базасидан фойдаланиш мумкин.

LNS серверининг IP-манзили аникланганидан сўнг L2TPнинг бу сервер билан туннели бор ёки йўклиги 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 «нукта-нукта» пакет режимини мааддлаши талаби қўйилади. LAC ва LNS орасида туннел яратишда бу туннел доирасида янги уланишга чакириш 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 килиши 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 усууларининг гавсифи келтирилмаган. Чакирик хусусидаги билдириш таркибида тармок сервери LNS томонидан фойдаланувчини аутентификациялаш учун ахборот бўлиши мумкин. Бу ахборотни концентратор LAC фойдаланувчи билан мулокот жараёнида йигали. Аутентификациялашнинг CHAP протоколидан фойдаланилганда билдириш пакетида чакириш-сўзи, фойдаланувчи исми ва унинг жавоби бўлади. PAP протоколи учун бу ахборот фойдала-

нувчи исми ва шифрланмаган паролдан иборат бўлади. Тармок сервери LNS бу ахборотдан, масофадаги фойдаланувчини ўз маълумотларини кайтадан киритишга мажбур килмаслик ва аутентификациялашнинг кўшимча циклини бажармаслик мақсадида, аутентификациялвш учун бирданига фойдаланиши мумкин.

Аутентификация натижаси жўнатилишида тармок сервери LNS ҳам фойдаланиш концентратори LACга фойдаланувчи узелининг IP-манзилини узатиши мумкин. Мохияти бўйича фойдаланиш концентратори LAC масофадаги фойдаланувчи узели ва локал тармокнинг тармок сервери орасида воситачи вазифасини бажаради. Масофадаги узелга корпоратив тармокнинг манзиллар пулидан манзилнинг ажратилиши фойдаланувчига провайдер манзиллар пулидан оддий манзил олинишидаги нокулайликлардан кутилишига имкон беради.

Учинчи боскичда провайдернинг фойдаланиш концентратори LAC ва локал тармокнинг сервери LNS орасида химояланган туннел яратилади. Натижада, инкапсуляцияланган кадрлар PPP туннел оркали концентратор LAC ва тармок сервери LNS орасида иккала йўналишда узатилиши мумкин. Масофадаги фойдаланувчидан PPP кадри келганида концентратор LAC ундан кадрни қоплаган байтларни, назорат йигинди байтларини чиқариб ташлайди, сўнгра уни L2TP протокол ёрдамида тармок протоколига инкапсуляциялади ва туннел оркали тармок сервери LNSга жўнатади. LNS сервер L2TP протоколдан фойдаланиб, келган пакетдан PPP кадрни чиқариб олиб ишлайди.

Туннелнинг зарурый кийматларини созлаш бошқариш хабарлари ёрдамида амалга оширилади. L2TP протоколи хар кандай пакетни коммутацияловчи транспорт устидан ишлаши мумкин. Умумий холда, бу транспорт, масалан, UDP протоколи, пакетларни кафолатли стказиш ни таъминламайди. Шу сабабли L2TP протоколи бу масалаларни хар бир масофадаги фойдаланувчи учун туннел ичida уланишларни ўрнатиш муолажаларидан фойдаланиб, мустакил ҳал этади.

Таъкидлаш лозимки, L2TP протоколи криптохимоянинг муайян усулларини белгиламайди ва шифрлашни турли стандартларидан фойдаланиш мумкинлигини фараз килади. 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 аутентификациялаши таъминлайди. Аутентификациялаш учун бу алгоритм узунлиги 128 хонага тенг бўлган «хэш»ни яратади.

Шундай қилиб, PPTP ва L2TP протоколларининг функционал имкониятлари турлича, PPTP протоколи факат IP-тармоқларда ишлатилиши мумкин ва унга туннелни яратиши ва ишлатиши учун алоҳида TCP уланиш зарур. L2TP протоколи нафакат IP-тармоқларда ишлатилиши мумкин, туннелни яратиш ва у оркали маълумотларни ташишда хизматчи хабарлар бир хил формат ва протоколлардан фойдаланади. L2TP протоколи ташкилот учун мухим бўлган маълумотларнинг кариб 100 %ли хавфсизлигини кафолатлаши мумкин.

L2TP протоколининг камчилиги сифатида куйидагиларни 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 охирги нуктлари орасида криптохимояланган туннел яратиш кўзда тутилмаган;
- L2TPнинг таклиф этилган спецификацияси стандарт шифрлашни факат 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 куришда ахборот алмашинувини криптографик химоялаш, жумладан, аутентификациялаш ҳамда ўзаро алоқа томонлари орасида воситачиликнинг қатор функцияларини амалга ошириш имконияти пайдо бўлади. Ҳакиқатан, OSI моделининг сеанс сатҳи мантикий уланиш-

ларни ўрнатишга ва бу уланишларни бошқаришга жавобгар. Шу сабабли, бу сатҳда суралган уланишларнинг жоизлигини текширувчи ва тармоклараро харакатлар химоясининг бошка функцияларининг бажарилишини таъминловчи дастур-воситачилардан фойдаланиш имконияти мавжуд.

Сеанс сатҳида химояланган виртуал канални шакллантириш протоколи химоянинг татбикӣ протоколлари ҳамда турли сервисларни тақдим этувчи юкори сатҳ протоколлари (HTTP, FTP, POP3, SMTP ва х. протоколлар) учун шаффоффдир. Аммо, сеанс сатҳида юкори сатҳли протоколларни амалга оширувчи иловаларга бевосита боғликлек бошланади. Шунинг учун мазкур сатҳга мос келувчи ахборот алмашиш протоколини амалга ошириш кўп холларда юкори сатҳли иловаларга ўзгаргиришлар киритилишини талаб этиди.

Сеанс сатҳида ахборот алмашишда SSL протоколи кенг тарқалган. Сеанс сатҳида ўзаро алоқа томонлари орасида воситачилек функцияларини бажариш учун IETF ташкилоти гомонидан стандарт сифатида SOCKS протоколи кабул килинган.

*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 ҳавфсизлигини таъминлашда ахборотни химоялашнинг криптографик усулларидан фойдаланади. SSL протоколи тармокнинг иккита абоненти орасида химояланган канал куришнинг барча функцияларини жумладан, уларни аутентификациялаш, узатилувчи маълумотларнинг конфиденциаллигини ва яхлитлигини таъминлаш функцияларини бажаради. Асимметрик ва симметрик криптотизимлардан комплекс фойдаланиш технологияси SSL протоколининг ядрои хисобланади.

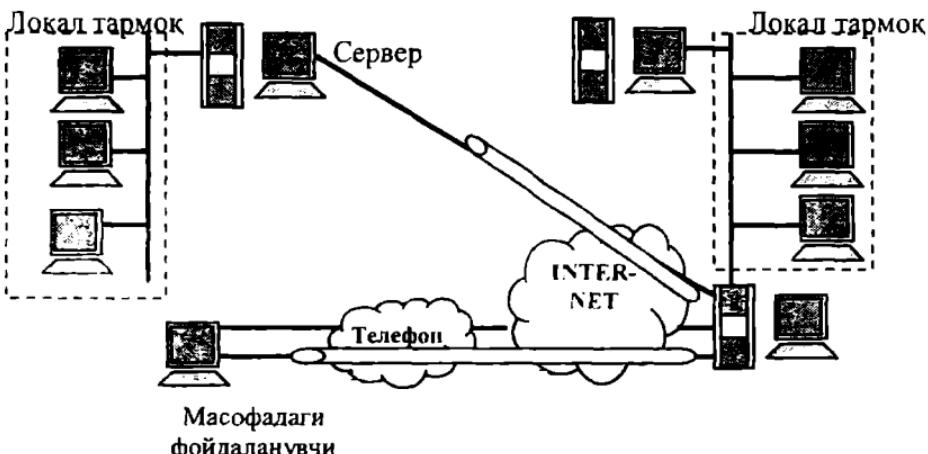
SSLда иккала томоннинг ўзаро аутентификациялаш фойдаланувчиларнинг (мижоз ва сервер) маҳсус сертификация марказларининг раками имзоси билан тасдиқланган очик қалитларининг раками сертификатлари билан алмашиш орқали бажарилади. SSL протоколи ҳамма қабул килган X.509 стандартларга мос келувчи сертификатларни ҳамда сертификатларни беришда ва ҳакиқийлигини текширишда ишлатилувчи PKI очик қалитлари инфратузилмаларининг стандартини мададлайди.

Конфиденциаллик уланиш ўрнатилишида томонлар алмашынадиган симметрик сессия калитларида узатилувчи хабарларни шифрлаш оркали таъминланади. Сессия калитлари хам шифрланган кўринищда узатилади. Бунда улар абонентларнинг сертификатларидан чиқариб олинган очик калитларда шифрланади. Ахборотларни шифрлашда симметрик калитларнинг ишлатилишига асосий сабаб-симметрик калитларда шифрлаш ва расшифровка килиш жараёнининг тезлиги асимметрик калитлар ишлатилишидагига қараганда юқорилиги.

Айланувчи ахборотнинг хакикийлиги ва яхлитлиги электрон ракамли имзони шакллантириш ва текшириш эвазига таъминланади.

Асимметрик шифрлаш алгоритмлари сифатида RSA хамда Диффи-Хеллман алгоритмлари ишлатилади. Симметрик шифрлаш алгоритмлари сифатида эса RC2, RC4, DES хамда Triple DES алгоритмлари ишлатилади. Хэш функцияларини хисоблашда MD5 ва SHA-1 стандартлари ишлатилиши мумкин. SSL протоколининг 3,0 версиясида криптографик алгоритмлари тўплами кенгайтирилувчи хисобланади.

SSL протоколига мувофик криптохимояланган туннеллар виртуал тармоқнинг охирги нукталари орасида яратилади. Ҳар бир химояланган туннелни бошлиб берувчилари-туннел охирги нукталаридаги компьютерларда ишловчи мижоз ва сервер (7.17-расм).



7.17-расм. SSL протоколи асосида шаклланган криптохимояланган туннеллар.

Химояланган уланишни шакллантиришда ва мададлашда SSL протоколи мижоз ва сервер ўзаро алокасининг қуидаги боскичларини кўзда тутади:

- SSL сессиясини ўрнатиш;
- химояланган ўзаро алоқа.

SSL сессияни ўрнатиш жараёнида қуидаги масалалар ечилади:

- томонларни аутентификациялаш;
- химояланган ахборот алмашинуvida ишлатилувчи криптографик алгоритмлар ва зичлаштириш алгоритмларини мувофикалаштириш;
- умумий маҳфий мастер-калитни шакллантириш;
- ахборот алмашишни криптографик химоялаш учун шакллантирилган мастер-калит асосида умумий маҳфий сеанс калитларини генерациялаш.

Кўл беришиш муолажаси деб ҳам аталувчи SSL-сессияни ўрнатилиш мурожаси ахборот алмашишни бевосита химоялашдан олдин пухта ишланади ва SSL протоколи таркибига кирувчи бошлангич 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 қуидаги учта режими маддлайди:

- томонларни ўзаро аутентификациялаш;
- мижозни аутентификацияламасдан серверни бир томонлама аутентификациялаш;
- тўлик анонимлик.

Охирги вариангдан фойдаланилганда томонларнинг ҳақиқийлигини кафолатламасдан ахборот алмашиш хавфсизлиги таъминланади. Бу ҳолда ўзаро алокадаги томонлар, алоқа қатнашчиларини алмаштириб қўйиш билан боғлик хужумлардан химояланмайдилар.

SSL протоколига мувофик ўзаро алокадаги томонларни аутентификациялашда ва умумий маҳфий калитни шакллантиришда кўпинча RSA алгоритмидан фойдаланилади.

Очиқ калитлар ва уларнинг эгалари орасидаги мувофикалик маҳсус сертификация марказлари томонидан берилувчи ракамли

сертификатлар ёрдамида ўрнатилади. Сертификат таркибида кўйидаги ахборот бўлган маълумотлар блокидир:

- сертификация марказининг номи;
- сертификат эгасининг исми;
- сертификат эгасининг очик қалити;
- сертификатнинг таъсир муддати;
- сертификатни ишлашда фойдаланиладиган идентификатор ва криптоалгоритмнинг параметрлари;
- сертификат таркибидаги барча маълумотларни тасдиқловчи сертификация марказининг ракамли имзоси.

Сертификат таркибидаги сертификация марказининг ракамли имзоси очик қалит ва унинг эгасининг ҳақиқийлигини ва бир маънода мослигини таъминлайди. Сертификация маркази очик қалитларнинг ҳақиқийлигини тасдиқловчи нотариус ролини ўтайди. Натижада, бу қалит эгаларига химояланган ўзаро алока хизматидан, олдиндан шахсий учрашувсиз фойдаланишларига имкон беради.

1999 йили SSL 3.0 версияси ўрнига, SSL протоколига асосланган ва ҳозирда Internet стандарти хисобланган TLS протоколи келди. SSL 3.0 ва TLS протоколлари орасидаги фарқ жуда ҳам жиддий эмас.

SSL ва TLS протоколларининг камчилиги – ўзларининг хабарларини ташишда тармоқ сатҳидаги факат битта – IP-протоколидан фойдаланишлари ва, демак, факат IP-тармокларда ишлай олишлари. Ундан ташқари, SSL/TLSнинг амалда кўлланиши татбиқий 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 ксийнги барча маълумотлар обрўсизлантирилади.

Ундан ташқари, SSLда аутентификациялашда ва ширфлашда бир хил қалитдан фойдаланилади. Бу эса маълум бир ҳолатларда заифликка олиб келиши мумкин. Бундай ечим турли қалитлар ишлатилиганига нисбатан кўп статистик маълумотларни йиғишга имкон беради.

*SOCKS* протоколи OSI моделининг сеанс сатхига мижоз-сервер иловаларининг ўзаро алоки муолажасини сервер-воситачи ёки proxy-сервер оркали ташкил этади.

Умумий холда, тармоқлараро экранларда анъанавий ишлатилувчи дастур-воситачилар куйидаги функцияларни бажариши мумкин:

- фойдаланувчими идентификациялаш ва аутентификациялаш;
- узатилувчи маълумотларни криптохимоялаш;
- ички тармок ресурсларидан фойдаланишни чегаралаш;
- ахборотлар оқимини фильтрлаш ва ўзгартириш, масалан, вирусларни кидириш ва ахборотни шаффоф шифрлаш;
- чикадиган ахборот оқимлари учун ички тармок манзилларини трансляциялаш.

Абвал SOCKS протоколи фақат мижоз иловаларининг серверга сўровларини кайта йўналтириш ҳамда бу иловаларга олинган жавобни кайтариш учун ишлаб чикилган эди. Ушбу муолажаларнинг ўзи тармок IP-манзиллари NATни (Network Address Translation) трансляциялаш функцияларини амалга ошириш имкониятини беради. Чиқувчи пакетлардаги жўнатувчиларнинг IP-манзилларини шлюзининг битта IP-манзили билан алмаштириш ички тармок топологиясини ташки фойдаланувчилардан беркитишга имкон беради ва натижада, рухсатсиз фойдаланиш масаласи мураккаблашади. Тармок манзилларини трансляциялаш хавфсизликни ошириш билан бир каторда хусусий манзиллаш тизимини мададлаш имконияти хисобига тармок ички манзили маконини кенгайтиришга имкон беради.

SOCKS протоколи асосида тармокли ўзаро алокани химоялаш бўйича воситачиликнинг бошқа функциялари ҳам амалга оширилиши мумкин. Масалан, SOCKS ахборот оқимлари йўналишни назоратлашда ва фойдаланувчилар ва ахборотлар атрибутларига боғлик холда фойдаланишни чегаралашда ишлатилиши мумкин. SOCKS протоколининг воситачилик функцияларини бажаришдаги самарали ишлатилиши унинг OSI моделининг сеанс сатхига мўлжалланганилиги билан таъминланади. Татбикий сатҳдаги воситачиларга караганда, сеанс сатхига энг юкори тезкорликка, юкори сатҳ протоколларига (HTTP, FTP, POP3, SMTP ва х.) боғлик бўлмасликка эришилади. Ундан ташқари, SOCKS протоколи IP протоколга боғланмаган ва операцион тизимга боғлик эмас. Маса-

лан, мижоз иловалари ва воситачи орасида ахборот алмашишда IPX протоколи ишлатилиши мумкин.

SOCKS протоколи туфайли тармоклараро экранлар ва виртуал хусусий тармоклар турли тармоклар орасида хавфсиз ўзаро алокани ва ахборот алмашинувини ташкил этишлари мумкин. SOCKS протоколи ушбу тизимларни хавфсиз бошкаришни унификацияланган стратегия асосида амалга оширишга имкон беради. Таъкидлаш лозимки, SOCKS протоколи асосида ҳар бир илова ва ҳар бир сеанс учун алоҳида химояланган туннел яратилиши мумкин.

SOCKS протоколи спецификациясига мувофик тармок шлюзиға (тармоклараро экранга) ўрнатилувчи SOCKS – сервер ва ҳар бир фойдаланувчи компьютерга ўрнатилувчи SOCKS – мижоз фарқланади. SOCKS-сервер ҳар қандай татбикӣ сервер билан бу серверга мос келувчи татбикӣ мижоз номидан ўзаро алокани таъминлайди. SOCKS-мижоз мижоз томонидан татбикӣ серверга бўлган барча сўровларни ушлаб колиб уларни SOCKS-серверга узатишга аталган. Таъкидлаш лозимки, мижоз иловаларининг сўровларини ва SOCKS-сервер билан ўзаро алокани ушлаб колишни бажарувчи SOCKS-мижозлар универсал мижоз дастурларига ўрнатилиши мумкин. SOCKS-серверга сеанс (сокет) сатҳидаги трафик маълум, шунинг учун у синчилаб 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 маъкулланган.

SOCKS протоколининг 4-версиясига биноан уланишни ўрнатишнинг умумий схемаси куйидагича:

- тармоқдаги қандайдир сервер билан боғланишни истаган мижоз SOCKS-сервер (ихтисослаштирилган роҳу-сервер) билан уланиб унга маҳсус 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 қиласи, SOCKS-сервер маълумотларни ретрансляциялайди;

SOCKS протоколининг 5-версияси тўртинчи версиянинг жиддий ривожи хисобланади. У куйидаги қўшимча имкониятларни амалга оширади:

– номларидан SOCKS-мижозлар мурожаат этувчи фойдаланувчиларни аугентификациялаш кўзда тутилган. SOCKS-сервер SOCKS-мижоз билан аутентификациялаш усулини келишиб олишлари мумкин. Аутентификациялаш компьютер ресурсларидан фойдаланишни чегаралашга имкон беради. Икки томонлама аутентификациялаш ҳам жоиз хисобланади, яъни фойдаланувчи, ўз навбатида, керакли SOCKS-сервер билан уланганига ишонч хосил килиши мумкин;

– доменли исмларни ишлатиш жоиз хисобланади: SOCKS-мижоз SOCKS-серверга нафакат уланишни ўрнатишда керак бўлган компьютернинг IP-манзилини, балки унинг DNS исмини ҳам узатиши мумкин;

– нафакат TCP-протокол, балки UDP протокол ҳам мададланади;

SOCKS протоколининг 5-версиясига биноан уланишни ўрнатишнинг умумий схемаси қўйидагича тавсифланиши мумкин:

– тармоқдаги кандайдир татбикӣ сервер билан уланиш ўрнатишни истаган татбикӣ мижознинг сўровини мана шу компьютерда ўрнатилган SOCKS-мижоз ушлаб колади;

– SOCKS-сервер билан уланган SOCKS-мижоз унга ўзи мададловчи аутентификациялашнинг барча усулларининг идентификаторларини билдиради;

– SOCKS-сервер аутентификациялашнинг қайси усулидан фойдаланишни ҳал қиласи (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 муваффакиятсиз аутентификациялашда SOCKS-сервер уланишни узади;

– муваффакиятли идентификациялашдан кейин SOCKS-мижоз SOCKS-серверга тармоқдаги сўралаётган татбикӣ сервер DNS исмини ёки IP-манзилини узатади, сўнгра SOCKS-сервер фойдала-

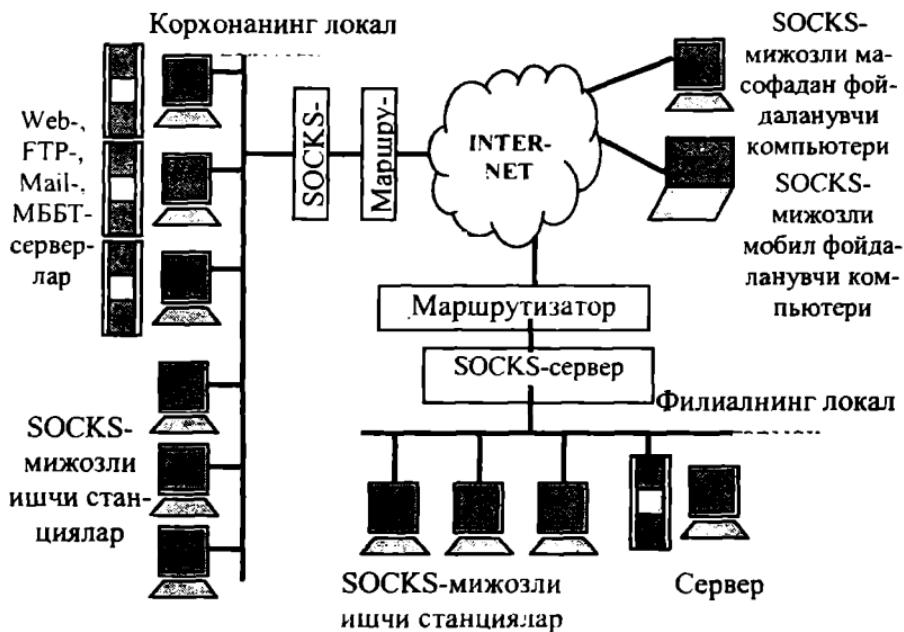
нишни чегаралашнинг мавжуд коидалари асосида ушбу татбикӣ сервер билан уланишни ўрнатиш бўйича қарор кабул қиласди;

– уланиш ўрнатилған ҳолда татбикӣ мижоз ва татбикӣ сервер бир-бирлари билан уланиш занжири оркали алоқа қиласдилар SOCKS-сервер маълумотларни ретрансляциялайди ҳамда тармокли ўзаро алоқа хавфсизлиги бўйича воситачилик функцияларини бажариши мумкин масалан аутентификациялаш жараёнида SOCKS-мижоз ва SOCKS-сервер сеанс қалитларини алмаштиришган бўлсалар, улар орасидаги барча трафик шифрланиши мумкин.

Фойдаланувчиларни SOCKS-сервер томонидан аутентификациялаш X.509 форматидаги ракамли сертификатларга ёки паролларга асосланиши мумкин. SOCKS-мижоз ва SOCKS-сервер орасидаги трафикни шифрлаш учун OSI моделининг сеансли ёки пастрок сатхларига мўлжалланган протоколлар ишлатилиши мумкин. SOCKS-сервер фойдаланувчиларни аутентификациялаш, IP-манзилларини трансляциялаш ва трафикни криптоҳимоялашдан бошка яна қуидаги функцияларни бажариши мумкин:

- ички тармоқ ресурсларидан фойдаланишни чегаралаш;
- ташки тармоқ ресурсларидан фойдаланишни чегаралаш;
- ҳабарлар оқимиини фильтрлаш, масалан, вирусларни динамик кидириш;
- ҳодисаларни қайдлаш ва уларга реакция кўрсатиш;
- ташки тармоқдан сўралган маълумотларни кэшлиш.

Шундай қилиб, SOCKS протоколи бўйича ҳимояланган виртуал тармокларни шакллантириш учун ҳар бир локал тармоқ билан Internet уланган нуктадаги компьютер-шлюзда SOCKS-сервер, локал тармоқдаги ишчи станцияларда ва масофадан фойдаланувчиларнинг компьютерларида эса SOCKS-мижоз ўрнатилади. Моҳияти бўйича, SOCKS-серверга SOCKS протоколини мададловчи тармоклараро экран сифатида караш мумкин (7.18-расм).



7.18-расм. SOCKS протоколи бўйича ўзаро алоқа схемаси.

Масофадаги фойдаланувчилар Internet га коммутацияланувчи ёки ажратилган линиялар оркали уланишлари мумкин. Химояланган виртуал тармок фойдаланувчиси қандайдир татбикӣ сервер билан уланишга уринганида SOCKS-мижоз SOCKS-сервер билан ўзаро алоқани бошлайди. Ўзаро алоқанинг биринчи боскичи тугаганидан сўнг фойдаланувчи аутентификацияланади, фойдаланиш коидаси эса унинг кўрсатилган манзилдаги компьютерда ишлайдиган муайян тармок иловаларига уланиш ҳуқуқига эга эканлигини кўрсатади. Кейинги ўзаро алоқалар криптографик химояланган канал бўйича юз бериши мумкин.

SOCKS-серверга, локал тармокларни рухсатсиз фойдаланишдан химоялашдан ташқари, бу локал тармок фойдаланувчиларининг Internetning очик ресурсларидан (Telnet, WWW, SMTP, POP ва х.) фойдаланишларининг назорати ҳам юкланиши мумкин. Фойдаланиш бутунлай авторизацияланган, чунки фойдаланувчининг компьютери эмас, балки ўзи идентификацияланади ва аутентификацияланади. Фойдаланиш коидалар муайян ходимнинг ваколатига кўра Internet нинг маълум ресурслари билан боғланишга рухсат бериши ёки бермаслиги мумкин. Фойдаланиш коидаларининг

таъсири бошка параметрлар, масалан, аутентификациялаш усули ёки сутка вактига боғлиқ бўлиши мумкин. Тармокли ўзаро алоқа хавф-сизлигининг янада юкори даражасига эришиш учун Internet томонидан фойдаланишга рухсат берилган локал тармок серверлари, SOCKS-серверга уланувчи, химояланган очик кисм тармокни хосил килувчи алоҳида сегментга ажратилиши лозим.

## 7.5. IPSec протоколлар стекини химояланган виртуал хусусий тармоклар куришда ишлатилиши

IPSec протоколи (Internet Protocol Security) асосан IP тармокларда маълумотларни хавфсиз узатишни таъминлашга аталган. IPSecнинг ишлатилиши қўйидагиларни кафолатлади:

- узатилаётган маълумотларнинг яхлитлигини, яъни маълумотлар узатилишида бузилмайди, йўколмайди ва тақорланмайди;
- жўнатувчининг аутентлигини, яъни маълумотлар ҳақиқий жўнатувчи томонидан узатилган;
- узатиладиган маълумотларнинг конфиденциаллигини, яъни маълумотлар шундай шаклда узатилади, 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 сатхи ISPrга қолдиради. IPSec протоколлар стеки тармок сатҳида ахборот химоясини таъминлади. Бу химоянинг ишловчи иловаларга кўринмаслигига олиб келади.

IP-пакет IP тармокларда коммуникациянинг фундаментал бирлиги хисобланади. Унинг тузилмаси 7.19-расмда келтирилган. IP-пакет таркибида манба манзили S ва ахборот кабул килувчининг 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 максадида, IPSec протоколларининг стеки катор стандартлаштирилган криптографик технологиялар асосида қурилган:

- калитларни алмаштириш очик тармоқдан фойдаланувчилар орасида маҳфий калитларни таксимлашнинг Диффи-Хеллман алгоритми бўйича амалга оширилади;
- иккала томоннинг ҳакикийлигини кафолатлаш ва main-in-the-middle ўртадаги одам хилидаги хужумларни олдини олиш максадида Диффи-Хеллман алгоритми бўйича алмашишларни имзолашда очик калитлар криптографиясидан фойдаланилади;
- очик калитларнинг ҳакикийлигини тасдиқлашда ракамли сертификатлар ишлатилади;
- маълумотларни шифрлашда блокли симметрик алгоритмлардан фойдаланилади;
- хэшлаш функциялари асосида ахборотларни аутентификациялаш алгоритмлари ишлатилади.

Ҳимояланган канални ўрнатиш ва мададлашдаги асосий масалалар куйидагилар:

- фойдаланувчилар ёки компьютерларни аутентификациялаш;
- ҳимояланган каналнинг охирги нукталари орасида узатилувчи маълумотларни шифрлаш ва аутентификациялаш;
- каналнинг охирги нукталарини маълумотларни аутентификациялашда ва шифрлашда керак бўладиган маҳфий калитлар билан таъминлаш.

Юкорида 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 ҳимояни инкапсуляцияловчи протокол ESP (Encapsulation Security Payload)ни ва сарлавҳани аутентификацияловчи протоколи AH(Authentication Header)ни амалга оширади. У сарлавҳаларни иштайди; пакетга қўлланиладиган хавфсизлик сиёсатини аниглаш учун SPD ва SAD маълумотлар базаси билан ўзаро алоқа килади;

- 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 саклайди. Чиқувчи SAлардан чиқувчи пакетларни химоялашда, кирувчи SAлардан эса IPSec сарлавҳали пакетларни ишлашда фойдаланилади. SAD маълумотлар базаси SA билан қўлда ёки калитларин бошқариш протоколла-ри 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 кисми де-йиш мумкин. IPSecнинг асосий модули иккита интерфейсни – кириш йўли ва чиқиш йўли интерфейсларни таъминлайди. Кириш йўли интерфейси кирувчи пакетлар томонидан, чиқиш йўли интер-фейси эса чиқувчи пакетлар томонидан фойдаланилади. IPSecнинг амалга оширилиши TCP/IP протоколлар стекининг транспорт ва тармоқ сатхлари 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 гурухга ажратиш мумкин:

– узатилувчи маълумотларни бевосита ишловчи (уларнинг хавфсизлигини таъминлаш учун) протоколлар;

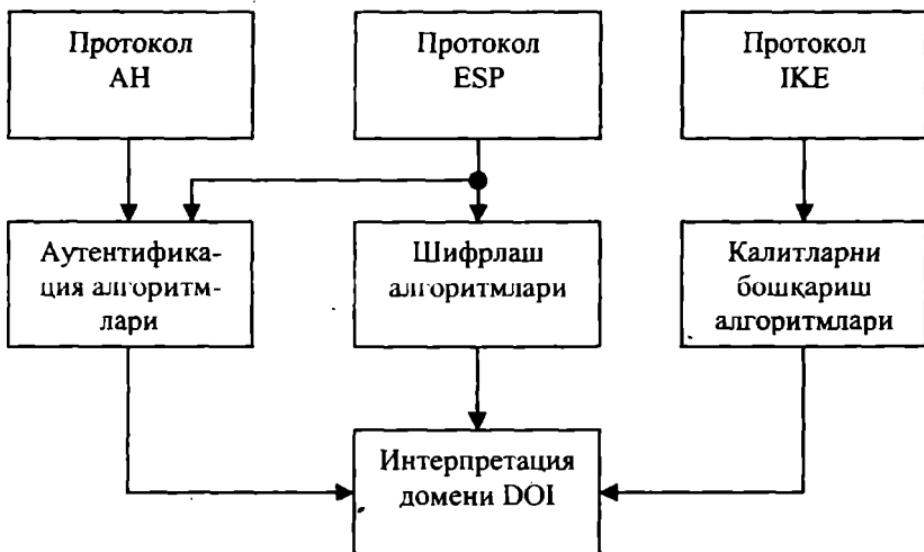
– биринчи гурух протоколларига керакли химояланган ула-нишлар параметрларини автоматик тарзда мувофиқлаштиришга имкон берувчи протоколлар.

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 мувофикаштирувчи ва қалитларни бошқариш протоколи IKE. Бу протокол химояланган канални инициализациялаш усулини, жумладан, ишлатилувчи криптохимоялаш алгоритмларини мувофикаштиришни ҳамда химояланган уланиш доирасида маҳфий қалитларни алмашиш ва бошқариш муолажаларини белгилайди;



7.20-расм. IPSec протоколлари стекининг архитектураси.

– сарлавҳани аутентификацияловчи протокол AH. Бу протокол маълумотлар манбанин аутентификациялашни, уларнинг, кабул килинганидан сўнг, яхлитлигини ва ҳақиқийлигини текшириш ва тақорий ахборотларнинг тикиштирилишидан химояни таъминлайди;

– химояни инкапсуляцияловчи протокол ESP. Бу протокол узатилувчи маълумотларни криптографик беркитишни, аутентификациялашни ва яхлитлигини таъминлайди ҳамда тақорий ахборотларнинг тикиштирилишидан химоялайди.

АН ва ESP протоколлари ҳар бири алохида ва биргаликда ишлатилиши мумкин. Бу протоколлар вазифаларининг қискача баёнидан кўриниб турибдики, уларнинг имкониятлари қисман бир хил.

АН протоколи факат маълумотларни яхлитлигини ва аутентификациялашни таъминлашга жавоб беради. ESP протоколи кувватлирок хисобланади, чунки у маълумотларни шифрлаши мумкин, ундан ташкари, АН протоколи вазифасини ҳам бажариши мумкин.

IKE, АН ва ESP протоколларининг ўзаро алокалари куйидагича кечади. Аввал IKE протоколи бўйича иккита нукта орасида мантикий уланиш ўрнатилади. Бу уланиш IPSec стандартларида «хавфсиз ассоциация» -Security Association, SA номини олган. Ушбу мантикий канал ўрнатилишида каналнинг охирги нукталарини аутентификациялаш бажарилади ҳамда маълумотларни химоялаш параметрлари, масалан, шифрлаш алгоритми, сессия маҳфий калити ва х. танланади. Сўнгра хавфсиз ассоциация SA томонидан ўрнатилган доирада АН ва ESP протоколи ишлай бошлайди. Бу протоколлар ёрдамида узатилувчи маълумотларнинг истаган химояси, танланган параметрлардан фойдаланилган холда бажарилади.

IPSec архитектурасининг ўрта сатҳини IKE протоколида кўлланилувчи параметрларни мувофикалаштириш ва калитларни бошкариш алгоритмлари ҳамда АН ва ESP протоколларида ишлатилувчи аутентификациялаш ва шифрлаш алгоритмлари ташкил этади.

Таъкидлаш лозимки, IPSec архитектурасининг юкори сатҳидаги виртуал канални химоялаш протоколлари (АН ва ESP) муайян криптографик алгоритмларга боғлик эмас. Аутентификациялаш ва шифрлашнинг кўп сонли турли-туман алгоритмларидан фойдаланиш имконияти туфайли IPSec тармокни ҳимоялашни ташкил этишнинг юкори даражадаги мосланувчанлигини таъминлайди. IPSecнинг мосланувчанлиги деганда ҳар бир масала учун унинг ечилишининг турли усуллари тавсия этилиши тушунилади. Бир масала учун танланган усул, одатда, бошқа масалаларни амалга ошириш усулларига боғлик эмас. Масалан, шифрлаш учун DES алгоритмининг танланиси маълумотларни аутентификациялашда ишлатилувчи дайджестни хисоблаш функциясини танлашга таъсир килмайди.

IPSec архитектурасининг *пастки сатҳи* интерпретациялаш домени DOI (Domain of Interpretation)дан иборат. Интерпретациялаш доменининг кўлланиш заруриятига қўйидагилар 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 х. 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 узатилувчи маълумотларни қўйидаги иккита режимида химоялаши мумкин:

- туннел режимида; IP пакетлар бутунлай, уларнинг сарлавҳаси билан бирга химояланади.
- транспорт режимида; IP пакетларнинг факат ичидагилари химояланади.

Туннел режими асосий режим хисобланади. Бу режимда дастлабки пакет янги IP пакетга жойланади ва маълумотлар тармок бўйича узатиш янги IP-пакет сарлавҳаси асосида амалга оширилади. Туннел режимида ишлашда ҳар бир оддий IP-пакет криптохимояланган кўринишда бутунлайча IPSec конвертига жойланади. IPSec конверти, ўз навбатида бошка химояланган IP-пакетга инкапсуляцияланади. Туннел режими одатда маҳсус ажратилган хавфсизлик шлюзларида – маршрутизаторлар ёки тармоклараро экранларда амалга оширилади. Бундай шлюзлар орасида химояланган туннеллар шакллантирилади.

Туннелнинг бошка томонида қабул қилинган химояланган IP-пакетлар «очилади» ва олинган дастлабки IP-пакетлар қабул

килувчи локал тармок компьютерлариға стандарт коидалар бүйича узатилади. IP-пакетларни туннеллаш туннелларни эгаси бўлмиш локал тармоқдаги оддий компьютерлар учун шаффоф хисобланади. Охирги тизимларда туннел режими масофадаги ва мобил фойдаланувчиларни мададлаш учун ишлатилиши мумкин. Бу ҳолда фойдаланувчилар компьютерида IPSecснинг туннел режимини амалга оширувчи дастурий таъминот ўрнатилиши лозим.

Транспорт режимида тармок орқали IP-пакетни узатиш бу пакетнинг дастлабки сарлавхаси ёрдамида амалга оширилади. IPSec конвертига криптохимояланган кўринишда факат 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 оқимиини химоялашни мададлашда ишлатилиши мумкин. Таъкидлаш лозимки, транспорт режимида ишлаш химояланган ўзаро алоқа гурухига кирувчи барча тизимларда ўз аксини топади ва аксарият холларда тармок иловаларини қайта дастурлаш талаб этилади.

Туннел ёки транспорт режимидан фойдаланиш маълумотларни химоялашга қўйиладиган талабларга ҳамда IPSec ишловчи узел ролига боғлик. Химояланувчи канални тугалловчи узел-хост (охирги узел) ёки шлюз (ораликдаги узел) бўлиши мумкин. Мос ҳолда, IPSecни қўллашнинг куйидаги учта асосий схемаси фарқланади:

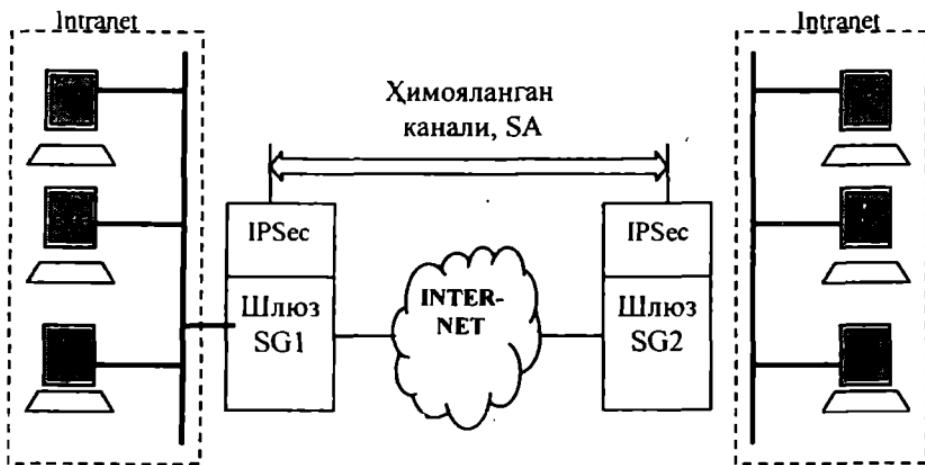
- «хост – хост»;
- «шлюз – шлюз»;
- «хост – шлюз»;

Биринчи схемада химояланган канал тармокнинг охирги иккита узели, яъни H1 ва H2 хостлар орасида ўрнатилади (7.21-расм), IPSecни мададловчи хостлар учун транспорт, ҳам туннел режимидан фойдаланишга рухсат берилади.



7.21-расм. «Хост-хост» схемаси.

Иккинчи схемага биноан, химояланган канал хар бирида IPSec протоколи ишловчи, *хавфсизлик шлюзлари SG1 ва SG2* (Security Gateway) деб аталувчи оралиқдаги иккита узеллар орасыда ўрнатилади (7.22-расм).

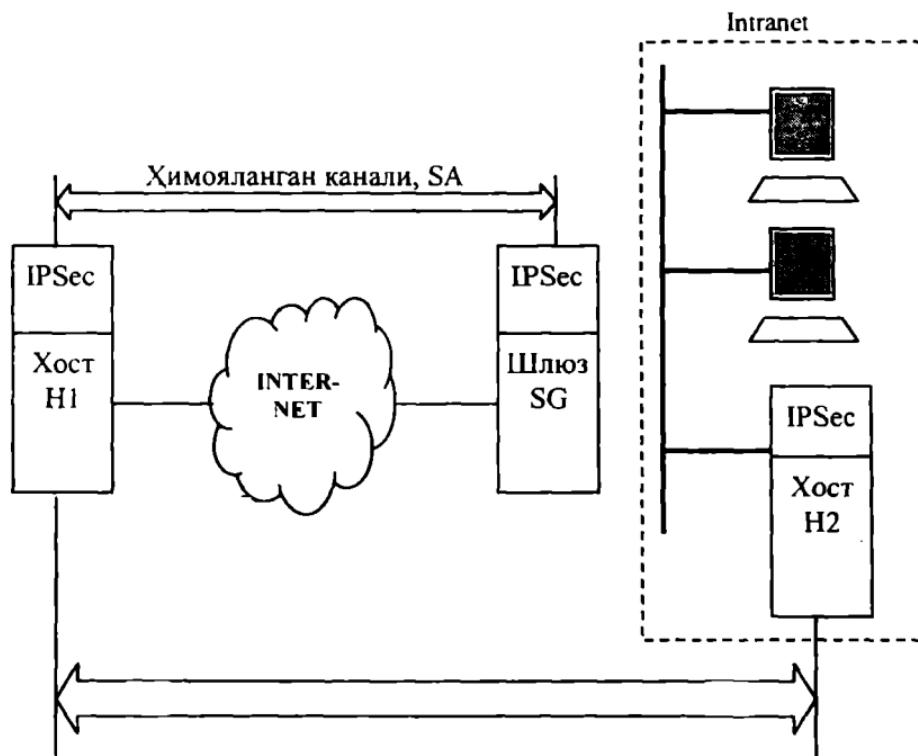


7.22-расм. «Шлюз-шлюз» схемаси.

Хавфсизлик шлюзи иккита тармокқа уланувчи тармок курилмаси бўлиб, ўзидан кейин жойлашган хостлар учун шифрлаш ва аутентификациялаш функцияларини бажаради. VPNнинг хавфсизлик шлюзи алоҳида дастурий маҳсулот, алоҳида аппарат курилма ҳамда VPN функциялари билан тўлдирилган маршрутизатор ёки тармоклараро экран кўринишида амалга оширилиши мумкин.

Маълумотларни химояланган алмасиши тармоқларга уланган, хавфсизлик шлюзларидан кейин жойлашган ҳар кандай иккита охирги узеллар орасида рўй бериши мумкин. Охирги узеллардан IPSec протоколни мададлаш талаб килинмайди, улар ўзларининг трафигини химояланмаган ҳолда корхонанинг ишончли тармоғи Intranet оркали узатади. Умумфойдаланувчи тармокка юборилувчи трафик хавфсизлик шлюзи оркали ўтади ва бу шлюз ўзининг номидан IPSec ёрдамида трафикни химоялашни таъминлади. Шлюзларга факат туннел режимида ишлашга рухсат берилади, вахоланки улар транспорт режимини ҳам мададлашлари мумкин (бу ҳолда самара кам бўлади).

«Хост – шлюз» схемаси кўпинча химояланган масофадан фойдаланишда 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 жүннатында хам транспорт ва хам туннел режимларидан фойдаланиши мумкин, шлюз эса хостта пакетларни факт туннел режимида жүннатади.

Бу схемани масофадаги H1 хост ва шлюз томонидан химояланувчи ички тармоққа тегишли бирор H2 хост орасида параллел яна бир химояланган канални яратып модификациялаш мумкин. Иккита SAдан бундай комбинациялаб фойдаланиш ички тармоқдаги трафикни хам ишончли химоялашта имкон беради.

Күрилган IPSec асосида химояланган канални куриш схемалари турли-туман виртуал химояланган тармоқтарни (VPN) яратында кенг күлланилади. IPSec асосида турли архитектурага эга бўлган виртуал химояланган тармоқлар, жумладан, масофадан фойдаланувчи VPN(Remote Access VPN), корпорация ичидаги VPN(Intranet VPN) ва корпорацияларо VPN(Extranet VPN) курилади.

IPSec асосидаги VPN-технологияларининг жозибалилигини куйидаги сабаблар орқали изоҳлаш мумкин:

- тармок сатхининг химояси тармоқда ишловчи барча татбиқий тизимлар учун шаффоф, яъни барча иловалар химояланган тармоқда ҳеч кандай тузатишсиз ва ўзгаришсиз ҳудди очик тармоқда ишлаганидек иштайверади;

- химоялаш тизимининг масштабланувчанлиги таъминланади, яъни мураккаблиги ва унумдорлиги турли бўлган обьектларни химоялаш учун мураккаблиги, унумдорлиги, нархи даражаси бўйича адекват бўлган химоялашнинг дастурий ёки дастурий-аппарат воситаларидан фойдаланиш мумкин;

- масштабланувчи катордаги ахборотни химоялаш маҳсулотлари бирга ишлай оладилар, шу сабабли уларни турли сатҳдаги обьектларда (масофадаги ягона терминаллардан то ихтиёрий масштабли локал тармоқларгача) ресурсларидан ва трафигидан барча бегоналар фойдалана ололмайдиган ягона корпоратив тармокка бирлаштириш мумкин.

# VIII боб. ОЧИҚ КАЛИТЛАРНИ БОШҚАРИШ ИНФРАТУЗИЛМАСИ РКІ

## 8.1. РКІнинг ишлаш принципи

Тарихан ахборот хавфсизлигини бошкарувчи хар қандай марказнинг вазифалари доирасига ахборот хавфсизлигининг турли воситалари томонидан ишлатилувчи калитларни бошқариш кирган. Бу-калитларни бериш, янгилаш, бекор килиш ва тарқатиш.

Симметрик криптографиядан фойдаланилғанда калитларни тарқатиш масаласи әнд мұраккаб мұаммога айланған, чунки:

- N фойдаланувчи учун химояланған  $N(N-1)/2$  калитни тарқатиш лозим әди. N бир неча юзга тенг бўлганида бу сермашаккат вазифага айланиши мумкин;
- бундай тизимнинг мұраккаблиги (калитларнинг кўплиги ва тарқатиш каналининг маҳфийлиги) хавфсизлик тизимини куриш коидаларининг бири – тизим оддийлигига тўғри келмайди, натижада, заиф жойларнинг пайдо бўлишига олиб келади.

Асимметрик криптография фактат N маҳфий калитни тавсия этиб, бу мұаммони четлаб ўтишга имкон яратади. Бунда хар бир фойдаланувчидаги фактат битта маҳфий калит ва маҳсус алгоритм бўйича маҳфий калитдан олинган очик калит бўлади.

Очик калитдан маҳфий калитни олиб бўлмаслиги сабабли очик калитни химояланмаган ҳолда барча ўзаро алока катнашчиларига тарқатиш мумкин. Ўзининг маҳфий калити ва ўзаро алокадаги шеригининг очик калити ёрдамида хар қандай фойдаланувчи хар қандай криптоамалларни бажариши мумкин: бўлинувчи сирни хисоблаш, ахборотнинг конфиденциаллиги ва яхлитлигини химоялаш, электрон ракамли имзони яратиш.

Шундай килиб, симметрик криптографиянинг иккита асосий мұаммоси ҳал этилади:

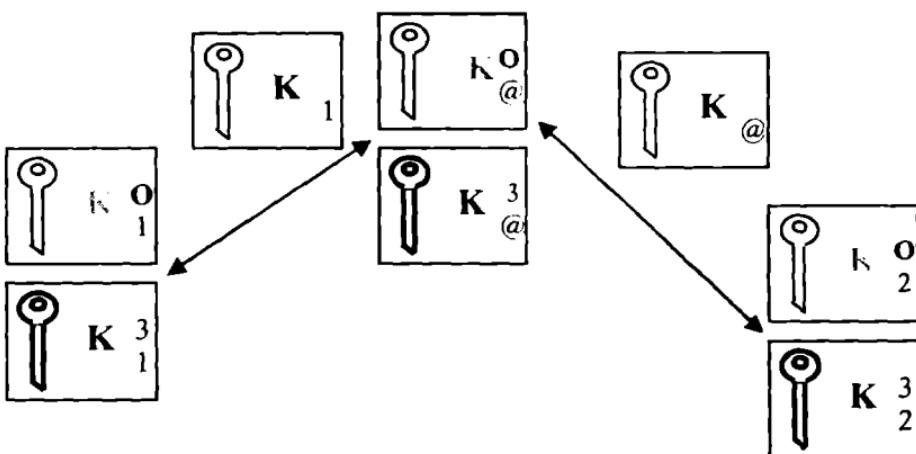
- калитлар сонининг қўплиги – улар энди атиги N та;
- тарқатишнинг мураккаблиги – уларни очик тарқатиш мумкин.

Аммо бу технологиянинг битта камчилиги – ҳужум килувчи нияти бузук одам ўзаро алока катнашчилари ўртасида жойлашганида тап-in-the-middle (ўртадаги одам) ҳужумига майиллиги.

Очик калитларни бошқариш инфратузилмаси PKI ушбу камчиликни бартараф килишга имкон беради ва тап-in-the-middle ҳужумидан самарали химояланишни таъминлайди. Очик калитлар инфратузилмаси корпоратив ахборот тизимларининг ишончли ишлаши учун аталган ва ички ва ташки фойдаланувчиларга ишончли муносабатлар занжири ёрдамида хавфсиз ахборот алмашишга имкон беради. Очик калитлар инфратузилмаси фойдаланувчининг шахсий маҳфий калитини унинг очик калити билан боғловчи электрон паспортга ўхшаб ишловчи ракамли сертификатларга асосланади.

***Man-in-the-middle ҳужумидан ҳимоялаши.*** Man-in-the-middle ҳужуми амалга оширилганида нияти бузук одам очик канал оркали узатилувчи ўзаро алоканинг конуний иштирокчилари калитларини секингина ўзининг очик калитига алмаштириб, конуний иштирокчиларнинг ҳар бири билан бўлинувчи сир яратиши ва сўнгра уларнинг барча ахборотларини ушлаб колиши ва расшифровка килиши мумкин.

Ҳужум қилувчининг харакатини ва бу ҳужумдан химояланиш усулини мисол оркали (8.1-расм) кўриб чиқайлик. Фараз килайлик, фойдаланувчилар 1 ва 2 ўзларига умумий бўлган бўлинувчи сирни Диффи-Хеллман схемаси бўйича хисоблаб, химояланган уланишни ўрнатишга карор килдилар. Аммо 1- ва 2- фойдаланувчиларнинг  $K_1$  ва  $K_2$  калитлари очик канал оркали узатилаётган онда нияти бузук, одам @ бу каналларни манзилатга етказмай ушлаб колди. Нияти бузук одам ўзининг маҳфий ва очик калитини яратиб, очик K калитини 1 ва 2-фойдаланувчиларга секингина уларнинг ҳакиқий 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 маҳфий калитларидан ва нияти бузук одам @нинг очик калити  $K_{\text{одам}}$  дан фойдаланадилар.



8. 1-расм. «Man-in-the-middle» ҳужумини амалга ошириш.

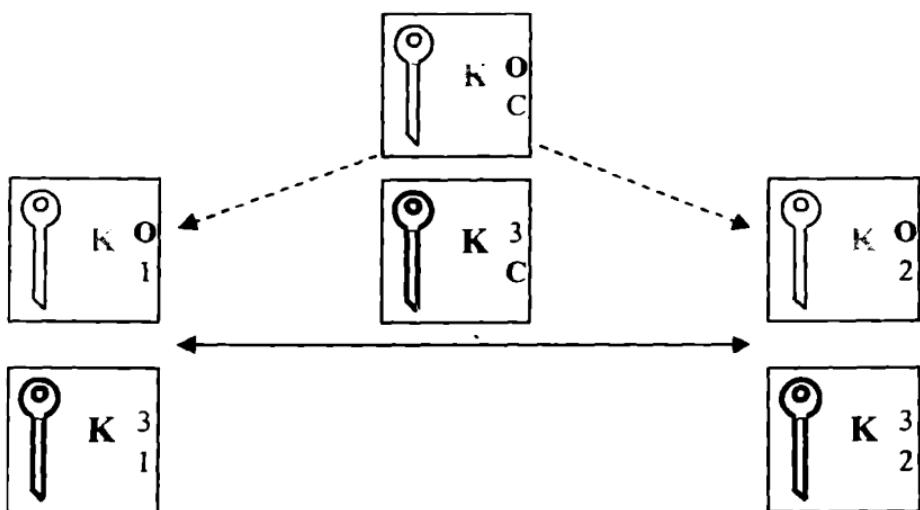
1-фойдаланувчи 2-фойдаланувчига шифрланган ахборотни жўнатган вактида нияти бузук одам @ уни ушлаб қолиши ва расшифровка килиши мумкин (унда 1-фойдаланувчи билан бўлинувчи сир  $K_{1@}$  бор). Сўнгра нияти бузук одам @ ахборотни (ўзгартирилгани бўлиши мумкин) ўзи ва 2-чи фойдаланувчи хисоблаган бўлинувчи сир  $K_{@2}$  дан фойдаланиб янгидан шифрлайди. Натижада, 2-фойдаланувчи 1-фойдаланувчи билан химояланган каналга эгаман деб ўйлаб, нияти бузук одам жўнатган ахборотни олади, расшифровка килади ва ишлатади.

Бу ҳужумга карши самарали восита – нотариус ёки сертификациялаш идораси CA (Certificate Authority). Очик калитларнинг нотариал тасдиқланган сертификатларини кўллаш man-in-the-middle ҳужумини олдини олишга имкон беради.

1-фойдаланувчи нотариусга боради, нотариус 1-фойдаланувчининг очик калитини ўзининг маҳфий калитидан фойдаланиб, электрон ракамли имзоси билан имзолайди. Бунда нотариус ракамли имзоси билан нафакат 1-фойдаланувчининг очик калитини, балки фойдаланувчи хусусидаги катор аниқ ахборотни (Ф.И.Ш., иш жойи ва х.) ҳамда имзонинг таъсир муддатини имзолайди. Ҳосил бўлган ҳужжат (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 хақиқатан 1 ёки 2- фойдаланувчига берилганлигини текширади. Нотариуснинг электрон ракамли имзосини текшириш фойдаланувчилар нотариусга ташриф буюрганларида эҳтиётдан олиб куйилган нотариусни очик калити ёрдамида шеригидан олган сертификатни расшифровка килиш оркали бажарилади. Натижада, нотариус СА оркали фойдаланувчилар орасида оддий ишонч занжири пайдо бўлади (8.2-расм).

Нияти бузук одам @ нотариусга бориб 1-фойдаланувчининг сертификатини ололмайди, чунки унга бу сертификатни олиш вактида паспортини кўрсатишига ва у 1- фойдаланувчи эканлигини исботлашига тўғри келади.



8.2-расм. Нотариус СА оркали фойдаланувчилар орасидаги оддий ишонч занжири.

**Очиқ калит сертификатлари.** Очик калит сертификатларини шакллантириш X.509 стандарт тарафидан тавсия этилган қатъий аутентификациялаш принципига ва очик калитли қриптотизим хусусиятларига асосланади.

Очиқ 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 раками имзо бўлади. Сертификация маркази СА сертификатлардаги очик калитларни аутентификациялашни таъминловчи ишончли учинчи томон хисобланади.

Сертификациялаш маркази ўзининг жуфт (очик-махфий) калитига эга бўлиб, маҳфий калит сертификатларни имзолаш учун ишлатилса, очик калит чоп этилади ва ундан фойдаланувчилар сертификатдаги очик калитнинг хақиқийлигини текширишда фойдаланадилар. Тарькидлаш лозимки, сертификация марказининг очик калитини хавфсиз узатиш нафакат сертификация марказига шахсан мурожаат асосида, балки бу очик калитни керакли ваколатга эга бўлган бошка сертификация маркази томонидан сертификациялаш асосида ҳам амалга ошириш мумкин. Сертификация маркази фойдаланувчининг очик калити сертификатини маълумотларнинг маълум тўпламини раками имзо билан тасдиқлаш орқали шакллантиради.

Одатда, маълумотларнинг бу тўпламига куйидагилар киради:

- очик калитнинг таъсир даври: даврнинг бошланиши ва нийояси саналарини ўз ичига олади;
  - калитнинг раками ва серияси;
  - фойдаланувчининг ноёб исми;
  - фойдаланувчининг очик калити хусусидаги ахборот: ушбу калит аталган алгоритмнинг идентификатори ва очик калитнинг ўзи;
  - электрон раками имзони текшириш муолажасида ишлатилувчи алгоритм (масалан, электрон раками 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 хеч бир томон сертификатни билинтиrmасдан ўзгартира олмайди (сертификатларни соҳталаштириш мумкин эмас).

Сертификатларни соҳталаштириш мумкин эмаслиги, уларни умумфойдаланувчи маълумотномаларда, химояламасдан чоп этишга имкон туғдиради.

Очиқ калит сертификатини яратиш жуфт жуфт калитни (очик-махфий) яратылған бошланади. Калитни генерациялаш мұолажаси қуидаги иккита усул орқали амалға оширилиши мүмкін:

– сертификация маркази калитлар жуфтини яратади. Очик калит сертификатга киритилади, унинг жуфти-махфий калит эса фойдаланувчига узатылади (фойдаланувчини аутентификациялашни ва калит узатилишининг конфиденциаллыгын таъминлаган холда).

– фойдаланувчи калитлар жуфтини ўзи яратади. Махфий калит фойдаланувчыда сакланади, очик калит эса химояланган канал орқали сертификация марказига юборилади.

Хар бир фойдаланувчи сертификация маркази томонидан шакилантирилған битта ёки бир нечта калитларнинг эгаси бўлиши мүмкін. Фойдаланувчи бир неча турли сертификация марказларидан олингандан сертификатларга ҳам эга бўлиши мүмкін.

Амалда бошка сертификация марказидан сертификат оладиган фойдаланувчиларни аутентификациялаш эктиёжи туғилади.

*Сертификатларни бошқариши тизимларининг базавий тузилматари.* Сертификатларни бошқариш тизими-ўзаро ахборот алмашища хавфсизликни таъминлаш максадида очик калитли криптографик технологиялардан фойдаланишга зарур бўлган дастурий-аппарат воситалари ҳамда ташкилий-техник тадбирлар комплекси.

Очиқ калитларни бошқариш инфратузилмаси PKI man-in-the-middle хужумларидан ишончли химоялашни амалға 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 қуидагиларга боғлик:

– ўзаро алокаси иштирокчилари сертификация маркази очик сертификатининг ҳақиқий нусхасига эга бўлишлари шарт;

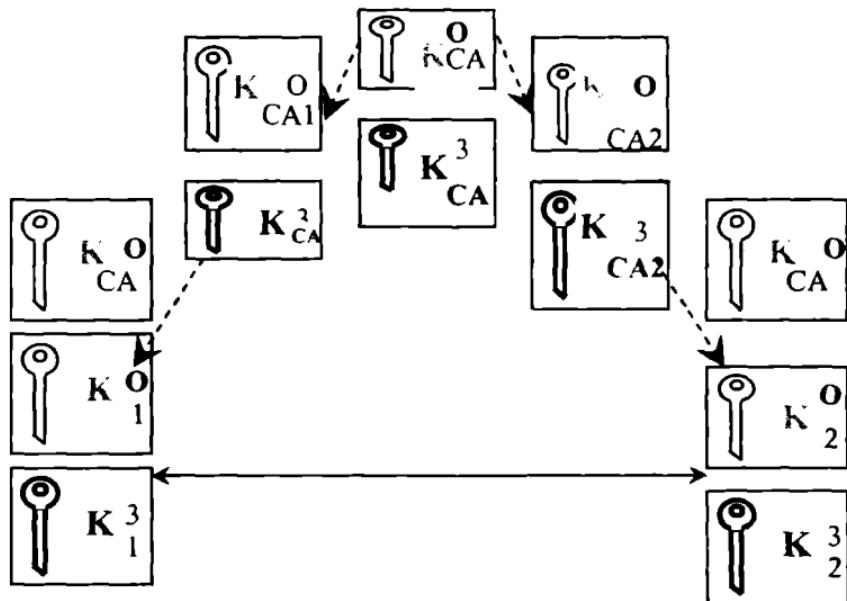
– ўзаро алокаси иштирокчилари ишлатадиган ахборотни химоялаш воситалари ўзаро алоқадаги шеригининг хар қандай сертификатини сертификация марказининг очик сертификатидан фойдаланиб автоматик тарзда текшира олиши лозим.

Баъзидан ўзаро алоқадаги шериклар сертификация марказидан жуда узокда бўлишлиги мүмкін. Бу холда СА, нотариусларининг таксимланган катламлари яратылади.

Сертификациялашнинг учта базавий модели фарқланади:

- сертификатларнинг иерархик (шажара) занжирига асосланган сертификациялашнинг иерархик модели;
- кросс-сертификациялаш модели (ўзаро сертификациялашни кўзда тутади);
- 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).*

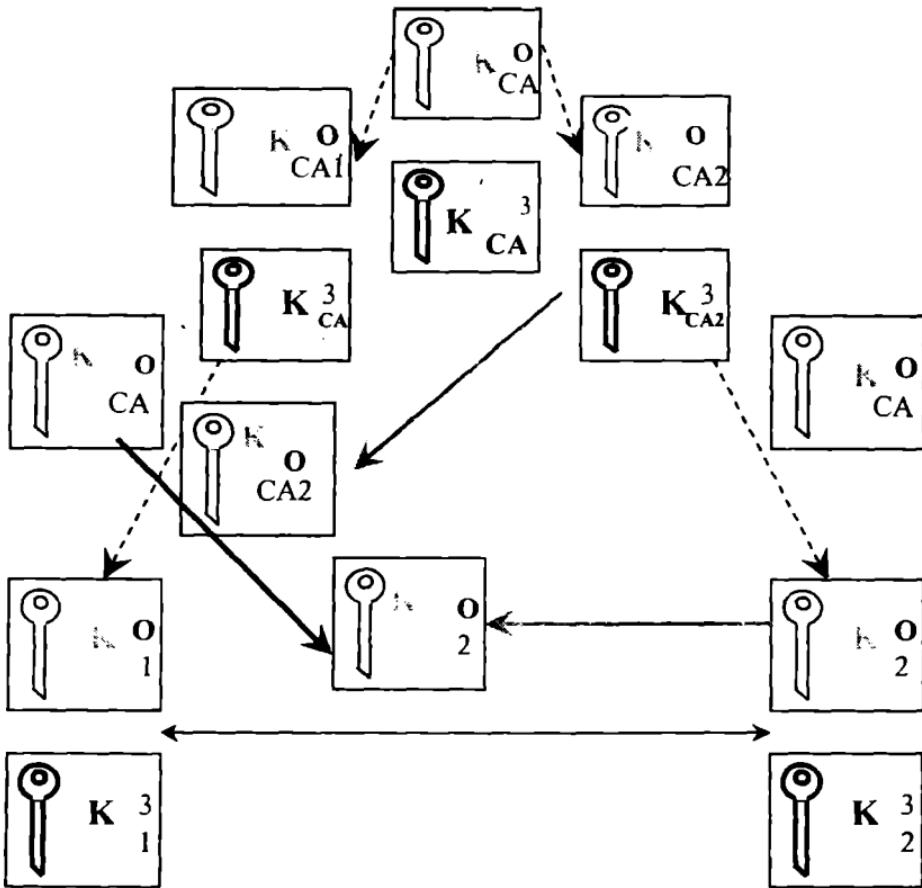


8.3-расм. САнинг икки сатҳли иерархияси.

Илдиз сертификация марказининг вазифаси тобе СА1 ва СА2ларни кайдлашдан иборат. Ҳар бир СА хавфсизликнинг ягона даражасини таъминлаш максадида сертификациялашнинг берилган сиёсатига мувоғик ишлайди. 8.3-расмда келтирилган мисолда СА нотариусларнинг яна бир иерархик сатҳи яратилиди. Нотариуслар:

- фойдаланувчиларга ўхшаб сертификатларини марказий САда имзолашади;
- марказий САга ўхшаб оддий фойдаланувчиларнинг сертификатларини маҳфий калитлари билан, имзолайдилар.

Масофадаги шерикнинг ҳакиқийлигини текшириш мантиқи куйидагича курилади (8.4-расм):



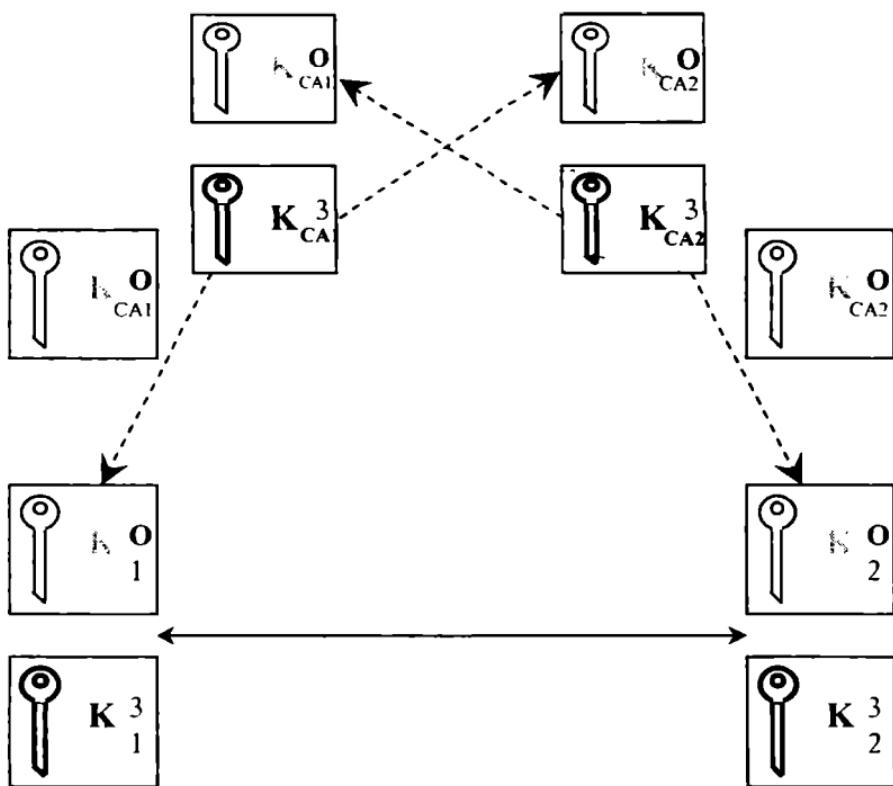
8.4-расм. Масофадаги абонент сертификатини текшириш схемаси.

- фойдаланувчи шеригининг сертификатини олиб, уни нотаниш СА имзолаганини аниклади;
- у шеригидан ушбу САнинг сертификатини сўрайди;
- САнинг сертификатини олиб, уни марказий СА сертификати билан текширади;
- муваффакиятли 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 бажараоли-

синлар. Тавсифланган иерархик схемани, зарурият туғилганда, иерархиянинг янги сатхларини киригип, давом эттириш мумкин.

Кросс-сертификациялаш моделида иерархиянинг бир шохидаги бўлмаган мустакил 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.

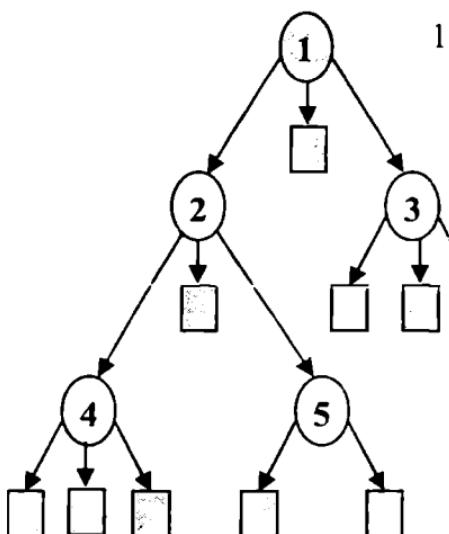
Таъкидлаш лозимки, кросс-сертификациялаш модели сертификатларни бошқариш тизимининг тармоқли архитектурасининг хусусий холи хисобланади.

Сертификатларни бошқариш тизимининг иерархик ва тармоқ архитектураларининг умумлаштирилган схемалари 8.6-расмда келтирилган.

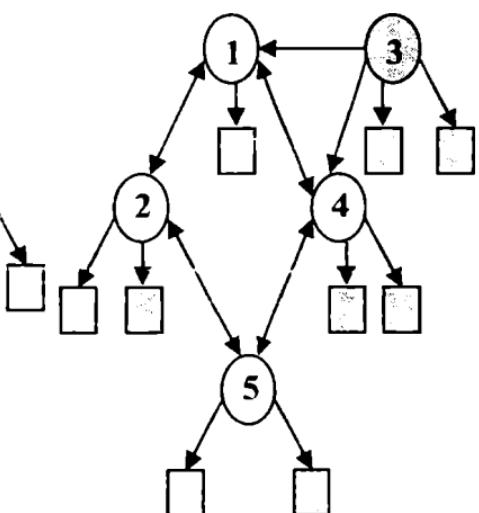
Сертификатларни бошкариш тизимининг иерархик тузилмаси куйидаги афзалликларга эга:

- у мавжуд федерал ва идора ташкилий-бошкарув тузилмаларга ўхшаш ва уларнинг принциплари бўйича қурилиши мумкин;
- у исмларнинг иерархик дараҳтига осонгина боғланиши мумкин;
- у ўзаро алоқадаги барча томонлар учун сертификатлар занжирини қидириш, қуриш ва верификациялашнинг оддий алгоритмини аниклайди;

Иерархик тузилма



Тармоқли тузилма



Сертификациялашнинг  
ишончли маркази



Сертификат чиқиши



Сертификациялашнинг  
тасдиқловчи маркази



Кросс-  
сертификациялаш



Фойдаланувчи

8.6-расм. Сертификатларни бошкариш тизимининг иерархик ва тармоқли архитектуралари.

– иккита фойдаланувчининг ўзаро алокани таъминлаши учун улардан бирининг иккинчисига ўзининг сертификатлар занжирини тақдим этиши кифоя, бу ўзаро алоқа билан боғлиқ муаммоларни камайтиради.

Иерархик архитектурага куйидаги камчиликлар характерли:

- барча охирги фойдаланувчиларнинг ўзаро алокасини таъминлаш учун фақат битта илдизли ишончли СА бўлиши шарт;
- тижорат тузилмаларининг ўзаро алокаси иерархикдан кўра кўпроқ тўғри характерга эга.

Сертификатларни бошкариш тизимининг *тармоқ архитектураси* куйидаги афзалликларга эга:

- у анчагина мослашувчан ва замонавий бизнесда мавжуд бўлган бевосита ишончли ўзаро муносабатларнинг ўрнатилишига имкон беради;
- охирги фойдаланувчи ҳеч бўлмагандга унинг сертификатини босиб чиқарган марказга ишониши шарт ва тизимдаги ишонч муносабатлари мана шунга асосланганд;
- фойдаланувчилари ўзаро тез-тез алоқа қилувчи турли тасдиковчи САларни бевосита кросс-сертификациялаш мумкин, бу занжирларни верификациялаш жараёнини қисқартиради;
- тасдиковчи СА калити обрўсизлантирилганидан сўнг тиклаш жараёни иерархик тузилмага караганда тармоқ тузилмасида оддийрок.

Аммо сертификатларни бошқаришнинг тармоқ архитектураси куйидаги камчиликларга эга:

- барча ўзаро алоқа томонлар учун сертификатлар занжирини қидириш ва қуриш алгоритми жуда мураккаб бўлиши мумкин;
- фойдаланувчи унинг сертификатини бошқа барча фойдаланувчилар томонидан текширилишини таъминловчи занжирни тақдим этаолмайди.

Эҳтимол, яқин орада сертификациялаш иерархиясининг энг юкори сатҳида турли ташкилотларнинг ишонч занжирлари алокасини таъминловчи давлат нотариуси бўлади.

## **8.2. Очиқ калитларни бошқариш инфратузилмасининг мантикий тузилмаси ва компонентлари**

Очиқ калитларни бошқариш инфратузилмаси РКИнинг асосий вазифалари қўйидагилар:

– ракамли калитлар ва сертификатларнинг ҳаёт циклини маддлаш (яъни калитларни генерациялаш, сертификатларни яратиш ва имзолаш, уларни тақсимлаш ва х.);

– обрўисизлантириш фактларини қайдлаш ва чакириб олинган сертификатларнинг «кора» рўйхатини чоп этиш;

– фойдаланувчининг тизимдан фойдаланиш вақтини имкони борича камайтирувчи идентификациялаш ва аутентификациялаш жараёнларини маддлаш:

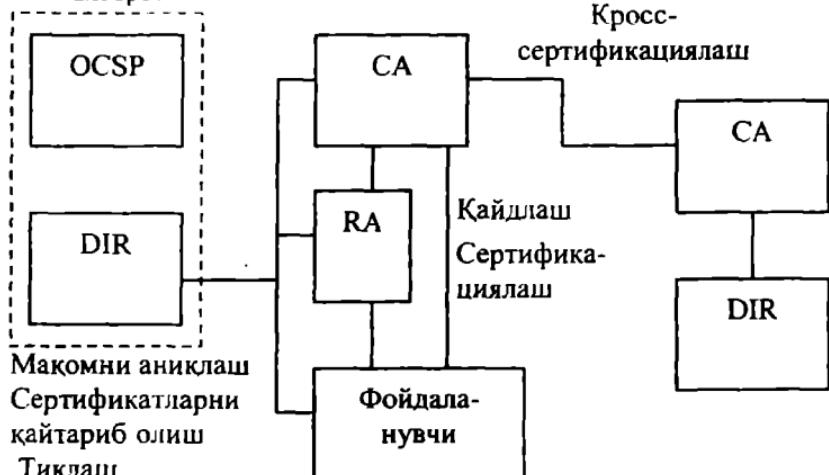
– мавжуд иловалар ва хавфсизлик кисм тизимининг барча компонентларини интеграциялаш механизмини (PKIга асосланган) амалга ошириш;

– барча фойдаланувчилар ва иловалар учун бир хил ва таркибида барча зарурий калит компонентлари ва сертификатлар бўлган хавфсизликнинг ягона токенидан фойдаланиш имкониятини тақдим этиш.

*Хавфсизлик токени* – фойдаланувчининг тизимдаги барча ҳукуклари ва курсовини аникловчи хавфсизликнинг шахсий воситаси, масалан смарт-карта.

8.7-расмда очик калитларни бошқариш инфратузилмасининг мантикий тузилмаси ва асосий компонентлари келтирилган.

#### Сертификатлар бўйича ахборот



8.7-расм. PKIning мантикий тузилмаси ва асосий компоненталари.

Расмда күйидаги белгилашлар қабул килинган:

- CA – сертификациялаш маркази;
- RA – кайдлаш маркази;
- OCSP – жорий сертификат мақомининг протоколи (Online Certificate Status Protocol);
- DIR – X.511, X.519, DAP, LDAP фойдаланиш протоколлари бўйича директория хизмати.

Кайдлаш маркази RA – PKI элементи, кайдлашни амалга оширувчи вакил, яъни фойдаланувчига сертификатни химояланган холда бериш имкониятини таъминлаш максадида фойдаланувчиларни аутентификациялашни ва уларни қайдлашни амалга оширади. Қайдлаш марказининг хусусияти шундан иборатки, у функционал нуктаи назаридан сертификация марказига қараганда фойдаланувчига яқинрок. Ундан ташқари, айнан қайдлаш маркази PKIning ўзаро алокага лаёқатлигини таъминловчӣ самарали интерфейс хисобланади.

Сертификация маркази CA – PKIning элементи (сертификатларнинг ишончли манбай, нотариус), унга сертификатларни яратиш ва ёки тасдиклаш ишониб топширилган. Сертификация марказининг ишлаш схемаси кўйидагича:

- CA шахсий калитларини генерациялайди ва фойдаланувчилар сертификатларини текширишга аталган CA сертификатларини шакллантиради;
- фойдаланувчилар сертификациялашга сўровларни шакллантирадилар ва уларни у ёки бу усул бўйича CAга етказадилар;
- CA фойдаланувчилар сўровлари асосида уларнинг сертификатларини шакллантиради;
- CA бекор килинган сертификат рўйхатларини (CRL) шакллантиради ва вакти-вакти билан янгилайди;
- фойдаланувчи сертификатлари, CA сертификатлари ва бекор килинганлар рўйхати CRL сертификатлар маркази томонидан чоп этилади (фойдаланувчиларга тарқатилади ёки умумфойдаланувчи маълумотномага жойлаштирилади).

PKI бажарадиган функцияларни шартли равишда бир неча гурӯхларга ажратиш мумкин:

- сертификатларни бошкариш функциялари;
- калитларни бошкариш функциялари;
- қўшимча функциялар (хизматлар).

Сертификатларни бошқариш функцияларига қуидагилар киради:

– қайдлаш. Нафакат функцияларнинг бир қисми, балки РКИнинг хавфсизлиги хам түгри қайдлашга ва идентификациялашга асосланган. Фойдаланувчилар сифатида физик фойдаланувчилар, татбикй дастур, тармок қурилмаси ва х. иштирок этиши мумкин. Идентификациялащда ишлатиладиган усулларни сертификациялаш сиёсати белгилайди. Шундай қилиб, фойдаланувчиларни идентификациялаш ва қайдлаш РКИ тизимининг минимал түлик компонентлари хисобланади;

– очиқ қалитларни сертификациялаш. Сертификациялаш жараёнига сертификациялаш маркази СА жавоб беради. Мохияттан, сертификациялаш жараёни фойдаланувчи исмини очиқ қалит билан боғлашдан иборат.

СА куйидаги харакатларни бажарган ҳолда фойдаланувчи ва пастрок сатхдаги СА сертификатларини имзолайди:

- фойдаланувчиларнинг хакиқийлигини текшириш;
- сертификатга идентификатор бериш;
- маълумотларни сертификатга киритиш;
- харакат вактини (бошланиш-ниҳояси) ўрнатиш;
- сертификатни имзолаш;
- сертификатни сертификатларнинг очиқ серверида чоп этиш.

*САнинг маҳфий қалитини сақлаш.* Бу тизимнинг энг нозик нуктаси. СА маҳфий қалитининг обрўсизлантирилиши унинг ихтиёридаги бутун тизимни бузади. *САнинг маҳфий қалити жойлашган компьютер ишончли кўрикланиши лозим;*

– *сертификатлар базасини сақлаш ва сертификатларни тақсимлаш.* Тизим ишлашининг қулийлигини таъминлаш максадида фойдаланувчиларнинг ва оралик САларнинг (энг юкори сатҳ ҶАсидан бўлак) барча сертификатлари сертификатлар сервери деб атальувчи умумфойдаланувчи серверга олиб қўйилади. Бу ҳолда фойдаланувчилар абонентнинг сертификатини, ҳатто у тармокда вактинча бўлмаган ҳолда хам, олишлари мумкин;

– *сертификатни янгилаш.* Ушбу жараён сертификат таъсири муддати ўтган ҳолда фаоллашади ва фойдаланувчи очиқ қалити учун янги сертификатни беришдан иборат бўлади. Агар қалитлар жуфти обрўсизлантирилган бўлса ёки янги сертификат сиёсат, кенгайиш ёки хусусият атамаларида олдингисидан фарқланса бу усул ишлатилмайди. Яроқлилик муддати даврида сертификатнинг исми

ва мансублиги (фойдаланувчининг бошка бўлимга ўтиши) каби жиддий бўлмаган хусусиятларининг ўзгариши ҳам сертификатни олдинги очик қалит билан янгилашни (регенерациялашни) талаб этишга олиб келиши мумкин.

– қалитларни янгилаш. Фойдаланувчилар ёки учинчи томон қалитларнинг янги жуфтини генерациялаганларида янги очик қалитга мос келувчи сертификатни яратиш зарур. Бу усульдан сертификатни янгилаш мумкин бўлмаган ҳолларида ҳам фойдаланилади;

– сертификатни қайтариб олиши мақомини аниқлаш. Ушбу жараён фойдаланувчига сертификатининг қайтариб олинган эмаслигини текширишга имкон беради. Бу жараён сертификатнинг очик қалитлар 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, қалитларнинг обрўсизлантирилиши, исмларнинг ўзгариши, фойдаланишнинг тўхташи ва х.) бўлиши мумкин.

– қалитларни бошқарииш функцияси – қалитларни генерациялаш ва таксимлаш асосий кисм гурухларига бўлинади.

*Калитларни тақсимлаш функциялари* ўз навбатида очик қалитларни тақсимлаш ва токенларни персоналлаштиришга бўлинади. Токенларни персоналлаштиришда физик курилмалар – токенлардан фойдаланиб махфий қалитларни ва кўшимча маълумотларни саклаш ташкил этилади; токенларнинг персонализацияси CA, RA ва фойдаланувчи томонидан мададланиши лозим. Масалан, смарт-картанинг персонализацияси ўрнатиш (файл тизимини яратиш) муолажасини, тасодифий PIN-кодни ёки паролни танлаш, бу смарт-картага тегишли барча маълумотларни етказиш ва саклашни ўз ичига олиши мумкин.

Кўшимча функциялар (хизматлар) гурухи таркибига куйидагилар киради:

– ўзаро сертификациялаш (турли САларда кросс-сертификациялаш);

– очик қалитни унинг унга куйиладиган арифметик талабларга мос келишини, яъни очик қалит ҳакиқий эканлигини текшириш;

– сертификатни текшириш; агар фойдаланувчи бошка фойдаланувчининг ракамли имзосига ишонишни хоҳласа ва мос серти-

фикатни текшираолмаса, текширишни ишончли учинчи томондан илтимос қилиши мумкин;

- архивлаш хизматлари ва x.

Очиқ калитлар инфратузилмаси PKI күйидаги катор иловалар ва стандартларни мададлайды:

- 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 тармокларни (VPN) ташкил этиш воситалари, хусусан Cisco Systems, Nortel Network компанияларининг телекоммуникация асбоб-ускуналари ҳамда ихтисослаштирилган дастурий гаъминот.

- электрон хужжат 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 x.

Ўз навбатида, очик калитлар инфратузилмаси санаб ўтилган функционал соҳаларни интеграциялаши мумкин. Натижада, очик калитлар инфратузилмаларини компания ахборот тизимиға интеграциялаш ва умумий стандартлар ва очик калит сертификатларидан фойдаланиш йўли билан ахборот хавфсизлигининг комплекс тизимини яратиш мумкин.

Юкорида келтирилганлар очик калитлар инфратузилмасини яратиш ва мададлаш хизматлари аҳамиятини ошишига олиб келади.

## **IX боб. АХБОРОТ-КОММУНИКАЦИОН ТИЗИМЛАРДА СУҚИЛИБ КИРИШЛАРНИ АНИҚЛАШ**

### **9.1. Хавфсизликни адаптив бошқариш концепцияси**

Ташкилотларда химоялаш билан боғлиқ бўлган муаммоларни ечиш учун аксарият ҳолларда кисман ёндашишлардан фойдаланишади. Бу ёндашишлар, одатда, аввало, фойдалана олувчи ресурсларнинг жорий даражаси орқали аникланади. Ундан ташкари, хавфсизлик маъмурлари кўпинча ўзларига тушунарли бўлган хавфсизлик хавф-хатарларига реакция кўрсатишади. Аслида хавф-хатарлар жуда кўп бўлиши мумкин. Корпоратив ахборот тизимини факат катъий жорий назорати ва хавфсизликнинг умумий сиссатини таъминловчи комплекс ёндашиш хавфсизлик хавф-хатарларини анчагина камайтириши мумкин.

Охирги вактда турли компаниялар томонидан қатор ёндашишлар ишлаб чиқилдики, бу ёндашишлар нафақат мавжуд заифликларни аниклашга, балки ўзгарган эски ёки пайдо бўлган янги заифликларни аниклашга ва уларга мос химоялаш воситаларини карши кўйишга 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 вакт режимида назоратлаш, аниклаш ва уларга реакция кўрсатишга имкон беради.

Тармокнинг адаптив хавфсизлиги куйидаги асосий учта элемент орқали таъминланади:

- хавф-хатарларни баҳолаш;
- химояланишни таҳлиллаш;
- хужумларни аниклаш.

*Хавф-хатарларни баҳолаш.* Заифликларни (келтирадиган зарарнинг жиддийлик даражаси бўйича), тармоқ кисм тизимларини

(жиддийлик даражаси бўйича), таҳдидларни (уларнинг амалга оширилиши эҳтимоллиги бўйича) аниклаш ва рутбалашдан иборат. Тармоқ конфигурацияси муттасил ўзгариши сабабли, хавфхатарларни баҳолаш жараёни ҳам узлуксиз ўтказилиши лозим. Корпоратив аҳборот тизимининг химоялаш тизимини қуриш хавфхатарларни баҳолашдан бошланиши лозим.

*Химояланишини таҳлиллаш* – тармоқнинг заиф жойларини кидириш. Тармоқ уланишлардан, узеллардан, хостлардан, ишчи станциялардан, иловалардан ва маълумот базаларидан таркиб топган. Буларнинг барчаси химояланиш самарадорлигининг сакланишига ҳамда ноъмалум заифликларининг аникланишига муҳтож. Химояла-нишни таҳлиллаш технологияси тармоқни тадқиклаш, нозик жойларини топиш, бу маълумотларни умумлаштириш ва улар бўйича хисобот бериш имкониятига эга. Агар бу технологияни амалга оширувчи тизим адаптив компонентга ҳам эга бўлса, аникланган заифликларни автоматик тарзда бартараф этиш мумкин. Химояланиши таҳлиллаш технологияси тармоқ хавфсизлиги сиёсатини, уни ташкилот ташқарисидан ёки ичкарисидан бузишга урнишлардан олдин, амалга оширишга имкон берувчи таъсирчан усул хисобланади.

Химояланиши таҳлиллаш технологияси томонидан идентификацияланувчи муаммоларнинг баъзилари куйидагилар:

- тизимлардаги «тешиклар» (*back door*) ва троян оти хилидаги дастур;
- кучсиз пароллар;
- химояланмаган тизимдан сукилиб киришга ва «хизмат килишдан воз кечиш» хилидаги хужумларга таъсирчанлик;
- операцион тизимлардаги зарурий янгиланишларнинг йўклиги;
- тармоқларо экранларнинг, Web-серверларнинг ва маълумотлар базасининг нотўғри созланиши ва х.

*Хужумларни аниклаш* – корпоратив тармоқдаги шубҳали характеристларни баҳолаш жараёни. Хужумларни аниклаш операцион тизим ва иловаларни кайдлаш журнallарини ёки реал вактдаги трафикни таҳлиллаш орқали амалга оширилади. Тармоқ узеллари ёки сегментларида жойлаштирилган хужумларни аниклаш компонент-

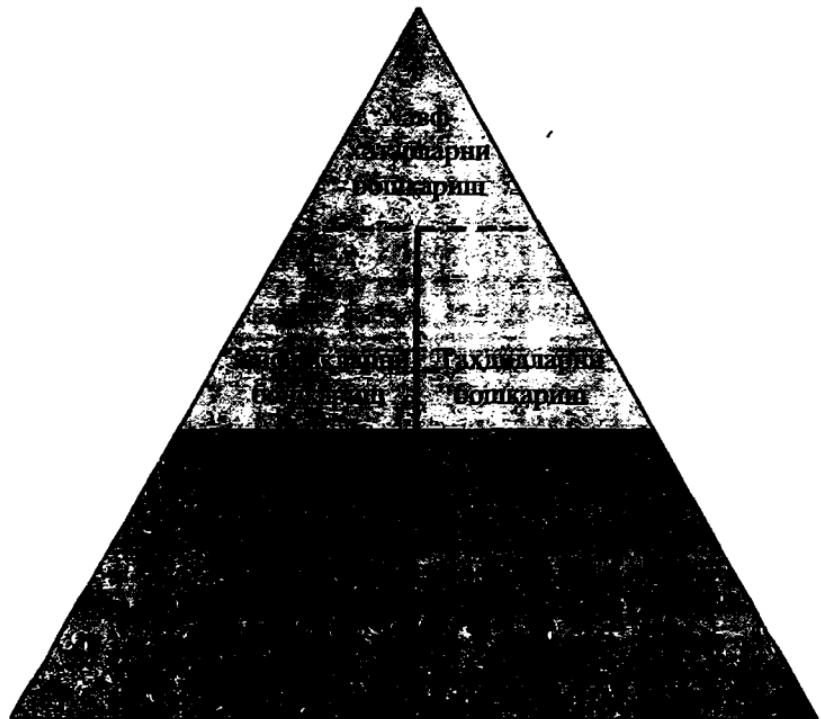
лари турли ходисаларни, хусусан, маълум заифликлардан фойдалана-  
нувчи харакатларни ҳам баҳолайди (9.1-расм).



9.1-расм. Химояланганликни таҳлиллаш ва ҳужумларни аниклаш тизимларининг ўзаро алокаси.

Хавфсизликни адаптив бошқариш модели ANSning адаптив компоненти, янги заифликлар хусусидаги энг охирги ахборотни тақдим қилган ҳолда, химояланишини таҳлиллаш жараёнини модификациялашга жавоб беради. У ҳужумларни аниклаш компонентини ҳам, уни ҳужумлар хусусидаги охирги ахборот билан тўлдириш оркали, модификациялади. Адаптив компонентнинг мисоли сифатида янги вирусларни аниклаш учун вирусга карши дастурнинг маълумотлар базасини янгилаш механизмини кўрсатиш мумкин.

Хавфсизликни адаптив бошқариш моделидан (9.2-расм) фойдаланиш барча таҳдидларни назоратлаш ва уларга ўз вактида самарали реакция кўрсатиш имконини беради. Бу эса ўз навбатида, нафакат таҳдидларнинг амалга оширилишига сабаб бўлувчи заифликларни бартараф килишга, балки заифликлар пайдо бўлиш шароитларини таҳлиллашга имкон беради.



9.2-расм. Хавфсизликни адаптив бошқариш модели.

Тармок хавфсизлигини адаптив бошқариш модели тармоқда суистеммол қылышни камайтиришга, тармоқдаги ходисалардан фойдаланувчилар, маъмурлар ва компания раҳбариятининг хабардорлик даражасини ошишига ҳам имкон беради. Гаъкидлаш лозимки, ушбу модель олдин ишлатилувчи ҳимоялаш механизмларидан (фойдаланишни чегаралаш, аутентификациялаш ва х.) воз кечмайди. Уларнинг функционаллигини янги технология эвазига кенгайтиради. Ўзларининг ахборот хавфсизлигини таъминлаш тизимларини замонавий талабларга мос келишини хоҳловчи ташкилотлар мавжуд ечимларни учта янги компонент-ҳимояланишни тахжиллаш, ҳужумларни аниклаш ва хавф-хатарни баҳолаш билан гўлдириши лозим.

## 9.2. Ҳимояланишни таҳлиллаш

Ҳимояланишни таҳлиллаш воситалари заифликларни топиб ва ўз вактида йўқ килиб ҳужумни амалга ошириш имкониятини бартараф килади. Натижада, ҳимоялаш воситаларини ишлатилишига бўладиган барча сарф-харажатлар камаяди.

Ҳимояланишни таҳлиллаш воситалари тармок сатҳида, операцион тизим сатҳида ва иловалар сатҳида ишлаши мумкин. Улар текширишлар сонини бора-бора кўпайтириш, ахборот тизимиға «ичкарилаб бориш» ва унинг барча сатҳларини тадқиқлаш орқали заифликларни кидириши мумкин.

*Тармоқ протоколлари ва сервислари ҳимояланишини таҳлиллаш воситалари.* Ҳар кандай тармоқда абонентларнинг ўзаро алокаси иккита ва ундан кўп узеллар орасида ахборот алмашиниш муолажаларини белгиловчи тармок протоколлари ва сервисларидан фойдаланишга асосланган. Тармок протоколлари ва сервисларини ишлаб чикишда уларга ишланувчи ахборот хавфсизлигини тъминлаш бўйича талаблар (одатда, шубҳасиз етарли бўлмаган) кўйилган. Шу сабабли, тармок протоколларида аниқланган заифликлар хусусида 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 одамарнинг корпоратив тармоқларга ҳужумларида қўлланылганига ўхшаш.

Заифликларни аниқлаш максадида сканерлаш текширувчи тизим хусусидаги дастлабки ахборотни, хусусан, рухсат этилган протоколлар ва очик портлар, операцион тизимнинг ишлатилувчи версиялари ва х. хусусидаги ахборотни олиш билан бошланади. Сканерлаш кенг тарқалган ҳужумлар, масалан, тўлиқ саралаш усули бўйича паролларни танлашдан фойдаланиб, суқилиб киришни имитациялашга уриниш билан тугайди.

Ҳимояланишни таҳлиллаш воситалари ёрдамида тармок сатҳида нафакат Internet нинг корпоратив тармоқдан рухсатсиз фойдаланиши имкониятини тестлаш, балки ташкилот ички тармоғида текширишни амалга ошириш мумкин. Тармок сатҳида ҳимояланишни таҳлиллаш тизими ташкилот хавфсизлик даражаси-

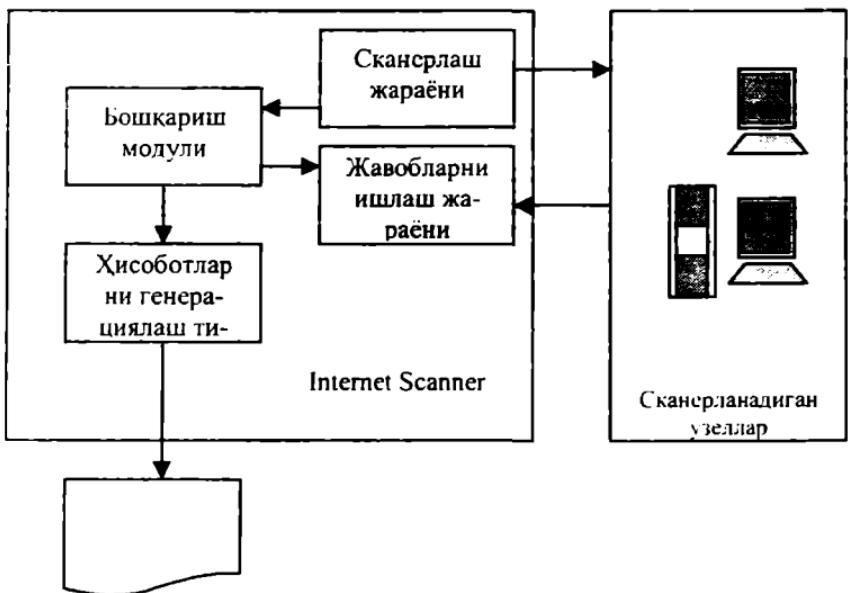
ни баҳолашга ҳамда тармок дастурий ва аппарат таъминотини созлаш самарадорлигини назоратлашга хизмат килади.

Химояланишни таҳлиллашни амалга оширувчи (Internet Scanner гизими мисолида) намунавий схема 9.3-расмда келтирилган.

Химояланишни таҳлиллаш воситаларининг бу синфи нафакат тармок протоколлари ва сервислари, балки тармок билан ишлашга жавобгар тизимли ва татбикӣ дастурий таъминоти заифликларини ҳам таҳлиллади. Бундай таъминот қаторига Web-, FTP-, ва почта серверларини, тармокларо экранларни, браузерларни ва х. киритиш 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 химояланишига таъсир эгувчи унинг созланишларини текширишга аталган. Бундай созлашлар қуидагиларни аниклади:



9.3-расм. Internet Scanner тизими мисолида химояланганликни таҳлиллаш схемаси.

- фойдаланувчиларнинг хисоб ёзуви, масалан, парол узунлиги ва унинг таъсир муддати;
- фойдаланувчиларнинг жиддий тизимли файллардан фойдаланиш хуқуклари;
- заиф тизимли файллар;
- ўрнатилган патчлар ва х.

Операцион тизим сатхидаги ҳимояланишни тахлиллаш тизимлари операцион тизимлар конфигурациясини назоратлашда ҳам ишлатилиши мумкин.

Тармок сатхи ҳимояланишни тахлиллаш воситаларидан фарқли равишда, ушбу тизимлар тахлиланувчи тизимни ташкаридан эмас, балки ичкаридан сканерлайди, яъни улар ташкаридаги нияти бузук одамлар хужумларини имитацияламайди. Операцион тизим сатхидаги ҳимояланишни тахлиллаш тизимларининг баъзилари (масалан, Internet Security Systems компаниясининг System Scanner тизими) заифликларни аниклаш имкониятидан ташкари, аникланган муаммоларнинг бир кисмини автоматик тарзда бартараф килишга ёки ташкилотда кабул килинган хавфсизлик сиёсатини конктирумайдиган тизим параметрларига тузатиш киритишга имкон беради.

*Танланувчи ҳимоялашини таҳлиллаш воситаларига қўйиладиган умумий талаблар.* Танланувчи тизимга қўйиладиган мажбурий талаб-корхона тармоқ инфратузилмасини ўзгартириш зарурятининг йўклиги. Акс ҳолда бундай кайтадан ташкил этишга килинадиган харажат ҳимояланишни тахлиллаш тизими нархидан ошиб кетиши мумкин. Ҳозирда бу талабга факат Internet Security Systems компаниясининг Security Systems тизими жавоб беради.

Ҳимояланишни тахлиллаш воситаларини нотўғри ишлатиш улардан нияти бузук одамларнинг корпоратив тармоққа сукилиб кириш учун фойдаланишларига имкон яратади. Шу сабабли, ҳимояланишни тахлиллаш воситалари ўзларининг компонентларидан ва йигилган маълумотлардан фойдаланишни чегараловчи механизmlар билан таъминланиши лозим. Бундай механизмларга куйидагилар киради:

- факат маъмур хуқукига эга бўлган фойдаланувчи томонидан ушбу воситаларни ишга тушириш;
- сканерлаш маълумотлари архивини шифрлаш;
- масофадан бошқаришда уланишни аутентификациялаш;
- каталоглар билан ишлаш учун маҳсус хуқукларни аниклаш .х.

Заифликларни аниклаш жараёнининг қуидаги имкониятлари-га эътиборни қартиш лозим:

- бир неча курилма ёки сервисларни параллел ишлаш эвазига сканерлаш тезлигини ошириш;
- тизимдан рухсатсиз фойдаланишни олдини олиш учун ҳар бир сканерланувчи узелга билдириш коғозини юбориш;
- ёлғон ишлашларни минималлаштириш учун тармоқни эксплуатация талабларига түғрилаш.

Корпоратив тармок холатининг доимо ўзгариб туриши, унинг ҳимояланишига таъсир кўрсатади. Шу сабабли, ҳимояланишни таҳлиллашнинг яхши тизими жадвал бўйича ишлаш режимига эга бўлиб, маъмур уни эслагунича ўзи тармок узеллари заифликларини текшириши ва пайдо бўлган муаммолар хусусида нафакат маъмурни огоҳлантириши, балки аникланган заифликларни йўқотиш усулларини тавсия этиши лозим.

Эътибор бериш зарур бўлган характеристикалардан бирисоботларни 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 мухим хисобланади. Факат матнли ахборот билан тўлдирилган ҳужжатларнинг фойдаси бўлмайди. Графиклардан фойдаланиш эса маъмурга ташкилот тармоғидаги барча муаммоларни яққол намоийиш этишга имкон беради. Ҳисоботларда аникланган муаммоларни йўқотиш бўйича тавсияларнинг мавжудлиги ҳимояланишни таҳлиллаш воситаларини танлашдаги мажбурий шарт хисобланади.

Доимо янги заифликларнинг аникланиши ҳимояланишни таҳлиллаш тизимининг заифликлар маълумотлари базасини тўлдира олиши имкониятига эга бўлишини такозо этади. Бу заифликларни тавсифловчи маҳсус тил ёрдамида ёки тизим ишлаб чиқарувчилари томонидан заифликларни вакти-вакти билан тўлдириш йўли билан амалга оширилади. Корпоратив тармок узелларининг ҳимояланиш даражасининг ўзгаришини таҳлиллаш учун танланувчи восита ўтказилган сканерлаш сеанслари хусусидаги ахборотни тўпланишига имкон бериши лозим.

### 9.3. Ҳужумларни аниклаш

*Тармоқ ахборотини таҳлиллаш усуллари.* Моҳияти бўйича, ҳужумларни аниклаш жараёни корпоратив тармоқда бўлаётган шубҳали ҳаракатларни баҳолаш жараёнидир. Бошқача айтганда ҳужумларни аниклаш хисоблаш ёки тармок ресурсларига йўналтирилган шубҳали ҳаракатларни идентификациялаш ва уларга реакция кўрсатиш жараёни. Ҳозирда ҳужумларни аниклаш тизимида қуидаги усуллар ишлатилади:

- статистик усул;
- эксперт тизимлари;
- нейрон тармоқлари.

*Статистик усул.* Статистик ёндашишнинг асосий афзаллиги – аллақачон ишлаб чиқилган ва ўзини танитган математик статистика аппаратурини ишлатиш ва субъект характерига мослаш.

Аввал таҳлилланувчи тизимнинг барча субъектлари учун профиллар зникланади. Ишлатиладиган профилларнинг эталондан ҳар қандай четланиши рухсат этилмаган фойдаланиш хисобланади. Статистик усуллар универсал хисобланади, 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 сезувчан маслар; баъзи ҳолларда бир ходисанинг ўзи, келиши тартибига кўра аномал ёки нормал фаолиятни характерлаши мумкин.

2. Аномал фаолиятни адекват идентификациялаш максадида ҳужумларни аниклаш тизими томонидан кузатилувчи характеристикалар учун чегаравий (бўсағавий) кийматларни бериш жуда кийин.

3. Статистик усуллар вакт ўтиши билан бузғунчилар томонидан шундай «ўрганилиши» мумкинки, ҳужум ҳаракатлари нормал каби қабул килинади.

*Эксперт тизимлари.* Эксперт тизими одам-эксперт билимларини камраб олувчи коидалар тўпламидан ташкил топган. Эксперт тизимидан фойдаланиш ҳужумларни аниклашнинг кенг тарқалган усули бўлиб, ҳужумлар хусусидаги ахборот коидалар кўринишида ифодаланади. Бу коидалар ҳаракатлар кетма-кетлиги ёки сигнатуралар кўринишида ёзилиши мумкин. Бу коидаларнинг ҳар бирининг бажарилишида рухсатсиз фаолият мавжудлиги хусусида

карор қабул килинади. Бундай ёндашишнинг муҳим афзалиги – ёлғон тревоганинг умуман бўлмаслиги.

Эксперт тизимининг маълумотлари базасида ҳозирда маълум бўлган аксарият хужумлар сценарияси бўлиши лозим. Эксперт тизимлари, долзарбликни саклаш максадида, маълумотлар базасини муттасил янгилашни талаб этади. Гарчи эксперт тизимлари кайдлаш журнallаридағи маълумотларни кўздан кечиришга яхши имкониятни тавсия килсада, сўралған янгиланиш эътиборсиз колдирилиши ёки маъмур томонидан қўлда амалга оширилиши мумкин. Бу энг камида, эксперт тизими имкониятларининг бўшашига олиб келади.

Эксперт тизимларининг камчиликлари ичida энг асосийси – номаълум хужумларни акслантира олмаслиги. Бунда олдиндан маълум хужумнинг хатто озгина ўзгариши хужумларни аниклаш тизимининг ишлашига жиддий тўсик бўлиши мумкин.

*Нейрон тармоқлари.* Хужумларни аниклаш усулларининг аксарияти коидалар ёки статистик ёндашиш асосида назоратланувчи муҳитни таҳлиллаш шаклларидан фойдаланади. Назоратланувчи муҳит сифатида кайдлаш журнallари ёки тармоқ трафиги кўрилиши мумкин. Бундай таҳлиллаш маъмур ёки хужумларни яниклаш тизими томонидан яратилган, олдиндан аникланган коидалар тўпламига таянади.

Хужумни вакт бўйича ёки бир неча нияти бузук одамлар ўртасида ҳар қандай бўлининиши эксперт тизимлар ёрдамида аниклашга қийинчилик туғдиради. Хужумлар ва улар усулларининг турли-туманлиги туфайли, эксперт тизимлари коидаларининг маълумотлар базасининг хатго, доимий янгиланиши ҳам хужумлар диапазонини аник идентификациялашни кафолатламайди.

Нейрон тармоқларидан фойдаланиш эксперт тизимларининг юкорида келтирилган муаммоларни бартараф этишининг бир усули хисобланади. Эксперт тизимлари фойдаланувчига кўрилаётган характеристикалар маълумотлар базасидаги коидаларга мос келиши ёки мос келмаслиги хусусида аник жавоб беролса, нейротармоқ ахборотни таҳлиллайди ва маълумотларни аниклашга ўрганган характеристикаларига мос келишини баҳолаш имкониятини тақдим этади. Нейротармоқли ифодалашнинг мослих даражаси 100 %га этиши мумкин, аммо танлаш хақиқийлиги тамоман қўйилган масала мисолларини таҳлиллаш сифатига боғлик.

Аввал предмет соҳасининг олдиндан танлаб олинган мисолида нейротармокни тӯғри идентификациялашга «ўргатишади». Нейротармок реакцияси таҳлиланади, коникарли натижаларга эришиш мақсадида тизим созланади. Нейротармок ҳам вакт ўтиши билан, предмет соҳаси билан боғлик маълумотларни таҳлиллашни ўтказишига караб «тажриба орттиради».

Нейротармокларнинг сунистъемол килинишни аниклашдаги муҳим афзалиги, уларнинг атайин килинадиган хужумлар характеристикаларини «ўрганиш» ва тармокда олдин қузатилганига ўхшамаган элементларни идентификациялаш кобилиятидир.

Юкорида тавсифланган хужумларни аниклаш усуулларининг ҳар бири афзаликларга ва камчиликларга эга. Шу сабабли, хозирда тавсифланган усуулларнинг факат биттасидан фойдаланувчи тизими учратиш кийин. Одатда, бу усууллар биргаликда ишлатилади.

*Хужумларни аниклаш тизимларининг туркумланиши.* Хужумларни аниклаш тизимлари IDS(Intrusion Detection System)да ишлатилувчи хужумларни аникловчи механизмлар бир неча умумий усуулларга асосланган. Таъкидлаш лозимки, бу усууллар бир-бiriни инкор ётмайди. Аксарият тизимларда бир неча усуулларнинг комбинациясидан фойдаланилади.

Хужумларни аниклаш тизимлари куйидаги аломатлари бўйича туркумланиши мумкин:

- реакция кўрсатиш усули бўйича;
- хужумларни фош этиш усули бўйича;
- хужум хусусидаги ахборотни йигиш усули бўйича.

Реакция кўрсатиш усули бўйича пассив ва актив IDSлар фарқланади. Пассив IDS лар хужум фактларини кайдлайди, маълумотларни журнал файлига ёзади ва огохлантиришлар беради. Актив IDSлар, масалан, тармокларро экранни кайта конфигурациялаш ёки маршрутизатордан фойдаланиш рўйхатини генерациялаш билан хужумга карши харакат килишга уринади.

Хужумларни фош этиши усули бўйича IDSларни куйидаги иккита категорияга ажратиш кабул килинган:

- аномал хатти-харакатни аниклаш (anomaly-based);
- сунистъемолликларни аниклаш (misuse detection ёки signature-based).

Аномал хатти-харакатни аниклаш йўли билан хужумларни аниклаш технологияси куйидаги гипотезага асосланган. Фойдаланувчининг аномал хатти-харакати (яъни хужуми ёки қандайдир

гаразли ҳаракати) – нормал хатти-харакатдан четлашиш. Аномал хатти-харакатга мисол тарикасида киска вакт оралиғида уланишларнинг катта сонини, марказий процессорнинг юқори юкланишини ва x. кўрсатиш мумкин.

Агар фойдаланувчининг нормал хатти-харакати профилини бир маънода тавсифлаш мумкин бўлганида, ундан ҳар қандай четланишларни аномал хатти-харакат сифатида идентификациялаш мумкин бўлар эди. Аммо, аномал хатти-харакат ҳар доим хам хужум бўлавермайди. Масалан, тармок маъмури томонидан юборилган кўп сонли сўровларни хужумларни аниклаш 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-харакатни аниклаш ва уни хужумлар синфиға киритиш;
- аномал хатти-харакат таърифиға мос келмайдиган хужумларни ўtkазиб юбориш. Бу ҳолат хужум бўлмаган аномал хатти-харакатни хужумлар синфиға киритишга нисбатан хавфлирок хисобланади.

Бу категория тизимларини созлашда ва эксплуатациясида маъмур қўйидаги кийинчиликларга дуч келади:

- фойдаланувчи профилини куриш сермехнат масала бўлиб, маъмурдан катта дастлабки ишларни талаб этади.
- юкорида келтирилган иккита кескин ҳаракатлардан бирининг пайдо бўлиши экстимоллигини пасайтириш учун фойдаланувчи хатти-харакатининг чегаравий кийматларини аниклаш зарур.

Аномал хатти-харакатларни аниклаш технологияси хужумларнинг янги хилини аниклашга мўлжалланган. Унинг кимчилиги – доимо «урганиш» зарурияти.

Сунистеммолликларни аниклаш йўли билан хужумларни аниклаш технологиясининг моҳияти хужумларни сигнатура кўринишида тавсифлаш ва ушбу сигнатурани назоратланувчи мақонда (тармок трафигида ёки кайдлаш журналида) кидиришдан

иборат. Хужум сигнатураси сифатида аномал фаолиятни характерловчи харакатлар шаблони ёки символлар сатри ишлатилиши мумкин. Бу сигнатуралар вирусга карши тизимларда ишлатилувчи маълумотлар базасига ўхшаш маълумотлар базасида сакланади. Таъкидлаш лозимки, вирусга карши резидент мониторлар хужумларни аниклаш тизимларининг хусусий холи ҳисобланади. Аммо бу йўналишлар бошидан параллел ривожланганлари сабабли, уларни ажратиш кабул килинган. Ушбу хил тизимлар барча маълум хужумларни аникласада, янги, ҳали маълум бўлмаган хужумларни аниклай олмайди.

Бу тизимларни эксплуатациясида ҳам маъмурлар муаммоларга дуч келади. Биринчи муаммо – сигнатураларни тавсифлаш механизmlарини, яъни хужумларни тавсифловчи тилларни яратиш. Иккинчи муаммо, биринчи муаммо билан боғлиқ бўлиб, хужумларни шундай тавсифлаш лозимки, унинг барча модификацияларини қайдлаш имкони туғилсин.

*Хужум хусусидаги ахборотни йигиш усули бўйича туркумлаш энг оммавий ҳисобланади:*

- тармок сатҳида хужумларни аниклаш (network-based);
- хост сатҳида хужумларни аниклаш (host-based);
- илова сатҳида хужумларни аниклаш (application-based).

Тармок сатҳида хужумларни аниклаш тизимида тармоқдаги трафикни эшлиши орқали нияти бузук одамларнинг мумкин бўлган харакатлари аникланади. Хужумни қидириш «хостдан-хостгача» принципи бўйича амалга оширилади. Ушбу хилга тааллукли тизимлар, одатда хужумлар сигнатурасидан ва «бир зумда» тахлиллашдан фойдаланиб, тармок трафигини тахлиллайди. «Бир зумда» тахлиллаш усулига биноан тармок трафиги реал ёки унга якинроқ вактда мониторингланади ва мос аниклаш алгоритмларидан фойдаланилади. Кўпинча рухсатсиз фойдаланиш фаолиятини характерловчи трафикдаги маълум сатрларни қидириш механизmlаридан фойдаланилади.

Хост сатҳида хужумларни аниклаш тизими маълум хостда нияти бузук одамларни мониторинглаш, детектиrlаш ва

харакатларига реакция күрсатишига аталган. Тизим химояланган хостда жойлашиб, унга карши йўналтирилган харакатларни текширади ва ошкор килади. Бу тизимлар операцион тизим ёки иловаларнинг қайдлаш журналларини тахлиллайди. Қайдлаш журналларини тахлиллаш усулини амалга ошириш осон бўлсада, у қуйидаги камчиликларга эга:

- журналда қайд этилувчи маълумотлар ҳажмининг катталиги назоратланувчи тизим ишлаши тезлигига салбий таъсир қўрсатади;
- қайдлаш журналини тахлиллашни мутахассислар ёрдамисиз амалга ошириб бўлмайди;
- хозиргача журналларни саклашнинг унификацияланган формати мавжуд эмас;
- қайдлаш журналларидағи ёзувни тахлиллаш реал вактда амалга оширилмайди.

IDSnинг учинчи хили маълум иловадаги муаммоларни қидиришига асосланган.

*Хужумларни аниклаш тизимининг компонентлари ва архитектураси.* Мавжуд ечимларнинг тахлилии хужумларни аниклашнинг намунавий тизими компонентларининг рўйхатини келтиришига имкон беради.

*Кузатиш модули* назоратланувчи макондан (қайдлаш журнали ёки тармоқ трафиги) маълумотларни йиғишини таъминлайди. Унинг қуйидаги номлари ҳам учрайди: сенсор (sensor), монитор (monitor), зонд(probe) ва х. Хужумларни аниклаш тизими архитектурасининг қурилишига боғлиқ ҳолда кузатиш модули бошқа компонентлардан алоҳида, бошқа компьютерда жойлашиши мумкин.

*Хужумларни аниклаш қисм тизими* асосий модул бўлиб, кузатиш модулидан олинадиган ахборотни тахлиллайди. Ушбу тахлиллаш натижаси бўйича қисм тизим хужумларни идентификациялаш, реакция кўрсатиш варианлари бўйича тўхтамга келиши, маълумотлар омборида хужумлар хусусидаги ахборотни саклаши мумкин ва х.

*Билиллар базасида*, хужумларни аниклаш тизимларида ишлатиладиган усулларга боғлиқ ҳолда, фойдаланувчилар ва хисоблаш

тизим профиллари, рухсатсиз фойдаланишларни характерловчи хужум сигнатуралари ёки шубҳали сатрлар сакланиши мумкин. Билимлар базаси хужумларни аниклаш тизимларини ишлаб чиқарувчилари, тизимдан фойдаланувчилар ёки учинчи томон, ма-салан, бу тизимни мададловчи аутсорсинг компанияси томонидан тўлдирилиши мумкин.

*Маълумотлар омбори хужумларни аниклаш тизими ишлаши жараёнида йифилган маълумотларнинг сакланишини таъминлайди.*

*График интерфейс* тизимнинг нихоятда зарурий компоненти бўлиб, хужумларни аниклаш тизими ишлашини бошқарувчи операцион тизимга боғлик холда де-факто Windows ва Unix стандартларига мос келиши лозим.

*Реакция кўрсатиш қисм тизими* аникланган хужумлар ва бошка назоратланувчи ходисаларга реакция кўрсатишни амалга оширади. Мавжуд тизимларда ишлатиладиган реакция кўрсатиш усууларини кўйидаги учта категорияга ажратиш мумкин:

- билдириш;
- саклаш;
- фаол реакция кўрсатиш.

Билдириш усули бўйича хужум хусусидаги ахборот хавфсизлик маъмурига, тизимнинг консолига ёки электрон почта бўйича, пейджерга факс ёки телефон орқали жўнатилиши мумкин.

Саклаш усулига реакция кўрсатишнинг кўйидаги вариантлари тааллукли:

- ходисаларни маълумотлар базасида қайдлаш;
- хужумларни реал вакт масштабида тиклаш.

Биринчи вариант химоялашнинг бошка тизимларида ҳам кенг кўлланилади. Иккинчи вариантни амалга ошириш учун хужум килувчини компания тармоғига ўтказиб юбориш ва унинг барча харакатларини қайдлаш лозим. Бу хавфсизлик маъмурига кейин вактнинг реал масштабида (ёки берилган тезликда) хужум килувчи томонидан килингандан барча харакатларни тиклашга, муваффақиятли таҳлиллашга ва уларни кейинчалик бартараф этишга ҳамда

мұхокама килиш жараёнида йигилған ахборотдан фойдаланишга имкон беради.

Фаол реакция күрсатиш категориясига қуидаги вариантлар тааллукли:

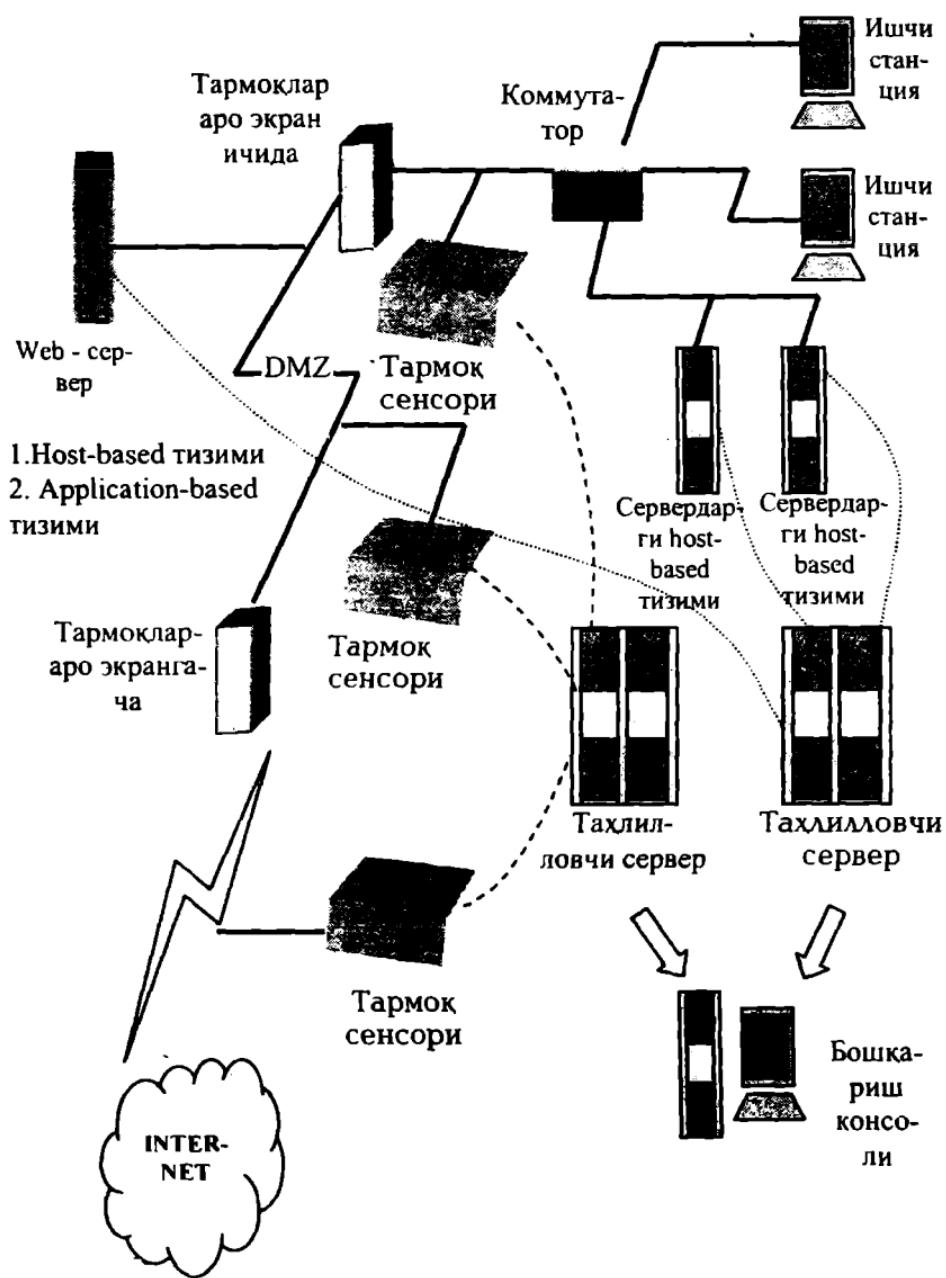
- хужум килувчи ишини блокировка килиш;
- хужум килинувчи узел билан сеансни тугаллаш;
- тармок асбоб-ускуналари ва химоя воситаларини бошкариш.

Реакция күрсатиш механизмларининг ушбу категорияси бир томондан етарлича самарали бўлса, иккинчи томондан улардан жуда эҳтиётлик билан фойдаланиш зарур, чунки уларни нотўғри ишлатиш бутун корпоратив ахборот тизими ишга лаёқатлигининг бузилишига олиб келиши мумкин.

*Компонентларни бошқариш қисм тизими* хужумларни аниклаш тизимининг турли компонентларини бошқаришга аталаған. «Бошқариш» атамаси оркали хужумларни аниклаш тизимининг турли компонентлари (масалан, кузатиш модуллари) учун хавфсизлик сиёсатини ўзгартириш ҳамда ушбу компонентлардан ахборотни (масалан, кайдланган хужум хусусидаги) олиш тушунилади. Бошқариш ички протоколлар ва интсрфейслар ва ишлаб чиқицган стандартлар (масалан, SNMP) ёрдамида амалга оширилиши мумкин.

Хужумларни аниклаш тизимлари иккита архитектура «автоном 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 оркали марказлаштирилган ҳолда бошқариб бўлмайди. «Агент-менеджер» архитектураси бу камчиликлардан холи. Бу ҳолда катта тармокнинг турли кисмларида жойлашган кўпгина IDSдан иборат хужумларни аниклашнинг тақсимланган тизими dIDS (distributed IDS)да маълумотларни йигиш серверлари ва марказий тахлилловчи сервер кайдланувчи маълумотларни марказлаштирилган йигишини ва тахлиллашни амалга оширади. dIDS модулларини бошқариш бошқаришнинг марказий консоли оркали амалга оширилади. Филиаллари турли ҳудудлар, ҳатто, шаҳарлар бўйича тарқалған йирик ташкилотлар учун бундай архитектуранинг ишлатилиши жиддий аҳамиятга эга.

dIDS ишлашининг умумий схемаси 9.4-расмда келтирилган.



9.4-расм. Тақсимланган IDS ишлашининг умумий схемаси.

Бундай тизим турли IDSлардан хужумлар хусусидаги ахбороттарни марказлаштирилиши эвазига корпоратив кисм тармок химояланишини кучайтиришга имкон беради. Хужумларни аникловчи тақсимланган тизим dIDS күйидаги кисм тизимлардан ташкил топған: бошқариш консоли, таҳлилловчи серверлар, тармок агентлари, хужум хусусидаги ахборотни йиғувчи сервер. Марказий таҳлилловчи сервер, одатда, маълумотлар базаси ва Web-сервердан ташкил топған бўлиб, хужумлар хусусидаги ахборотни саклашга ва кулагай Web-интерфейс ёрдамида маълумотларни манипуляциялашга имкон беради. Тармок агенти dIDSнинг энг муҳим компонентларидан бири хисобланиб, 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 гурухлашда фойдаланиладиган параметрларни белгилайди.

Маълумотларни гурухлашни күйидаги параметрлар бўйича амалга ошириш мумкин:

- хужум килувчининг IP-манзили;
- қабул килувчининг порти;
- агент номери;
- сана, вақт;
- протокол;
- хужум хиллари ва х.

IDSдан фойдаланиш самарадорлигига қандайдир щубҳалар бўлишига қарамай, фойдаланувчилар IDSнинг бемалол тарқатилувчи ва тижорат воситаларидан кенг фойдаланадилар.

#### **9.4. Компьютер вируслари ва вирусдан ҳимояланиш муаммолари**

Компьютер вирусининг кўп таърифлари мавжуд. Биринчи таърифни 1984 йили Фред Коэн берган: «Компьютер вируси – бошка дастурларни, уларга ўзини ёки ўзгартирилган нусхасини ки-

ритиш оркали, уларни модификациялаш билан заҳарловчи дастур. Бунда киритилган дастур кейинги кўпайиш кобилиягини сақлайди». Вируснинг ўз-ўзидан кўпайиши ва хисоблаш жараёнини модификациялаш кобилияти бу таърифдаги таянч тушунчалар хисобланади. Компьютер вирусининг ушбу хусусиятлари тирик табиат организмларида биологик вирусларнинг паразитланишига ўхшаш.

Хозирда компьютер вируси деганда куйидаги хусусиятларга эга бўлган дастурий код тушунилади:

- аслига мос келиши шарт бўлмаган, аммо аслининг хусусиятларига (ўз-ўзини тиклаш) эга бўлган нусхаларни яратиш кобилияти;

- хисоблаш тизимининг бажарилувчи объектларига яратилувчи нусхаларнинг киритилишини таъминловчи механизмларнинг мавжудлиги.

Таъкидлаш лозимки, бу хусусиятлар зарурӣ, аммо етарли эмас. Кўрсатилган хусусиятларни хисоблаш мухитидаги заар келтирувчи дастур таъсирининг деструктивлик ва сир бой бермаслик хусусиятлари билан тўлдириш лозим.

Вирусларни куйидаги 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 таркалган туркумлаш хисобланади (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 олувчи дастур коди вазифасини бажаради.

*Макровируслар* ахборотни ишловчи замонавий тизимларнинг макродастурларини ва файлларини, хусусан Microsoft Word, Microsoft Excel ва х. каби оммавий мухаррирларнинг файл-хужжатларини ва электрон жадвалларини заҳарлайди.

*Тармоқ вируслари* ўзини таркатишда компьютер тармоклари 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 хиллари ҳам мавжуд, масалан – тармокли макровирус таҳрирланувчи хужжатларни заҳарлайди ҳамда ўзининг нусхаларини электрон поча оркали тарқатади. Бошқа бир мисол сифатида файл-юклама вирусларини кўрсатиш мумкинки, улар файлларни ҳамда дискларнинг юкландиган секторини заҳарлайди.

*Вирусларнинг ҳаёт даври.* Ҳар кандай дастурдагидек компьютер вируслари ҳаёти даврининг иккита асосий боскичини – сақланиш ва бажарилиш боскичларини ажратиш мумкин.

Сақланиши боскичи вируснинг дискда у киритилган обьект билан биргаликда шундайгина сақланиш даврига тўғри келади. Бу боскичда вирус вирусга қарши дастур таъминотига заиф бўлади, чунки у фаол эмас ва химояланиш учун операцион тизимни назорат қила олмайди.

Компьютер вирусларининг бажарилиши даври, одатда, бешта боскични ўз ичига олади:

1. Вирусни хотирага юклаш.
2. Қурбонни кидириш.
3. Топилган қурбонни заҳарлаш.
4. Деструктив функцияларни бажариш.
5. Бошқаришни вирус дастур-элтувчисига ўtkазиш.

*Вирусни хотирага юклаш.* Вирусни хотирага юклаш операцион тизим ёрдамида вирус киритилган бажарилувчи обьект билан бир вактда амалга оширилади. Масалан, агар фойдаланувчи вирус бўлган дастурий файлни ишга туширса, равшанки, вирус коди ушбу файл кисми сифатида хотирага юкланди. Оддий ҳолда, вирусни юклаш жараёни-дискдан оператив хотирага нусхалаш бўлиб, сўнгра бошқариш вирус бадани кодига узатилади. Бу харакатлар операцион тизим томонидан бажарилади, вируснинг ўзи пассив холатда бўлади. Мураккаброк вазифаларда вирус бошқаришни олганидан сўнг ўзининг ишлаши учун кўшимча харакатлар бажариши мумкин. Бу билан боғлиқ иккита жихат кўрилади.

Биринчиси вирусларни аниқлаш муолажасининг максимал мураккаблашиши билан боғлиқ. Сақланиш боскичидаги баъзи вируслар химояланишни таъминлаш максадидаги етарлича мураккаб алгоритмдан фойдаланади. Бундай мураккаблашишга вирус асосий бадани-

ни шифрлашни киритиш мумкин. Аммо факт шифрлашни ишлатиш чала чора хисобланади, чунки юкланиш боскичида расшифровкани таъминловчи вирус кисми очик кўринишида сакланиши лозим. Бундай ҳолатдан қутилиш учун вирусларни ишлаб чикувчилар расшифровка қилувчи кодини «мутациялаш» механизмидан фойдаланади. Бу усулнинг мохияти шундан иборатки, объектга вирус нусхаси киритилишида унинг расшифровка қилувчига тааллуқли кисми шундай модификацияланадики, оригинал билан матнли фарқланиш пайдо бўлади, аммо иш натижаси ўзгармайди.

Кодни мутациялаш механизмидан фойдаланувчи вируслар *полиморф* вируслар номини олган. Политморф вируслар (polymorphic)-қийин аникланадиган вируслар бўлиб, сигнатураларга эга эмас, яъни таркибида бирорта ҳам кодининг доимий кисми йўқ. Полиморфизм файлли, юкламали ва макровирусларда учрайди.

Стелс-алгоритмлардан фойдаланилганда вируслар ўзларини тизимда тўла ёки кисман беркитишлари мумкин. Стелс-алгоритмларидан фойдаланадиган вируслар – *стелс-вируслар* (Stealth) деб юритилади. Стелс-вируслар операцион тизимнинг шикастланган файлларга мурожаатини ушлаб колиш йўли билан ўзини яшаш маконидалигини яширади ва операцион тизимни ахборотни шикастланмаган кисмiga йўналтиради.

Иккинчи жихат *резидент вируслар* деб аталувчи вируслар билан боғлик. Вирус ва у киритилган объект опération тизим учун бир бутун бўлганлиги сабабли, юкланишдан сўнг улар, табиий, ягона манзил маконида жойлашади. Объект иши тутаганидан сўнг у оператив хотирадан бўшалади. Бунда бир вактнинг ўзида вирус ҳам бўшалиб сакланишнинг пассив боскичига ўтади. Аммо баъзи вируслар хили хотирада сакланиш ва вирус элтувчи иши тугашидан сўнг фаол колиш кобилиятига эга. Бундай вируслар резидент номини олган. Резидент вируслар, одатда, факт операцион тизимга рухсат этилган имтиёзли режимлардан фойдаланиб яшаш маконини захарлайди ва маълум шароитларда зааркунандалик вазифасини бажаради. Резидент вируслар хотирада жойлашади ва компьютер ўчирилишигача ёки операцион тизим кайта юкланишигача фаол холда бўлади.

Резидент бўлмаган вируслар факт фаоллашган вактларида хотирага тушиб захарлаш ва зааркунандалик вазифаларини бажаради. Кейин бу вируслар хотирани бутунлай тарқ этиб яшаш маконида колади.

Таъкидлаш лозимки, вирусларни резидент ва резидент бўлмаганларга ажратиш факат файл вирусларига тааллукли. Юкланивчи ва макровируслар резидент вирусларга тегишли.

**Курбонни қидириши.** Курбонни қидириш усули бўйича вируслар иккита синфга бўлинади. Биринчи синфга операцион тизим функцияларидан фойдаланиб фаол қидиришни амалга оширувчи вируслар киради. Иккинчи синфга қидиришнинг пассив механизmlарини амалга оширувчи, яъни дастурий файлларга тузок қўювчи вируслар тааллукли.

**Топилган қурбонни заҳарлаш.** Оддий холда заҳарлаш деганда курбон сифатида танланган обьектда вирус кодининг ўз-ўзини нусхалashi тушунилади.

Аввал файл вирусларининг заҳарлаш хусусиятларини кўрайлик. Бунда иккита синф вируслари фарқланади. Биринчи синф вируслари ўзининг кодини дастурий файлга бевосита киритмайди, балки файл номини ўзгартириб, вирус бадани бўлган янги файлни яратади. Иккинчи синфга курбон файлларига бевосита кирувчи вируслар тааллукли. Бу вируслар киритилиш жойлари билан характерланади. Куйидаги вариантлар бўлиши мумкин:

1. **Файл бошига киритиши.** Ушбу усул MS-DOSнинг *com*-файллари учун энг қулай хисобланади, чунки ушбу форматда хизматчиян сарлавҳалар кўзда тутилган.

2. **Файл охирига киритиши.** Бу усул энг кўп тарқалган бўлиб, вируслар кодига бошқаришни узатиш дастурнинг биринчи командаси (*com*) ёки файл сарлавҳасини (*exe*) модификациялаш орқали таъминланади.

3. **Файл ўртасига киритиши.** Одатда, бу усулдан вируслар тузилмаси олдиндан маълум файлларга (масалан, *Command.com* файлли) ёки таркибида бир хил кийматли байтлар кетма-кетлиги бўлган, узунилиги вирус жойлашишига етарли файлларга татбиқан фойдаланади.

Юклама вируслар учун заҳарлаш боскичининг хусусиятлари улар киритилувчи обьектлар – кайишкоқ ва каттиқ дискларнинг юкланиш секторларининг сифати ва каттиқ дискнинг бош юклама ёзуви (MBR) оркали аниқланади. Асосий муаммо-ушбу обьект ўлчамларининг чегараланганилиги. Шу сабабли, вируслар ўзларининг курбон жойида сифмаган қисмини дискда саклаши, ҳамда заҳарланган юкловчи оригинал кодини ташиши лозим.

**Макровируслар** учун захарлаш жараёни танланган хужожат-курбонда вирус кодини саклашдан иборат. Баъзи ахборотни ишлаш дастурлари учун буни амалга ошириш осон эмас, чунки хужожат файллари форматининг макропрограммаларни саклаши кўзда тутилмаган бўлиши мумкин.

**Деструктив функцияларни бажариш.** Деструктив имкониятлари бўйича безиён, хавфсиз, хавфли ва жуда хавфли вируслар фарқланади.

**Безиён вируслар** – ўз-ўзидан тарқалиш механизми амалга оширилувчи вируслар. Улар тизимга зарар келтирмайди, факат дискдаги бўш хотирани сарфлайди холос.

**Хавфсиз вируслар** – тизимда мавжудлиги турли таассурот (овоз, видео) билан боғлик вируслар, бўш хотирани камайтиrsада, дастур ва маълумотларга зиён етказмайди.

**Хавфли вируслар** – компьютер ишлашида жиддий нуксонларга сабаб бўлувчи вируслар. Натижада, дастур ва маълумотлар бузилиши мумкин.

**Жуда хавфли вируслар** – дастур ва маълумотларни бузилишига хамда компьютер ишлашига зарур ахборотни ўчирилишига бевосита олиб келувчи, муолажалари олдиндан ишлаш алгоритмларига жойланган вируслар.

**Бошқаришни вирус дастур** – элтувчисига ўтқазиш. Таъкидлани тозимки, вируслар бузувчилар ва бузмайдиганларга бўлинади.

**Бузувчи вируслар** дастурлар заҳарланганида уларнинг ишга лаёкатлигини саклаш хусусида кайғурмайдилар, шу сабабли уларга ушбу боскичнинг маъноси йўк.

**Бузмайдиган вируслар** учун ушбу боскич хотирада дастурни коррект ишланиши шарт бўлган кўринишда тиклаш ва бошқаришни вирус дастур-элтувчисига ўтқазиш билан боғлик.

**Зарар келтирувчи дастурларнинг бошқа хиллари.** Вируслардан ташқари зарар келтирувчи дастурларнинг куйидаги хиллари мавжуд:

- троян дастурлари;
- мантикий бомбалар;
- масофадаги компьютерларни яширинча маъмурловчи хакср утилиталари;
- Internetдан ва бошқа конфиденциал ахборотдан фойдаланиш паролларини ўғирловчи дастурлар.

Улар орасида аник чегара йўқ: троян дастурлари таркибида вируслар бўлиши, вирусларга мантикий бомбалар жойлаштирилиши мумкин ва х.

Троян дастурлар ўзлари кўпаймайди ва тарқатилмайди. Ташқаридан троян дастурлар мутлако беозор кўринади, хатто, фойдали функцияларни тавсия этади. Аммо фойдаланувчи бундай дастурни компьютерига юклаб, ишга туширса, дастур билдиримай зарар келтирувчи функцияларни бажариши мумкин. Кўпинча троян дастурлар вирусларни дастлабки тарқатишда, Internet оркали масофадаги компьютердан фойдаланишда, маълумотларни ўғирлашда ёки уларни йўқ килишда ишлатилади.

*Мантикий бомба* – маълум шароитларда зарар келтирувчи харакатларни бажарувчи дастур ёки унинг алоҳида модуллари. Мантикий бомба, масалан, маълум сана келганда ёки маълумотлар базасида ёзув пайдо бўлганида ёки йўқ бўлганида ва х. ишга тушиб мумкин. Бундай бомба вирусларга, троян дастурларга ва оддий дастурларга жойлаштирилиши мумкин.

*Вируслар ва зарар келтирувчи дастурларни тарқатишни каналлари.* Компьютерлар ва корпоратив тармоқларни химояловчи самарадор тизимни яратиш учун каердан хавф туғилишини аник тасаввур этиш лозим. Вируслар тарқалишнинг жуда хилма-хил каналларини топади. Бунинг устига эски усусларга янгиси қўшилади.

*Тарқатишнинг классик (мумтоз) усуслари.* Файл вируслари дастур файллари билан биргаликда дискетлар ва дастурлар алмасишида, тармоқ катологларидан, Web- ёки FTP – серверлардан дастурлар юкланишида тарқатилади. Юклама вируслар компьютерга фойдаланувчи заҳарланган дискетани дисководда колдириб, сўнгра операцион тизимни қайта юклашида тушиб колади. Юклама вирус компьютерга вирусларнинг бошқа хили оркали киритилиши мумкин. Макрокоманда вируслари MicroSoft Word, Excel, Access файллари каби офис хужжатларининг заҳарланган файллари алманишида тарқалади.

Агар заҳарланган компьютер локал тармоқка уланган бўлса вирус осонгина файл-сервер дискларига тушиб колиши, у ердан каталоглар оркали тармоқнинг барча компьютерларига ўтиши мумкин. Шу тарика вирус эпидемияси бошланади. Вирус тармоқда шу вирус тушиб қолган компьютер фойдаланувчиси ҳукуқлари каби ҳукукка эга эканлигини тизим маъмури унутмаслиги лозим. Шунинг учун у фойдаланувчи фойдаланадиган барча каталогларга ту-

шиб қолиши мүмкін. Агар вирус тармоқ маъмур ишчи станцияси-  
га тушиб колса оқибати жуда оғир бўлиши мүмкін.

### Электрон почта.

Хозирда Internet глобал тармоғи вирусларнинг асосий манбаи хисобланади. Вируслар билан заҳарланишларнинг аксарияти MicroSoft Word форматида хатлар алмашишда содир бўлади. Электрон почта макрокоманда вирусларини тарқатиш канали вазифаси-  
ни ўтайди, чунки ахборотлар билан бир каторда кўпинча офис хуҷоатлари жўнатилади.

Вируслар билан заҳарлаш билмасдан ва ёмон ниятда амалга оширилиши мүмкін. Масалан, макровирус билан заҳарланган мухарирдан фойдаланувчи ўзи шубха килмаган ҳолда, манзилатларга заҳарланган хатларни жўнатиши мүмкін. Иккинчи тарафдан нияти бузук одам атайин электрон почта оркали ҳар қандай хавфли дастурий кодни жўнатиши мүмкін.

Троян Web-сайтлар. Фойдаланувчилар вирусни ёки троян дас-  
турни Internet сайтларининг оддий қузатишида, троян Web-сайтни кўрганида олиши мүмкін. Фойдаланувчи браузерларидаги хато-  
ликлар кўпинча троян Web-сайтлари фаол компонентларининг фойдаланувчи компьютерларига зарар келтирувчи дастурларни киритишига сабаб бўлади. Троян сайтни кўришга таклифни фойда-  
ланувчи оддий электрон хат оркали олиши мүмкін.

### Локал тармоқлар.

Локал тармоқлар ҳам тезликда заҳарланиш воситаси хисобланади. Агар химоянинг зарурий чоралари кўрилмаса, заҳарланган ишчи станция локал тармоқка киришда сервердаги бир ёки бир неча хизматчи файлларни заҳарлайди. Бундай файллар си-  
фатида Login.com хизматчи файлни, фирмада кўлланиувчи Excel-  
жадваллар ва стандарт хужжат-шаблонларни кўрсатиш мүмкін.  
Фойдаланувчилар бу тармоқка киришида сервердан заҳарланган файлларни ишга туширади, натижада, вирус фойдаланувчи компьтеридан фойдалана олади.

Зарар келтирувчи дастурларни тарқатишнинг бошқа канал-  
лари.

Вирусларни тарқатиш каналларидан бири дастурий таъминот-  
нинг карокчи нусхалари хисобланади. Дискетлар ва CD-  
дисклардаги нокунуний нусхаларда кўпинча турли-туман вируслар  
билин заҳарланган файллар бўлади. Вирусларни тарқатиш манба-

ларига электрон анжуманлар ва FTP ва BBS файл-серверлар ҳам тааллукли.

Ўқув юртларида ва Internet-марказларида ўрнатилган ва умум-фойдаланиш режимида ишловчи компьютерлар ҳам осонгина вирусларни таркатиш 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, та-комиллашади. Ҳар кандай 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 таркатиш каналларидан ҳамда компьютер тизимларга татбиқ этишнинг янги технологияларидан фойдаланиши мумкин. Вирусдан заҳарланиш хавфини йўкотиш учун корпоратив тармокнинг тизим маъмури, нафакат вирусга қарши усувлардан фойдаланиши, балки компьютер вируслари дунёсини доимо кузатиб бориши шарт.

## 9.5. Вирусга қарши дастурлар

Компьютер вирусларини аниклаш ва улардан ҳимояланиш учун маҳсус дастурларнинг бир неча хиллари ишлаб чикилган бўлиб, бу дастурлар компьютер вирусларини аниклаш ва йўкотишга 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 аниклашнинг асосий усувлари куйидагилар:

- этalon билан таккослаш усули;
- эвристик тахлил;
- вирусга қарши мониторинг;
- ўзгаришларни аникловчи усул;
- компьютернинг киритиш-чикариш базавий тизимиға (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 муйян вирусга хос коднинг қандайдир ўзгармас кетма-кетлигидир. Вирусга карши дастур маълум вирус никобларини кидиришда текширилувчи файлларни кетма-кет кўриб чиқади (сканерлайди). Вирусга карши сканерлар факат никоб учун белгиланган, олдиндан маълум вирусларни топа олади. Оддий сканерлар компьютерни янги вирусларнинг сукилиб киришидан химояламайди. Янги дастурни ёки юклама секторини заҳарлашда кодини тўла ўзгартира оловчи шифрланувчи ва полиморф вируслар учун никоб ажратиш мумкин эмас. Шу сабабли сканер уларни аникламайди.

*Эвристик таҳлил.* Компьютер вируси кўпайиши учун хотирада нусхаланиш, секторга ёзилиш каби қандайдир муйян харакатларни амалга ошириши лозим. Эвристик таҳлиллагичда бундай харакатларнинг рўйхати мавжуд. Эвристик таҳлиллагич дастурларни, диск ва дискет юклама секторларини, уларда вирусга хос кодларни аниклашга уринган холда, текширади. Таҳлиллагич заҳарланган файлни топиб, монитор экранига ахборот чиқарди ва шахсий ёки тизимли журналга ёзади. Эвристик таҳлил олдин маълум бўлмаган вирусларни аниклайди.

*Вирусга қарши мониторинг.* Ушбу усулнинг моҳияти шундан иборатки, компьютер хотирасида бошқа дастурлар томонидан ба жарилувчи шубҳали харакатларни мониторингловчи вирусга қарши дастур доимо бўлади. Вирусга қарши мониторинг барча ишга туширилувчи дастурларни, яратилувчи, очилувчи ва сақланувчи хужжатларни, Internet оркали олинган ёки дискетдан ёки хар қандай компакт-дискдан нусхалangan дастур ва хужжатларнинг файлларини текширишга имкон беради. Агар қандайдир дастур хавфли харакатни килишга уринмокчи бўлса, вирусга қарши монитор фойдаланувчига хабар беради.

*Ўзгаришларни аниқловчи усул.* Дискни тафтиш килувчи деб аталувчи ушбу усулни амалга оширишда вирусга қарши дастур дискнинг хужумга дучор бўлиши мумкин бўлган барча соҳаларини олдиндан хотирлайди, сўнгра уларни вакти-вакти билан текширади. Вирус компьютерларни заҳарлаганида каттиқ диск гаркибини ўзгартиради: масалан, дастур ёки хужжат файлига ўзининг кодини кўшиб кўяди, Autoexec.bat файлига дастур-вирусни чакиришни кўшади, юклама секторни ўзгартиради, файл-йўлдош яратади. Disk

соҳалари характеристикаларининг кийматлари солиширилганида вирусга карши дастур маълум ва ноъмалум вируслар томонидан килинган ўзгаришларни аниглаши мумкин.

*Компьютерларнинг киритиш-чиқариш базавий тизимиға (BIOSiga) 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 ўзгариришга уринса, химоя ишга тушади ва фойдаланувчи огохлантирилади. Аммо бу химоя жуда ҳам ишончли эмас.

*Вирусга қарши дастурларнинг хиллари.* Вирусга карши дастурларнинг куйидаги хиллари фарқланади:

- дастур-фаглар (вирусга қарши сканерлар);
- дастур-тафтишчилар (CRC-сканерлар);
- дастур-блокировка килувчилар;
- 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 куввати анчагина ошади. Турли хил блокировка килувчилар ва иммунизаторлар ҳам ишлатилади.

*Дастур-фаглар* (сканерлар) вирусларни аниглашда этalon билан таккослаш усулидан, эвристик тахлиллашдан 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 кайтаради. Дастур-фаглар аввал оператив хотирани сканерлайди, вирусларни аниклайди ва уларни йўқотади, сўнгра файлларни даволашга киришади. Файллар ичida вирусларни катта сонини қидиришга ва йўқ килишга аталган дастур-фаглар, яъни полифаглар ҳам мавжуд.

Дастур-фаглар иккита категорияга бўлинади: универсал ва ихтиносослаштирилган сканерлар. Универсал сканерлар сканер ишлаши мўлжалланган операцион тизим хилига боғлик бўлмаган холда,

вирусларнинг барча хилларини кидиришга ва заарсизлантиришга мўлжалланган. Ихтисослаштирилган сканерлар вирусларнинг чегараланган сонини ёки уларнинг бир синфини, масалан макровирусларни заарсизлантиришга аталган. Факат макровирусларга мўлжалланган ихтисослаштирилган сканерлар MS WORD ва Excel мухитларида хужжат алмасиниш тизимини химоялашда энг кулаги ва ишончли ечим ҳисобланади.

Дастур-фаглар сканерлашни «бир зумда» бажарувчи мониторинглашнинг резидент воситаларига ва факат сўров бўйича тизими текширишни тъминловчи резидент бўлмаган сканерларга хам бўлинади. Мониторинглашнинг резидент воситалари тизими ишончлирок химоялашни тъминлайди, чунки улар вируслар пайдо бўлишига дарров реакция кўрсатади, резидент бўлмаган сканер эса вирусни аниклаш кобилиятига факат навбатдаги ишга туширилишида эга бўлади.

Дастур-фагларнинг афзалиги сифатида уларнинг универсаллигини кўрсатиш мумкин. Дастур-фагларнинг камчилиги сифатида вирусларни кидириш тазлигининг нисбатан катта эмаслигини ва вирусга карши базаларнинг нисбатан катта ўлчамларини кўрсатиш мумкин. Ундан ташкари: янги вирусларнинг доим пайдо бўлиши сабабли дастур-фаглар тездан эскиради ва улар версияларининг мунтазам янгиланиши талаб этилади.

*Дастур-тағтишчилар* (CRC-сканерлар) вирусларни кидиришда ўзгаришларни аниқловчи усулдан фойдаланади. CRC-сканерлар дисқдаги файллар-тизимлиқ сектордагилар учун CRC-йигиндини (циклик назорат кодини) ҳисоблашга асосланган. Бу CRC-йигиндилар вирусга карши маълумотлар баъзасида файллар узунлиги, саналар ва охирги модификацияси ва бошка параметрлар хусусидаги кўшимча ахборотлар билан бир каторда сакланади. CRC-сканерлар ишга туширилишида маълумотлар базасидаги маълумот билан реал ҳисобланган кийматларни таккослади. Агар маълумотлар базасидаги ёзилган файл хусусидаги ахборот реал кийматларга мос келмаса, CRC-сканерлар файл ўзгаририлганлиги ёки вирус билан заҳарланганлиги хусусида хабар беради. Одатда, холатларни таккослаш операцион тизим юкланишдан сўнг дарҳол ўтказилади.

CRC-сканерларнинг ҳамчилиги сифатида уларнинг янги файллардаги вирусларни аниклай 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 килувчилар резидент дастурлар бўлиб, вирус хавфи вазиятларини тўхтатиб қолиб, у хусусида фойдаланувчига хабар беради. Вирус хавфи вазиятларига вирусларнинг кўпайиши онларидаги характерли чакириклар киради. Блокировка килувчиларнинг афзаликлари сифатида вируслар кўпайшининг илк боскичидаги уларни тўхтатиб колишини кўрсатиш мумкин. Бу айникса, кўпдан бери маълум вируснинг мунтазам пайдо бўлишида муҳим хисобланади. Аммо, улар файл ва дискларни даволамайди. Блокировка килувчиларнинг камчилиги сифатида улар химоясининг айланиб ўтиш йўлларининг мавжудлигини ва уларнинг «хираликлигини» (масалан, улар бажарилувчи файлларнинг ҳар кандай нусхаланишига уриниш хусусида мунтазам огохлантиради) кўрсатиш мумкин. Таъкидлаш лозимки, компьютер аппарат компоненти сифатида яратилган вирусга қарши блокировка килувчилар мавжуд.

*Дастур-иммунизаторлар* – файллар заҳарланишини олдини оловчи дастурлар икки хилга бўлинади: заҳарланиш хусусида ҳабар берувчи ва вируснинг қандайдир хили бўйича заҳарланишини блокировка килувчи. 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 заҳарланишини аниклай олмайдилар. Шу сабабли бу хил иммунизаторлар ҳозирда ишлатилмайди.

Иккинчи хил иммунизаторлар тизимни вируснинг маълум тури билан заҳарланишдан ҳимоялади. Бу иммунизатор дастур ёки дискни шундай модификациялайдики, бу модификациялаш уларнинг ишига таъсир этмайди, вирус эса уларни заҳарланган деб кабул килади ва сукилиб кирмайди. Иммунизациялашнинг бу хили универсал бўлаолмайди, чунки файлларни барча маълум вируслардан иммунизациялаш мумкин эмас. Аммо бундай иммунизаторлар чала чора сифатида компьютерни янги ноъмалум вирусдан, у вирусга қарши сканерлар томонидан аникланишига кадар, ишончли ҳимоялаши мумкин.

*Вирусга қарши дастурнинг сифат мезонлари.* Вирусга қарши дастурни бир неча мезонлар бўйича баҳолаш мумкин. Кўйида бу мезонлар муҳимлиги даражаси пасайиши тартибда келтирилган:

– ишончлилик ва ишлаш кулайлиги фойдаланувчилардан махсус харакатларни талаб этувчи техник муаммоларнинг йўклиги; вирусга карши дастурнинг ишончлилиги энг мухим мезон хисобланади, чунки энг яхши вирусга қарши дастур сканерлаш жараёни охиригача олиб бора олмаса, у бефойда хисобланади;

– вирусларни барча тарқалган хилларини аниклаш фазилати, ички файл-хужжатлар/жадвалларни (MS Office), жойлаштирилган ва архивланган файлларни сканерлаш, вирусга қарши дастурнинг асосий вазифаси-100 % вирусларни аниклаш ва уларни даволаш;

– барча оммавий платформалар (DOS, Windows 95/NT, Novell NetWare, OS/2, Alpha, Linux ва x.) 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 мухим мезон хисобланади, чунки муайян операцион тизимга мўлжалланган дастургина бу тизим функцияларидан тўла фойдаланиш мумкин. Файлларни «бир зумда» текшириш имконияти ҳам вирусга қарши дастурларнинг етарлича мухим мезони хисобланади. Компьютерга келувчи файлларни ва қўйилувчи дискетларни бир лаҳзада ва мажбурий текшириш вирусдан заҳарланмасликка 100 %ли кафолат беради. Агар вирусга қарши дастурнинг сервер вариантида тармокни маъмурлаш имконияти бўлса, унинг қиймати янада ошади.

**Ишлаш тезлиги.** Вирусга қарши дастурнинг ишлаш тезлиги ҳам унинг мухим мезони хисобланади. Турли вирусга қарши дастурларда вирусни кидиришнинг ҳар хил алгоритмларидан фойдаланилади. Бир алгоритм тезкор ва сифатли бўлса, иккинчиси суст ва сифати паст бўлиши мумкин.

**Ҳимоянинг профилактика чоралари.** Ҳар бир компьютерда вируслар билан заҳарланган файллар ва дискларни ўз вактида аникланган вирусларни тамомила йўқотиш вирус эпидемиясининг бошка компьютерларга тарқалишининг олдини олади. Ҳар қандай вирусни аниклашни ва йўқ килишни кафолатловчи

мутлак ишончли дастурлар мавжуд эмас. Компьютер вируслари билан курашишнинг мухим усули ўз вактидаги профилактика хисобланади.

Вирусдан захарланиш эҳтимоллигини жиддий камайтириш ва дисклардаги ахборотни ишончли сакланишини таъминлаш учун куйидаги профилактика чораларини бажариш лозим:

- факат конуний, расмий йўл билан олинган дастурй таъминотдан фойдаланиш;

- компьютерни замонавий вирусга карши дастурлар билан таъминлаш ва улар версияларини доимо янгилаш;

- бошқа компьютерларда дискетда ёзилган ахборотни ўкишдан один бу дискетда вирус борлигини ўзининг компьютеридаги вирусга карши дастур ёрдамида доимо текшириш;

- ахборотни иккилаш. Аввало дастурий таъминотнинг дистрибутив элгувчиларини саклашга ва ишчи ахборотни сакланишига эътибор бериш;

- компьютер тармоқларидан олинувчи барча бажарилувчи файлларни назоратлашда вирусга карши дастурдан фойдаланиш;

- компьютерни юклама вируслардан заҳарланишига йўл кўймаслик учун, операцион тизим ишга туширилганида ёки қайта юкланишида дисковод чўнтагида дискетани колдирмаслик.

Вирусга карши дастурларнинг ҳар бири ўзининг афзалликларига ва камчиликларига эга. Факат вирусга карши дастурларнинг бир неча хилини комилекс ишлатилиши мақбул натижага олиб келиши мумкин.

Куйида вирусдан заҳарланиш профилактикасига, вирусларни аниклаш ва йўқотишга мўлжалланган баъзи дастурий комплекслар тавсифланган.

AVP (Антивирус Касперского Personal) – Россиянинг вирусга карши пакети. Пакет таркибига куйидагилар киради:

- Office Guard – блокировка килувчи, макровирусдан 100 % химояланишни таъминлади;

- Inspector – тафтишчи, компьютердаги барча ўзгаришларни кузатади, вирус фаоллиги аникланганида дискнинг асл нусхасини

тиклашга ва зарар келтирувчи кодларни чиқариб ташлашга имкон беради;

– Monitor – вирусларни ушлаб колувчи, компьютер хотирасида доимо ҳозир бўлиб, файллар ишга туширилганида, яратилишида ёки нусхаланишида уларни вирусга карши текширади;

– Scanner – вирусга карши модул, локал ва тармок дисклар таркибини кенг кўламли текшириш имконини беради. Сканерни қўл ёрдамида ёки берилган вактда автоматик тарзда ишга тушириш мумкин.

Пакет ёрдамида электрон почтани вирусга карши фильтрлаш ва почта корреспонденциясини комплекс текшириш амалга оширилади. Вирусга карши базани янгилаш Internet орқали бажарилади.

Dr.Web – Россиянинг вирусга карши оммавий дастури, Windows 9x/NT/2000/XP учун мўлжалланган бўлиб, файлли, юклама ва файл-юклама вирусларни кидиради ва зарарсизлантиради. Дастур таркибида резидент қоровул 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 хакида маълум бўлган барча вирус хилларини аниклашга имкон беради. Dr.Web дастурининг мухим хусусияти – оддий сигнатурули кидириш натижа бермайдиган мураккаб шифрланган ва полиморф вирусларни аниклаш имкониятидир.

Symantec Antivirus – Symantec компаниясининг корпоратив фойдаланувчиларга таклиф этган вирусга карши маҳсулоти тўплами.

Symantec маҳсулотидан ишчи жойларининг умумий сони 100 ва ундан ортик бўлганида ва бўлмаганда битта Windows NT/2000/NetWare сервери мавжудлигида фойдаланиш мақсадга мувофик хисобланади. Ушбу пакетнинг башкалардан ажралиб турдиган хусусияти куйидагилар:

– бошқаришнинг иерархик модели;

– янги вирус пайдо бўлишига реакция қилиш механизмининг мавжудлиги.

AntiVir Personal Edition – вирусга қарши дастур AVP, Dr.Web ва х.лар имкониятлариdek имкониятларга эга. Дастур комплектига куйидагилар киради:

- дискларни сканерловчи;
- резидент коровул;
- бошқариш дастури;
- режалаштирувчи.

Дастур Internet дан юкланувчи файлларни сканерлайди. Internet оркали янгиланишларни автоматик тарзда текшириш ва юклаш функцияси ҳам мавжуд. Дастур хотирани, юкланиш секторини текширишда ва унда вируслар бўйича кенг кўламдаги маълумотнома мавжуд.

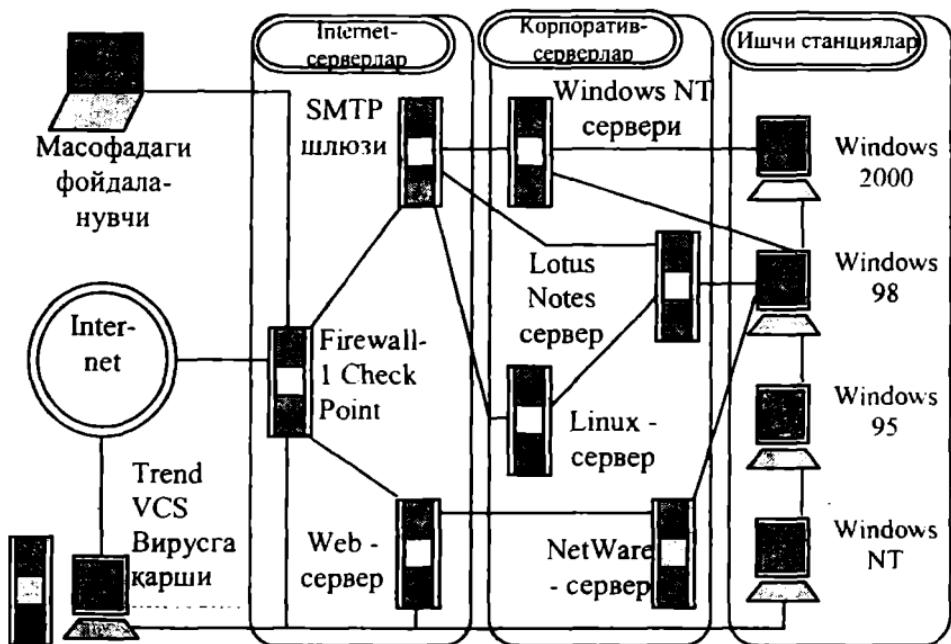
## **9.6. Вирусга қарши ҳимоя тизимини қуриш**

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 тармокка вирусларнинг сукилиб кириш файллари билан доимо тўкнашадилар. Internet/intranet корпоратив тизимларига вирус ҳужумлари мунтазам бўлиб туради, фойдаланувчи ишчи станциясининг захарланган ахборот элтувчиси томонидан захарланиши эса одат тусини олган.

Корпоратив тармок вируслар ва бошка зарар келтирувчи дастурлар ҳужумларига дучор бўлганида тармоқнинг вирусга қарши ҳимояси кўпинча вирусга қарши локал дастурий таъминот ёрдамида, сканерлаш ва катор ишчи станцияларни даволаш билан тугайди ва ҳимоя таъминланади деб хисобланади. Аслида муаммонинг бундай локализациялаш минимал чора хисобланади ва корпоратив тармоқнинг кейинги барқарор ишлашини кафолатламайди. Бошкacha айтганда, вирусга қарши локал ечимларнинг ишлатилиши

корхонани вирусдан самарали химоялаш учун зарурий, аммо етарли восита хисобланмайди.



9.6-расм. Корпоратив тармок намунаий архитектураси.

Вирусга карши химоянинг самарали корпоратив тизими - «мижоз-сервер» технологияси бўйича амалга оширилган, тармоддаги ҳар кандай шубҳали харакатни сезгирилик билан фахмлаб олувчи, тескари боғланишли мосланувчан тизимдир. Бундай тизим корпоратив тармокнинг ички тузилмаси доирасида вирусларнинг ва бошка ганим дастурларнинг тарқалишига йўл қўймайди. Вирусга карши химоянинг самарали корпоратив тизими турли вирус хужумларини-маълумларини, ҳам номаълумларини, улар намоён бўлишининг дастлабки боскичида, аниклади ва бета-рафлаштиради.

Албатта, турли вазиятлар бўлиши мумкин, масалан, масофадан фойдаланувчининг заҳарланган компьютерини корпоратив серверга улаганда ёки макровируслар бўлган WORD ёки Excel файлли дискетлардан иш жойларида фойдаланишда тармок заҳарланиши мумкин. Аммо, сифатли курилган вирусга карши химоянинг кор-

поратив тизими учун бу жиддий эмас, чунки, биринчидан, захарланишнинг кўрсатилган ҳолатлари камдан-кам учрайди, иккинчидан, вируслар вақтида аникланади ва бетарафлаштирилади. Натижада, уларнинг кўпайишига ва корпоратив тармок доирасида таркалишига йўл кўйилмайди.

Уланадиган ишли станциялари сони ошган сари корпоратив тармокнинг хизмат кўрсатиш нархи оша боради. Корпоратив тармокни вируслардан химоялаш харажатлари корхона умумий харажатлари рўйхагида охирги бандни эгалламайди.

Ушбу харажатларни корпоратив тармокни вирусга карши 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 тармоқдаги барча вирусга карши воситаларни самарали бошқаришга имкон беради. Вирусга карши химояни марказлаштирилган бошқариш максади жуда оддий – вирусларнинг барча сукилиб кириш нукталарини блокировка килиш. Куйидаги сукилиб киришларни ва захарланишларни кўрсатиш мумкин:

- ташувчи манбалардан (флоппи-дисклар, компакт-дисклар, Zip, Jazz, Floptical ва х.) охирги захарланган файллардан фойдаланишда ишли станцияларга вирусларнинг сукилиб кириши;

- Web ёки FTP Internetдан орқали олинган локал ишли станциясида сакланган захарланган текин дастурий таъминот ёрдамида захарланиш;

- масофадаги ёки мобил фойдаланувчиларнинг захарланган ишли станциялари корпоратив тармокка уланганида вирусларнинг сукилиб кириши;

- корпоратив тармокка уланган масофадаги сервердаги вируслар билан захарланиш;

- иловаларида макровируслар билан захарланган Excel ва Word файллар бўлган элекtron почтанинг тарқалиши.

Вируслардан ва бошка заарар келтирувчи дастурлардан химояловчи корпоратив тизимни куриш куйидаги босқичларни ўз ичига олади.

*Биринчи босқичда* химояланувчи тармокнинг ўзига хос хусусиятлари аникланади ва бир неча вирусга қарши химоя варианtlари танланади ва асосланади. Бу босқичда куйидагилар бажарилади:

- компьютер тизими ва вирусга қарши ҳимоя воситаларининг аудити;
- ахборот тизимини текшириш ва *картирлаш*;
- вирусларнинг сукилиб кириши билан боғлиқ таҳдидларнинг амалга ошириш сценарийсини таҳлиллаш.

Натижада, вирусга қарши ҳимоянинг умумий холати баҳоланади.

*Иккинчи босқичда* вирусга қарши ҳавфсизлик сиёсати ишлаб чикилади. Бу босқичда қўйидагилар бажарилади:

- ахборот ресурсларини туркумлашнинг тури;
- вирусга қарши ҳавфсизликни таъминловчи кучларни яратиш-ваколатларни тақсимлаш;
- вирусга қарши ҳавфсизликни ташкилий-хукукий мададлаш;
- вирусга қарши ҳавфсизлик инструментларига талабларни аниклаш;
- вирусга қарши ҳавфсизликни таъминлаш харажатларини хисоблаш.

Натижада, корхонанинг вирусга қарши ҳавфсизлик сиёсати ишлаб чикилади.

Учинчи босқичда дастурий воситалари, ахборот ресурсларини инвентаризациялаш ва мониторингини автоматлаштириш воситалари танланади. Вирусга қарши ҳавфсизликни таъминлаш бўйича ташкилий тадбирлар рўйхати ишлаб чикилади.

Натижада корхонанинг вирусга қарши ҳавфсизлигини таъминловчи режа ишлаб чикилади.

*Тўртинчи босқичда* вирусга қарши танланган ва тасдикланган ҳавфсизлик режаси амалга оширилади. Бу босқичда вирусга қарши воситалар етказиб берилади, жорий этилади ва мададланади.

Натижада, корпоратив вирусга қарши ҳимоялашнинг самарали тизими яратилишига имкон туғилади.

# **Хбоб. МАЪЛУМОТЛАРНИ УЗАТИШ ТАРМОГИДА АХБОРОТНИ ҲИМОЯЛАШ**

## **10.1. Маълумотларни узатиш тармокларида ахборот ҳимоясини таъминлаш**

Маълумотларни узатиш тармокларида ахборот ҳимоясини таъминлаш масаласи маълумотлар узатиш тармогининг муайян архитектурасини амалга оширувчи ва унинг барқарор ишлашини таъминловчи аппарат-дастурий воситалари билан боғлиқ холда ечилиши лозим.

Маълумотларни узатиш тармокларида ахборот ҳавфсизлигини таъминлашга куйидаги талаблар қўйилади:

- маълумотларни узатиш тармокларида ахборот ҳавфсизлигига бўладиган маълум таҳдидлардан ҳимоялаш хизмати ва механизmlарини белгиловчи *функционал талаблар*;
- ахборот ҳавфсизлигига бўладиган маълум таҳдидлардан ҳимоялаш механизмини маълумотларни узатиш тармоғи архитектурасига кай тарзда жорий этилиши лозимлигини белгиловчи *архитектуравий талаблар*;

– бошқаришнинг қандай функциялари ишлаб чиқилиши ва улар кай тарзда маълумотларни узатиш тармоғига жорий этилишини белгиловчи *бошқариш (маъмурлаш) талаблари*.

**Функционал талаблар.** Маълумотларни узатиш тармоғи компонентларига ва архитектурасига реал таъсир этувчи умумий функционал галаблар куйидагилар:

– *фойдаланувчини аутентификациятни*. Маълумотларни узатиш тармоғида ахборот ҳавфсизлигини таъминловчи тизим ахборотни (маълумотларни) узатиш жараёнида иштирок этувчи компонентининг (объект, субъект ва фойдаланувчининг) ҳакиқийлигини аниклаш имкониятини таъминлаши лозим;

– *назоратланувчи фойдаланиши*. Маълумотларни узатиш тармоғида ахборот ҳавфсизлигини таъминловчи тизим тармок субъектлари ва фойдаланувчиларининг рухсат 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 химоялаш учун зарур хисобланади;

– *маълумотлар яхлитлигини таъминлаш*. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминловчи тизим таркибидаги фойдаланувчи ва бошқариш ахбороти бўлган маълумотларнинг сакланиш ва узатилиш яхлитлигини кафолатлаши лозим. Маълумотларнинг бузилиши, сохталаштирилиши, кечиктирилиши, рухсатсиз кайталаниши ахборот узатилишининг блокировка килинишига 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 килинган барча ҳаракатлар ва тармоқда содир бўлган барча ҳодисалар хусусидаги ахборотнинг сакланиш имконияти таъминланиши лозим;

– *хавфни билдирувчи сигнални генерациялаш*. Маълумотларни узатиш тармоғи тармоқ ахборот хавфсизлиги обьектлари томонидан хавфсизликнинг бузилиши хусусидаги сигнални генерациялаш имконини таъминлаши лозим;

– *аудит*. Аудит тизимни бошқаришнинг самарадорлигини баҳолаш ҳамда ахборот хавфсизлигининг бузилишини аниқлаш максадида тизимли ёзувларни ва амалларни мустакил таҳлиллаш ва тадқиқлаш сифатида кўрилиши лозим;

– *тиклаш*. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш тизими хавфсизликнинг бузилишини тиклаш кобилиятига эга бўлиши лозим. Ҳар доим, қачон ахборот хавфсизлигини бузишга уриниш содир бўлганида, тизим ушбу уриниш хусусидаги ахборотни шундай ишлаци лозимки, ушбу уриниш маълумотларни узатиш тармоғининг ўтказиш кобилиятини ва фойдаланувчанлигини жиддий пасайишига олиб келмасин;

– *мосланувчанлик*. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш тизимига кўйиладиган мухим концептуал талаб-мосланувчанлик талаби, яъни алоқа тармоғининг тузилмаси, технологияси ва ишлаш шароити ўзгарганида мослашув кобилияти талабидир.

*Архитектуравий талаблар*. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш тизими ахборот хавф-

сизлигининг турли сиёсатини мададлаши, яъни мосланувчан бўлиши лозим. Тизимга қуидаги асосий хизматлар киритилиши мумкин:

- шифрлаш калитларини ва паролларни шакллантириш, саклаш ва тақсимлаш 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 мустакил тарзда у ёки бу ҳимоя механизмларидан фойдаланиб очилиши мумкин. Бунда ҳимоянинг битта механизми ахборот хавфсизлигининг турли хизматларида кўлланилиши мумкин.

**Бошқариш (маъмурлаш) талаблари.** Маълумотларни узатиш тармоғида ахборот хавфсизлигини маъмурлаш хизмати ҳимоянинг техник восигатарини тўлдирувчи ҳимоя чораларининг маълум комплексини ўз ичига олади. Бу ҳимоя чоралари бузғунчининг тармоқ ахборот хавфсизлигига таҳдидни кучайтиришга қаратилган у ёки бу таъсирни ўтказишини кийинлаштириш мақсадида мавжуд ҳимоя тизимиға оператив тарзда ўзгартиришлар киритишга имкон яратади.

Маъмурлаш хизматининг асосий вазифалари қуидагилар:

- ҳимоя хизмати ва механизмига зарур ахборотни таркatiш;
- ҳимоя хизмати ва механизмининг ишлаши хусусидаги ахборотни йиғиши ва таҳлиллаш;
- ҳимояланувчи объектларни аниқлаш;
- хизмат функцияларини самарали амалга ошириш мақсадида ҳимоя механизмларини комбинациялаш;
- маълумотларни узатиш тармоғининг ишончли ва баркарор ишлашини таъминлаш хизматларига жавобгар бошқа маъмурлар билан ўзаро алоқа;

– маълумотларни узатувчи тармоқнинг бузилган ишлаш жарайини тиклаш.

Хавфсизлик маъмури маъмурлаш хизматининг мухим элементи хисобланади. Ахборот хавфсизлигининг хар қандай воситаларидан фойдаланилмасин, маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш сифати маъмурнинг қобилиятига, унинг тиришишига, техник жихозланганлигига боғлиқ.

Таъкидлаш лозимки, бирорта ҳам реал химояланган маълумотларни узатиш тармоғи мутлақ химояланган бўлмайди. Шунга карамасдан химоянинг адекват чоралари бузғунчи таъсири самарасини (зарар келтириш харажатининг кутилаётган зарар ўлчамига нисбатини) анчагина пасайтиради.

## 10.2. Алоқа каналларида маълумотларни химоялаш усуллари

Маълумотларни узатишни химоялаш масаласини ечиш усулларининг учта асосий гурухи мавжуд: каналга мўлжалланган химоялаш усуллари, чеккалараро химоялаш усуллари ва уланишга мўлжалланган химоялаш усуллари. Биринчиси ҳар бир канал учун мустакил равишда маълумотлар оқимини химоялашни таъминласа, иккинчиси ҳар бир хабарни, уни манбадан манзилгача узатишда умумий химоялашни таъминлайди. Учинчи усул иккинчи усулнинг бир тури хисобланади.

*Каналга мўлжалланган усуллар* манба ва манзила боғлиқ бўлмаган ҳолда, алоҳида узеллар орасидаги алоҳида алоқа канали бўйича узатилаётган хабарлар оқимини химоялашни таъминлайди. Бу хил химояни таъминлашда бузғунчининг узелга (пакетни коммутацияловчи марказга) караганда каналга таъсир этиш кулагилиги фараз килинади. Ундан ташқари, маълумотларни узатиш тармоғидаги узелларни фойдаланувчи терминалларини химоялагандек химоялаш мумкин эмас ёки иқтисод нуктаи назаридан фойдасиз. Ушбу гурух усулларининг камчилиги-кисм тармоқ узелларидан бирининг очилиши тармоқ орқали ўтаётган хабарлар оқимининг талайгина кисмини очилишига олиб келиши мумкин.

Терминаллар ва тармоқлар ўртасидаги алоқа каналларини каналга мўлжалланган химоялаш харажатлари бевосита дахлдор тарафлар томонидан қоплансада, маълумотларни узатиш кисм тармоғи ичидаги каналга мўлжалланган химоялаш усулларининг

умумий нархи кисм тармокдан фойдаланувчиларнинг барчаси ўртасида хисоблаб чиқилиши мумкин.

Чеккалараро ҳимоялаш усуллари хабарларни манба узеллари ва кабул килувчи 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, очилиши мумкин.

Уланишга мўлжалланган усуллар. Аксарият кўлланиш соҳаларида маълумотларни узатиш тармоғини манбадан манзилгача уланишни ёки виртуал канални ўрнатиш учун фойдаланувчига тақдим этилувчи мухит сифатида тасаввур этиш мумкин. Бундай тасаввур этишда ҳимоянинг уланишга мўлжалланиши фараз килинади, яъни, ҳар бир уланиш ёки виртуал канал алоҳида ҳимояланади. Шундай килиб, уланишга мўлжалланган усуллар чеккалар аро ҳимоялаш усулларининг бир тури хисобланади. Уланишга мўлжалланган усуллар турли шароитларда умумий ҳимоянинг юкори даражасини таъминлайди ва ҳимояга кўйиладиган талаблар хусусидаги фойдаланувчининг идрокига мос келади. Чунки, уланишга мўлжалланган ахборот конфиденциаллигини ҳимоялаш усуллари асбоб-ускунани ҳимоялашни, масалан, факат хабарлар манбаида ва кабул килувчида ахборотдан руҳсатсиз фойдаланишдан ҳимоялашни кўзда тутади. Айни вактда ҳимоялашнинг каналга мўлжалланган усуллари руҳсатсиз фойдаланишдан ҳимоялашнинг маълумотларни узатиш тармоғидаги ҳар бир узели томонидан таъминланишини талаб этиши мумкин. Аммо, баъзида иккала усулни кўллаганда ҳимоялашнинг тежамли даражасига эришилади.

Маълумотларни узатишни ҳимоялашнинг у ёки бу усулидан фойдаланишдаги асосий вазифалар кўйидагилар:

- хабарлар мазмунининг фош килинишини олдини олиш;
- хабарлар оқимининг таҳлилланишини олдини олиш;
- хабарлар оқими ҳақиқийлигини бузилганлигини аниклаш;
- ёлғон уланишни аниклаш.

Ахборот тизимлари ёки маълумотларни узатиш тармокларида ахборот ҳавфсизлигини таъминлаш мақсадида маълумотларни узатишни ҳимоялаш усулларидан нафакат бузғунчи таъсири оқибатларини аниклашни, балки, агар оқибатлар вактинча харак-

терга эга бўлганида, узилган (бузилган) узатиш жараёнини автоматик тарзда тикилашни талаб этиш керак.

Хозирда юкорида келтирилган вазифаларнинг бажарилишини таъминловчи ҳимоялашнинг стандартлаштирилган механизмлари мавжуд эмас. Ҳар бир муайян ҳолда маълумотларни узатиш хавфсизлиги масалалари ахборотларни криптографик ўзгартириш усуллари, ахборотларни хабарларга бардош кодлаш усуллари, хабарларнинг ҳакикийлигини таъминловчи усуллар, тизимлар ишлашининг ишончлилигини, яшовчанлигини ва баркарорлигини таъминловчи усулларга асосланган ҳимоялашнинг турли механизмларини биргалиқда ишлатиш орқали ҳал этилади.

*Ҳабарлар мазмунининг фош қилинини олдини олишида ҳимоялашнинг каналга мўлжалланган ҳамда уланишга мўлжалланган усулларидан фойдаланиш мумкин.*

Юкорида айтиб ўтилганидек, каналли шифрлаш алоқа тармоғининг ҳар бир каналида мустақил тарзда бажарилиши мумкин. Каналли шифрлашда, одатда, оқимили шифрлаш ишлатилади ва узеллар орасида шифрланган матн битларининг узлуксиз оқими мададланади. Тармоқларда коммутациялаш (маршрутлаш) вазифалари факат узелларда бажарилиши сабабли, алоқа каналида пакстнинг сарлавҳалари билан бирга ахборот кисмини ҳам шифрлаш мумкин.

Аммо маълумотлар факат каналда (каналлар орқали уланган узелларда эмас) шифрланиши сабабли барча оралик узеллар ҳимояланиши лозим. Бунинг устига узелларни нафакат физик ҳимояланиши, балки бу узелларнинг аппарат-дастурий воситалари томонидан узеллар орқали ўтувчи ҳар бир уланишдаги ахборотни яккалаши кафолатланиши зарур.

Чеккалараро шифрлашда маршрутизаторда ишланувчи ҳар бир ҳабар (сарлавҳанинг баъзи маълумотлари бундан истисно) йўл бошида шифрланади ва белгилangan жойга стмагунча расшифровка қилинмайди. Ҳар бир уланиш учун ўзининг калити ишлатилиши мумкин.

*Ҳабарлар оқимини таҳлилланишидан ҳимоялаш, одатда, турли синфларга мансуб ҳабарлар узунлиги ва частотасининг кийматларини, манба манзилларини ва ҳабарлар оқими манзилларини беркитишга йўл ирилган. Агар каналли шифрлаш ишлатилса, узеллар орасида ...аълумотлар узатилганида шифрланган матн битларининг узлуксиз оқими ўрнатилиши мумкин. Бу эса частота*

киматларини ва уланишнинг давомлигини беркитишга имкон беради. Бундай ёндашиша тармокнинг самарали ўтказиши қобилияти пасаймайди, чунки ҳеч қандай қўшимча ахборот талаб этилмайди. Аммо, узел очилса бу узел орқали ўтувчи хабарларнинг бутун оқими таҳлиллаш мавзуига айланади.

Химоялашнинг чеккалараро усулларидан фойдаланилганда узатилувчи хабарларнинг ҳакиқий частотаси ва узунлигини беркитиш учун турли узунликдаги «бўш» хабарлар генерацияланиши, ҳакиқий хабар эса бўш символлар билан тўлдирилиши мумкин. Қабул килувчи бегона кенгайишларни ва «бўш» хабарларни аниклашда хабардаги шифрланган ҳошиядан фойдаланиши мумкин.

Аксарият иловаларда оқимни таҳлиллаш орқали ахборотни чикариб олиш иккинчи даражали хавф сифатида талкин килиниши ва маҳсус карши чоралар кўрилмаслиги мумкин.

*Хабарлар сатҳида ҳақиқийликни тасдиқлаши* хабарларни кечикириш, уларни йўқ килиш, алмаштириб кўйиш ёки кайталаш каби таъсирлардан ҳимоялашни таъминламайди. Шунга карамасдан, бундай таҳдидлардан ҳимоялашнинг турли усуллари мавжуд:

- хабарларни ракамлаш. Ҳар бир хабарни ракамлаб, ракамни хабар таркибиға киритиб, демак, шифрлаб узатиш орқали хабарнинг ҳакиқийлигига ишонч хосил килиш мумкин. Тармокнинг ҳар бир обьекти у билан алоқада бўлувчи обьектларнинг ҳар бири учун алоҳида санагичларга (счётчикларга) эга бўлиши лозимлиги бу муолажанинг камчилиги хисобланади.

- вактни белгилаш. Қабул килувчи ҳар бир узатилган хабарнинг куни ва вактини билган ҳолда унинг адекватлигини текшириши мумкин. Бундай белгилашнинг интервали ва аниклиги ўндаидан танланиши лозимки, бир томондан хатоли хабарлар, иккинчи томондан узатиш каналига хос бўлган табиий кечикиш аникланиши мумкин бўлсин.

- тасодифий сонлардан фойдаланиш. Вактнинг реал масштабида икки томонлама алоқа ишлатилганида қабул килувчи жўнатувчига хабар жўнатилмасдан олдин тасодифий сон юборади. Жўнатувчи бу сонни шифрланган хабарга шундай ўрнатадики, қабул килувчи уни текшириши мумкин бўлсин. Шу тарзда ёлғон хабарлар чикариб ташланиши мумкин.

– хар бир уланиш учун алоҳида калитдан фойдаланиш. Натижада, олингандар хабарда уланишнинг ошкор бўлмаган идентификацияланиши амалга оширилади.

*Хабарлар оқими узилишини аниқлаш* масаласини «сўров-жавоб» протоколидан фойдаланиб ҳал этиш мумкин. Бундай протоколнинг таркибида уланишнинг вактинчалик яхлитлигини ва макомини ўрнатувчи хабарлар жуфтини алмашиб муолажаси бўлади. Уланишнинг хар бир чеккасида «хабар-сўров» узатишни вакти-вакти билан ишга туширувчи таймер ишлатилади ва «хабар-сўров» узатишга уланишнинг бошқа чеккасидан жавоб олинади. Хар бир «хабар-сўров»да передатчик ахбороти мавжуд бўлиб, бу ахборот уланишдаги хабар йўқотилишини аниқлашга имкон беради.

*Ёлғон уланишини аниқлаш* учун хар бир чеккадаги «уланишга жавобгар»нинг ҳақиқийлигини ва уланишнинг вактинчалик яхлитлигини текширишга ишончли асосни таъминловчи карши чоралар ишлаб чиқилган.

Уланиш бошланиши вактида хар бир чеккада уланишга жавобгарнинг ҳақиқийлигини текшириш кейинги хабарлар оқимининг ҳақиқийлиги хусусида карор кабул килишга асос хисобланади.

Уланишнинг вактинчалик яхлитлигини текшириш бузгунчининг олдинги қонуний уланиш ёзувидан фойдаланиб, фойдаланувчини хато фикрга солишидан ёки адаштиришидан, маълумотлар узатиш жараёнини бузишидан химоялайди.

# **ХІ боб. СИМСИЗ АЛОҚА ТИЗИМЛАРИДА АХБОРОТ ХИМОЯСИ**

## **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 кулай ва хохлаган жойларida электрон почтани олишларига ёки Web-саҳифаларни кўздан кеширишларига имкон беради.

Симсиз тармоқларнинг турли хиллари мавжуд, аммо уларнинг энг муҳим хусусияти боғланишнинг компьютер курилмалари орасида амалга оширилишидир. Компьютер курилмаларига шахсий рақамли ёрдамчилар (Personal digital assistance, PDA), ноутбуклар, шахсий компьютерлар, серверлар ва принтерлар таалукли. Одатда, уяли телефонларни компьютер курилмалари каторига киритишмайди, аммо энг янги телефонлар ва ҳатто наушниклар маълум хисоблаш имкониятларига ва тармоқ адаптерларига эга. Якин орада электрон курилмаларнинг аксарияти симсиз тармоқларга уланиш имкониятини таъминлайди.

Боғланиш таъминланадиган физик худуд ўлчамларига боғлиқ холда симсиз тармоқларнинг қуидаги категориялари фарқланади:

- 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 ма софаси билан (17 метргача) ажралиб туради ва катта бўлмаган бинода ишлатилади. Бундай тармоқларнинг характеристикалари ўргача бўлиб, узатиш тезлиги одатда 2Мб/с дан ошмайди.

Бундай тармок, масалан, фойдаланувчи PDA сида ва унинг шахсий компьютерида ёки ноутбукида маълумотларни симсиз синхронлашни таъминлаши мумкин. Худди шу тариқа принтер билан симсиз уланиш таъминланади. Компьютерни ташки қурилмалар билан уловчи симлар чигалликларининг йўқолиши етарлича жиддий афзаллик бўлиб, бунинг эвазига ташки қурилмаларнинг бошлангич ўрнатилиши ва кейинги, зарурият туғилганда, жойининг ўзгартирилиши анчагина осонлашади.

## Жадвал

Тармок хили	Таъсир доираси	Характеристикаси	Стандартлар	Қўлланиш соҳаси
Шахсий симсиз тармоқлар	Фойдаланувчидан бевосита якинликда	ўртacha	Bluetooth, IEEE, 802.15, IRDA	Ташки қурилмалар кабеллари нинг ўрнида
Локал симсиз тармоқлар	Бинолар ва кампуслар доирасида	юқори	IEEE 802.15, Wi-Fi, Hipert-LAN	Симли тармоқларни Мобил кенгайтириш
Регионал симсиз тармоқлар	Шаҳар доирасида	юқори	Патентли, IEEE 802.16, WIMAX	Бинолар 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	Бинодан ташқарида Internetдан мобил фойдаланиш

Симсиз шахсий тармоқларнинг аксарият узатувчи-кабул килувчиларнинг (transceiver) кам кувват исьтемол килиши ва ихчамлиги микропроцессорлар билан таъминланган, катта бўлмаган фойдаланувчи қурилмаларини самарали мададлашга ҳамда ком-

пьютер курилмасини узок вакт мобайнида битта батареяда (ёки аккумуляторда) ишлашига имкон беради. Ундан ташқари, кам кувват истеммол килиниши симсиз шахсий тармоқларни уяли телефонларга, PDA ларга ва наушникларга татбик этишга сабаб бўлди.

Симсиз шахсий тармоқлар Internet га ва иловаларга уланишдан биргаликда фойдаланиш мақсадида ноутбуклар ва шахсий компьютерларнинг ўзаро алокасини таъминлаши мумкин. Бу таъсир доираси битта хона билан чегаралангандар тармоқларга тўғри келади.

**Симсиз локал тармоқлар** офисларнинг ичидаги ташқарисида, ишлаб чиқариш биноларида узатишларнинг юкори 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 бошка хоналарида бўла туриб фойдаланиши мумкин. Бу хизматчига ўз вазифаларини самарали бажаришга имкон беради. Симсиз локал тармоқлар узатишнинг 54Мбит/сгача тезлигига барча офис ёки майший иловалар талабларини кондириш имконига эга. Характеристикалари, компонентлари, нархи ва бажарадиган амаллари бўйича бундай тармоқлар Ethernet хилидаги анъанавий симли локал тармоқларига ўхшаш.

**Симсиз регионал тармоқлар** юзаси бўйича шахарга тенг бўлган худудга хизмат килади. 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 шахар масштабида фойдаланиб, турли туманлардан бериладиган иш нарядларидан фойдаланишини таъминлайди. Натижада, симсиз регионал тармоқлар мавжуд тармоқ инфратузилмаларини бир срга 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 шахарларда ва кишлек жойларда симсиз регионал тармоқларни мижозлар ихтиёрига тақдим этади. Бундай тармоқлар, кўпинча

симли уланишларни ёткизиш билан боғлик чегараланишларга эга бўлган оддий симли уланишларга нисбатан самарали хисобланади.

Симсиз регионал тармоқларнинг характеристикалари турлича. Уланишларда инфракизил 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. Иктисадий мулоҳазаларга таянган ҳолда, телекоммуникация компаниялари кўпгина фойдаланувчилар учун узок масофадан уланишни таъминловчи симсиз глобал тармоқнинг нисбатан киммат инфратузилмасини яратадилар. Бундай ечимнинг харажати барча фойдаланувчилар ўртасида таксимланади, натижада, абонент тўлови унчалик юкори бўлмайди.

Кўпгина телекоммуникация компанияларининг кооперацияси туфайли симсиз глобал тармоқларнинг таъсир доираси чегараланмаган. Телекоммуникация хизматини таъминловчиларнинг бирига тўлаб, симсиз глобал тармоқ орқали дунёнинг хар кандай нуктасидан катор 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 килишни, фойдаланувчи уйдан ёки офисдан ташкарида бўлганида корпоратив иловалардан фойдаланишни таъминловчи иловалардир. Абонентлар, масалан, таксида кетаётгандарида ёки шаҳар бўйича сайр килаётгандарида уланишни ўрнатишлари мумкин. Умуман, симсиз глобал тармоқдан фойдаланувчилар худудий чегараланмаганлар.

Симсиз глобал тармоқлар технологиясини татбик этишдаги муаммолардан бири унинг бино ичидаги фойдаланувчилар учун боғланишни таъминлай олмаслиги. Чунки бундай тармоқ инфратузилмалари бино ташкарисида жойлашган ва радиосигналлар бинода айтирлича сусайди. Симсиз глобал тармоқларни бино ичига ўрнатилиши эса кимматга тушади ва техник нуктаи назаридан асосланмаган.

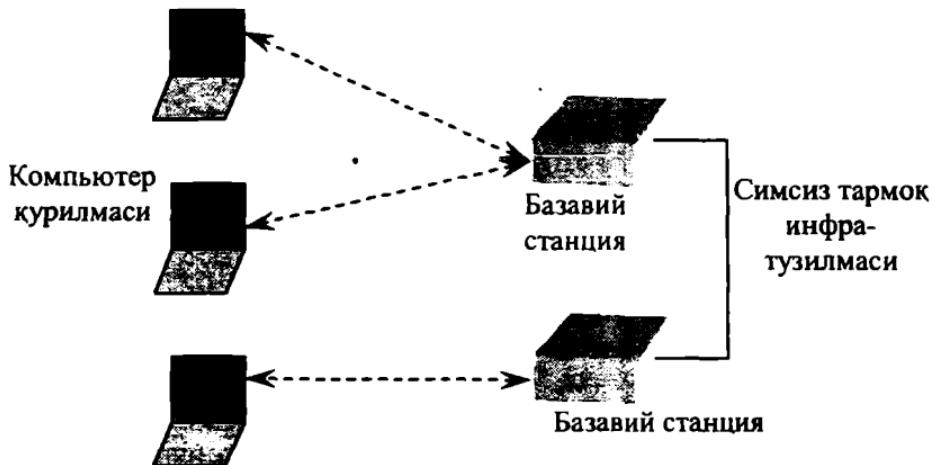
Симсиз шахсий, локал, регионал ва глобал тармоқлар бир-бирини тўлдирувчи бўлиб, турли талабларни қондиради. Аммо, баъзида бир тармоқни иккинчисидан фарқлаб бўлмайди. Масалан,

бино ичидаги симсиз локал тармок фойдаланувчи PDAси билан шахсий компьютерини симсиз шахсий тармок каби улашни таъминлаши мумкин. Турли симсиз тармоклар орасидаги фаркни аниклашда уларда ишлатиладиган технологиялар ва стандартлардан фойдаланишади (жадвалга каралсинг).

Агар фойдаланувчи нуктаи назаридан истикбол хусусида сўз юритилса, симсиз тармоклар орасида чегаранинг йўколиши шарт. Турли хил симсиз тармок ишини мададловчи компьютер курилмалари тармоғи интерфейсининг платалари пайдо бўлмокда. Масалан, сайёхда ёки тижоратчида ҳам симсиз локал ҳам симсиз глобал тармок билан ўзаро алоқа килувчи замонавий уяли телефон бўлиши мумкин.

**Симсиз тармок тузилмаси.** Симсиз тармокларда симли тармоқда ишлатиладиган компонентлар ишлатилади. Аммо, симсиз тармокларда ахборот ҳаво мухити (medium) орқали узатишга яроқли кўринишга ўзгартирилиши лозим.

11.1-расмда симсиз тармокларда ишлатиладиган компонентларнинг асосийлари кўрсатилган. Уларга фойдаланувчилар, компьютер курилмалари, базавий станциялар ва симсиз инфратузилма киради.



11.1-расм. Симсиз тармоқда ишлатиладиган асосий компонентлар.

**Фойдаланувчилар.** Симсиз тармок фойдаланувчига хизмат килишилиги сабабали, фойдаланувчига симсиз тармокнинг мухим кисми сифатида караш мумкин. Фойдаланувчи симсиз тармокдан фойдаланиш жараёнини бошлайди ва унинг ўзи тугаллади. Шу сабабли унга «охирги фойдаланувчи» атамаси жоиз хисобланади. Одатда, фойдаланувчи симсиз тармок билан ўзаро алокани таъминлаш билан бир каторда, муайян иловалар билан боғлик бошқа вазифаларни бажарувчи *компьютер қурилмалари* (*computer device*) билан иш кўради.

Мобиллик – симсиз тармокнинг 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 тармок инфратузилмасига узлуксиз ёки тез-тез тикланувчи ула нишини таъминлаши лозим.

Баъзи фойдаланувчиларга факат компьютер қурилмасининг портативлиги зарур, яъни улар вактнинг маълум оралигига симсиз тармок билан ишлаганида бир жойда бўладилар. Бундай фойдаланишга мисол тарикасида мажлислар залида симсиз тармокка уланган ноутбукда ишловчи ходимни кўрсатиш мумкин.

**Компьютер қурилмалари.** Компьютер қурилмаларининг (баъзида уларни мижозлар деб аташади) кўпгина хиллари симсиз тармок билан ишлайолади. Баъзи компьютер қурилмалари фойдаланувчилар учун атайн қурилган бўлса, бошқалари охирги тизим хисобланади. 11.2-расмда симсиз тармокларнинг компьютер қурилмалари келтирилган.



Принтер



Мобил телефон



Ноутбук



Маълумотларни ийғувчи  
қурилма



Шахсий  
компьютер



PDA



Оддий телефон

11.2-расм. Симсиз тармокларнинг компьютер қурилмалари.

Мобил иловалар ишини таъминлаш ва одамларга ўзлари билан узок вакт мобайнида олиб юришларида куляйлик туғдириш учун компьютер курилмалари ихчам бўлиши лозим. Одатда, улар катта бўлмаган экранга, кам сонли тутгачаларга ва ўлчамлари кичик батареяга эга. Компьютер курилмалари мобилликка эга бўлга холда факат баъзи иловаларни мададлайди. Нисбатан юкори характеристикаларни талаб этувчи иловаларни бажаришда катта экранга ва катта клавиатурага эга бўлган ўлчамлари катта компьютер курилмаларидан фойдаланилади. Аммо улар массасининг катталиги ва бир жойдан иккинчи жойга кўчиришнинг нокулайлиги муаммо хисобланади. Симсиз тармокларнинг компьютер курилмалари серверлар, маълумотлар базаси ва Web-узеллар каби охирги тизимларни ҳам ўз ичига олади.

Фойдаланувчилар мавжуд компьютер курилмаларини симсиз тармокда ишлатиш учун (масалан, симсиз тармоқ интерфейси платасини ноутбукка ўрнатиш орқали) мослаштиришлари мумкин. *Тармоқ интерфейси платаси ёки тармоқ адаптери* (network interface card) компьютер курилмаси ва симсиз тармоқ инфратузилмаси орасида интерфейсни таъминлайди. Бу плата компьютер курилмаси ичига ўрнатилади, баъзида ташки тармоқ адаптери ҳам ишлатилади. Бундай адаптерлар, ишга туширилиши билан компьютер курилмаси ташкарисида колади.

Компьютер курилмалари Windows-XP, Linux ёки MAC OS каби операцион тизимга ҳам эга бўлиб, бу операцион тизим симсиз тармок иловаларини амалга ошириш учун зарур бўлган дастурий таъминотни ишга туширади.

**Ҳаво мұҳити.** Ҳаво компьютер курилмалари ва симсиз инфратузилмага орасида ахборот оқимини узатиш канали хисобланади. Симсиз тармоклар орқали алоқани нутқ орқали мулокотга ўхшатиш мумкин. Агар сұхбатдошлар орасидаги масофа ошаверса, улар бир-бирларини ёмон эшита бошлайдилар.

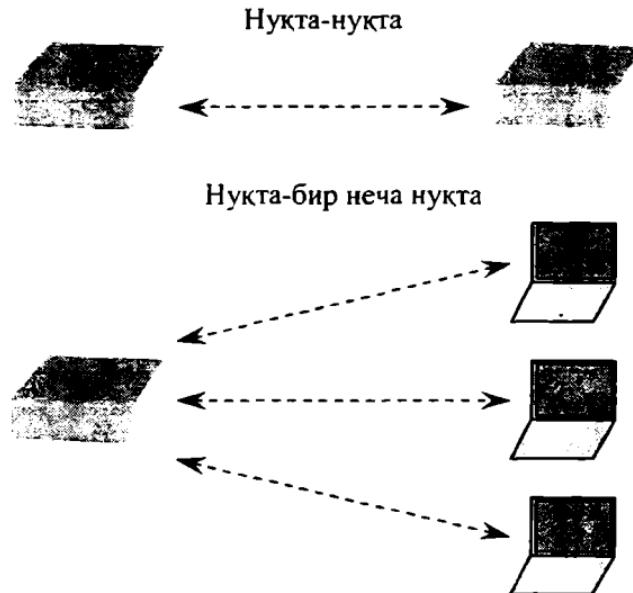
Симсиз тармокларнинг ахборот сигналлари ҳам ҳаво орқали таркалади, аммо ўзининг хусусияти эвазига нутқ сигналарига қараганда анчагина катта масофага тарқалиши мумкин. Бу сигналлар одамга эшитилмайди, шу сабабли уларни, сўзлашга халақит беринидан қўркмай, янада юкори сатхларгача кучайтириш мумкин. Аммо алоқа сифати тўсикларнинг мавжудлигига боғлик. Тўсиклар сигналлар тарқалишига халақит қиласи ёки уларни сусайтиради, натижада сигналлар сатхи пасаяди, уларнинг тарқалиш узоклиги камайади.

Ёмғир, кор, туман, тутун (смог) симсиз тармокларда ахборот сигналларини тарқалишига таъсир этувчи об-ҳаво шароитлари хисобланади. Масалан, кучли жала алоқа узунлигини икки мартага камайтириши мумкин. Бинолар ва дараҳтлар каби бошқа тўсиклар

тарқалиш шароитларига ва симсиз тармок характеристикаларига таъсир этиши мумкин. Симсиз регионал ва глобал тармокларни жойлаштиришни режалаштиришда бу муаммоларнинг мухимлиги ортади.

**Симсиз тармоқ инфратузилмаси.** Симсиз тармоқ инфратузилмаси фойдаланувчилар ва охирги тизимларнинг ўзаро симсиз алокаларини таъминлайди. Уни базавий станциялар, фойдаланиш контроллерлари, уланиш ўрнатилишини таъминловчи иловаларнинг дастурий таъминоти ва тақсимловчи тизим ташкил этиши мумкин.

Базавий станция инфратузилманинг таркалган компоненти хисобланади. У ҳаво мухити оркали таркалувчи симсиз тармоқ ахборот сигналларининг симли тармокка узатилишини таъминлайди. Базавий станцияни баъзида *тақсимловчи тизим* деб ҳам юритиша-ди. 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 компьютеридаги симсиз тармоқ интерфейси платаси-нинг ишлаш принципидан 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 узатиши имкониятига эга. «Нукта-бир неча нукта» конфигурацияси ҳолида базавий станция биттадан ортик компьютер курилмаси ёки бир неча базавий станциялар билан боғланиши мумкин. Бундай хил боғланишни, масалан, симсиз локал тармоқ гаркибидағи фойдаланиш нуктаси таъминлайди. Фойдаланиш нуктаси битта курилма бўлиб, кўпгина компьютер курилмалари бир-бирлари билан ҳамда симсиз тармоқ инфратузилмасидаги тизимлар билан боғланиш мақсадида у билан уланишни ўрнатади.

*Фойдаланиш контроллерлари.* Фойдаланиш контроллерлари, одатда, тармоқнинг ўтказувчи кисмида, фойдаланиш нуктаси ва тармоқнинг химояланиш кисми орасида жойлашган аппарат узели хисобланади. Фойдаланиш контроллерлари очик симсиз тармоқ ва муҳим ресурслар орасида трафикни тартибга солиш мақсадида фойдаланиш нукталарини марказлаштирилган назоратини таъминлайди. Баъзи ҳолларда фойдаланишни бошкариш вазифасини фойдаланиш нуктаси бажаради.

Фойдаланиш контроллерлари кенг кўлланилади. 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 вакти-вакти билан симсиз уланишдан маҳрум бўлишлари мумкин, аммо нисбатан мураккаб бўлмаган иловаларни бажаришда ишлатилувчи протоколлар етарлича баркарор хисобланади.

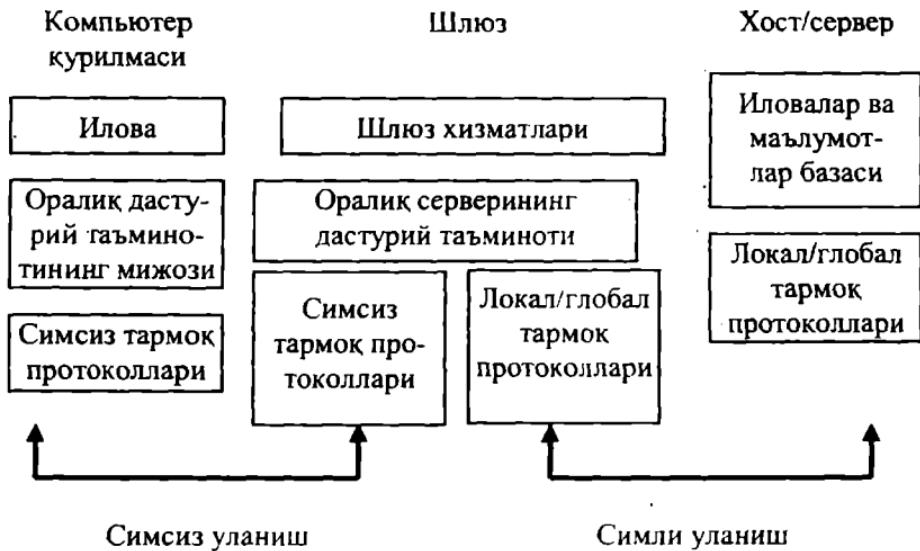
Аммо, бундай оддий иловалар билан бир қаторда маҳсус, янада мураккаб иловалар ишлашини таъминловчи дастурий таъминот зарур. Куйида уланишни таъминловчи иловаларнинг асосийлари келтирилган.

*Терминал эмулятори (terminal emulation).* Терминал эмуляторининг дастурий таъминоти компьютер курилмасида 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 килишга 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 охирги фойдаланувчи қурилмасидаги дастурий таъминот иловага юкланган барча вазифаларни бажаради ва, одатда, марказий серверда жойлашган маълумотлар базаси билан ўзаро алоқада бўлади.

*Оралиқ дастурий таъминот* (*Wireless middleware*). Оралиқ дастурий таъминот фойдаланувчининг компьютер қурилмаси ва илова дастурий таъминоти ёки сервердаги маълумотлар базаси орасида оралиқ уланишни амалга оширади (11.4-расм).



11.4-расм. Оралиқ дастурий таъминоти.

Оралиқ дастур симли тармокка уланган кўшимча компьютерда (оралиқ шлюзида) бажарилади. У фойдаланувчининг компьютер қурилмаси ва серверлар орасида айланувчи пакетларни ишлайди. Бу дастурний таъминот симсиз тармокда самарали ва ишончли боғланишни яратишга имкон беради, чунки маълумотлар базасига уланиш ва иловаларнинг дастурий таъминоти билан ўзаро алоқа

янада ишончли симли тармок орқали амалга оширилади. Баъзида бу технологияни чидамли боғланиш (session persistence) деб атасади.

*Тақсимланган тизим.* Симсиз тармок камдан-кам тўла маънода симсиз ишлатилади. Таркибида кўпинча симли уланишлар бўлган таксимловчи тизим одатда фойдаланиш нукталарини, фойдаланиш контроллерларини ва серверларни бир бутунга бирлаштириш учун зарур бўлади. Аксарият холларда таксимловчи вазифасини оддий Internet тармоғи бажаради.

## 11.2. Симсиз тармоқлар ҳавфсизлигига таҳдидлар

Симсиз технологиядан фойдаланилиб жуда катта афзаликларга эришиш мумкин. Бу технология фойдаланувчиларга алоқани йўқотмасдан бемалол харакатланиш хиссиётини берса, тармок 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. Ҳавфсиз симсиз иловани яратиш учун симсиз «хужумлар» ўтувчи бўлиши мумкин бўлган барча йўналишларни аниклаш лозим. Афуски, иловалар хеч качон бутунлай ҳавфсиз бўлмайди, аммо симсиз технологиялардаги ҳавфхатарни синчилаб ўрганиш ҳар холда химояланиш даражасини ошишига ёрдам беради. Демак, мумкин бўлган таҳдидларни таҳлиллаб, тармокни шундай қуриш лозимки, хужумларга халакит бериш ва ностандарт «хужумлар»дан химояланишга тайёр туриш имкони бўлсин.

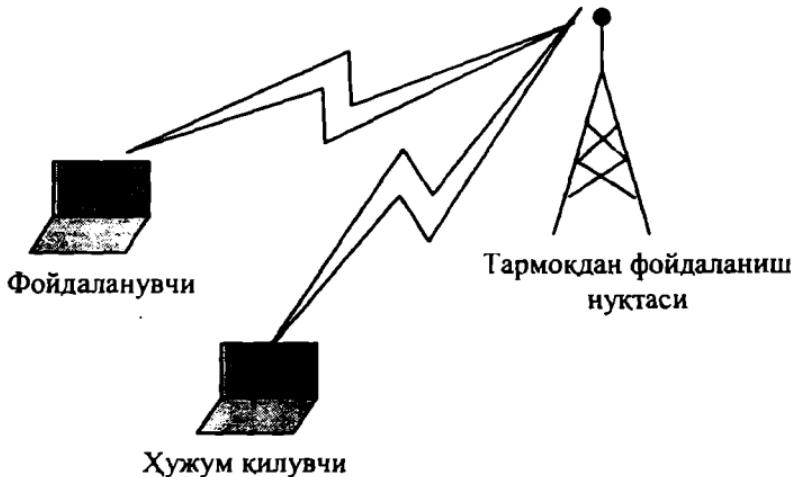
*Назоратланмайдиган ҳудуд.* Симли ва симсиз тармоқлар орасидаги асосий фарқ тармок четки нукталари орасидаги мутлако назоратланмайдиган зона билан боғлик. Уяли тармоқларнинг етарлича кенг маконида симсиз мухит асло назоратланмайди. Замонавий симсиз технологиялар тармок маконини бошқариш воситаларининг чегараланган тўпламини тақдим этади. Бу симсиз тузилмаларнинг якинидаги хужум килувчиларга симли дунёда мумкин бўлмаган хужумларни амалга оширишга имкон беради.

*Яширинчча эшлиши.* Симсиз тармоқлар каби очик ва бошқарилмайдиган мухитда энг тарқалган муаммό – аноним хужумларнинг мумкинлиги. Аноним заараркунандалар 11.5-расмда

күрсатилганидек радиосигналларни ушлаб колиб, узатилувчи маълумотларни расшифровка килиши мумкин.

Узатишни ушлаб колиш учун нияти бузук одам узатгич (передатчик) олдида бўлиши лозим. Ушлаб колишнинг бундай турларини умуман қайдлаш мумкин эмас ва уларга халакит бериш ундан хам кийин. Антенналар ва кучайтиргичлардан фойдаланиш, ушлаб колиш жараёнида нияти бузук одамларга нишондан айтарлича узок массфада бўлишларига имкон беради.

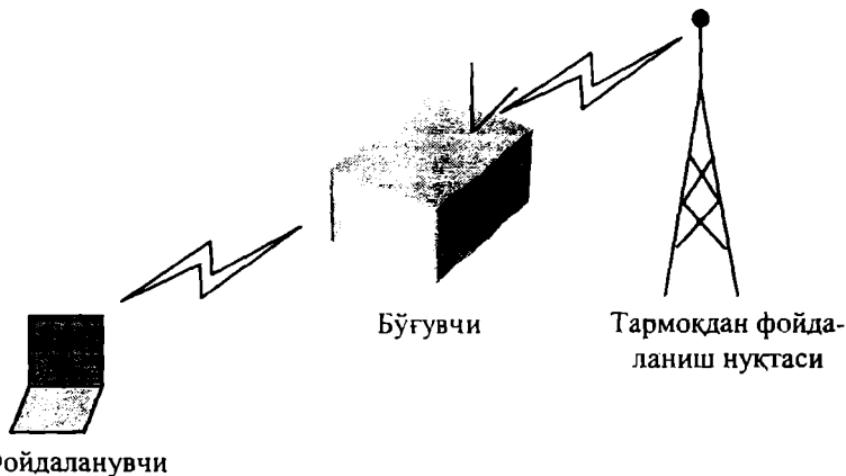
Яширинча эшитишнинг яна бир усули – симсиз тармоққа уланиш. Локал симсиз тармоқда яширинча фаол эшитиш одатда *Address Resolution Protocol* (ARP) протоколидан нотўғри фойдаланишга асосланган. Бошида бу технология тармоқни «эшитиш» мақсадида яратилган эди. Аслида, биз маълумотлар боғланиши сатҳида «*man in the middle*» (MITM – «ўртада одам», пастрокка каралсин) хилидаги хужум билан иш кўрамиз. Хужум килувчи локал симсиз тармоқнинг нишон станциясига сўралмаган ARP-жавобларни юборди, нишон станцияси эса хужум килувчига ўзидан ўтаётган барча трафикни жўнатади. Сўнгра нияти бузук одам пакетларни кўрсатилган манзилларга йўллади. Шундай қилиб, симсиз станция бошқа симсиз мижознинг (ёки локал тармоқдаги симли мижознинг) трафигини ушлаб колиши мумкин.



11.5-расм. Симсиз коммуникацияларда яширинча эшитиш.

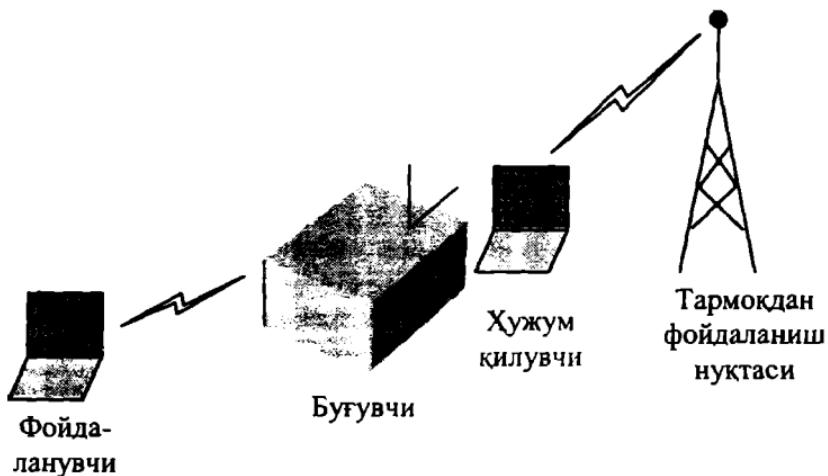
*Бўғиши.* Тармоқларда бўғиши атайин ёки атайин бўлмаган интерференциянинг алока каналидаги жўнатувчи ва қабул қилувчи имкониятидан ошганида содир бўлади. Натижада, бу канал ишдан чиқарилади. Ҳужум қилувчи бўғишининг турли усулларидан фойдаланиши мумкин.

*Хизмат кўрсатишдан воз кечиши.* DoS (Denial of Service – хизмат кўрсатишдан воз кечиши) хилидаги ҳужум тармоқни бутунлай ишдан чиқариши мумкин. Бутун тармоқда, жумладан базавий станцияларда ва мижоз терминалларида, шундай кучли интерференция пайдо бўладики, станциялар бир-бирлари билан боғлана олмайдилар (11.6-расм). Бу ҳужум маълум доирадаги барча коммуникацияни ўчиради. Симсиз тармоқка бўладиган DoS ҳужумни олдини олиш ёки тўхтатиш қийин. Симсиз тармоқ технологияларининг аксарияти лицензияланмаган частоталардан фойдаланади, демак, бир канча электрон қурилмалардан интерференция бўлиши мумкин.



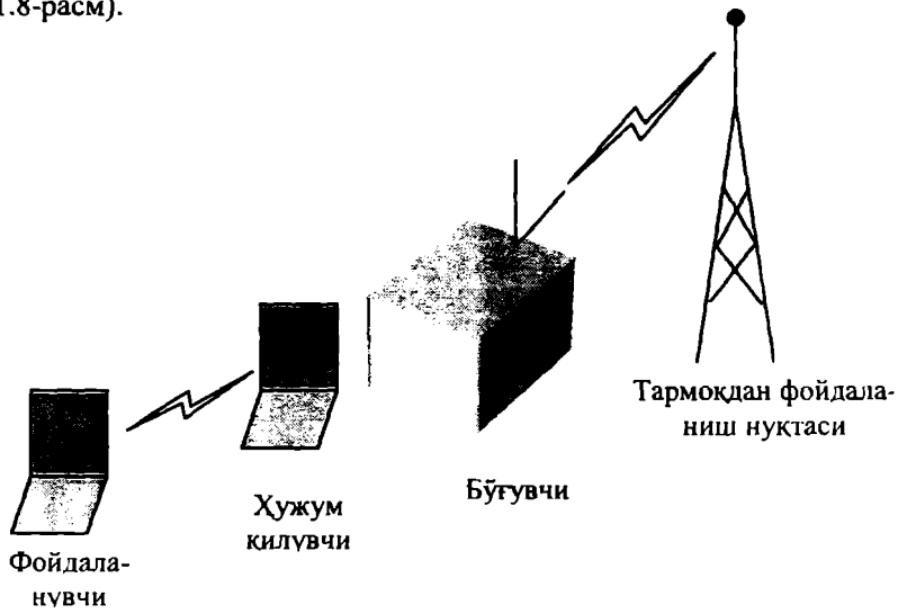
11.6-расм. Симсиз коммуникацияларда бўғиши ҳужумлари.

*Мижозларни бўғиши.* Мижоз станциясини бўғиши фирибгарга ўзини бўғилган мижоз ўрнига қўйишига имкон беради (11.7-расм). Мижоз уланишни амалга ошира олмасин деган максадда унга хизмат кўрсатишдан воз кечиши учун ҳам буғишидан фойдаланилади. Жуда моҳирлик билан қилинган ҳужумлар нияти бузук одам станциясини базавий станцияга улаш максадида мавжуд уланишни узади.



*11.7-расм. Уланишни ушлаб  
колиш мақсадида мижозни бўғиши ҳужуми.*

**Базавий станцияни бўғиши.** Базавий станцияни бўғиши уни ҳужум килувчи станция билан алмаштиришга имкон беради (11.8-расм).



*11.8-расм. Уланишни ушлаб қолиш мақсадида  
базавий станцияни бўғиши ҳужуми.*

Бундай бўғиш фойдаланувчиларни хизматлардан фойдаланишдан, телекоммуникация компанияларини эса фойдадан маҳрум киласди.

Юкорида кайд этилганидек, аксарият симсиз технологиялар лицензияланмаган частоталардан фойдаланади. Шу сабабли кўпгина курилмалар – радиотелефонлар, кузатиш тизимлари ва микротўлқинли ўчоклар – симсиз тармок ишига таъсири этиши ва симсиз уланишни бўғиши мумкин. Бундай атайин бўлмаган бўғиш холларини олдини олиш учун, кимматбаҳо симсиз асбоб-ускунани сотиб олишдан аввал у ўрнатиладиган жойни синчилкаб таҳлиллаш лозим. Бундай таҳлил коммуникацияларга бегона курилмаларнинг таъсири этмаслигига ишонч хосил килишга имкон беради ва маъносиз харажатлардан асрайди.

**Бостириб кириш ва маълумотларни модификациялаш.** Нияти бузук одам уланишни ушлаб колиш, маълумотларни ёки командаларни узатиш максадида маълумотларнинг мавжуд оқимига ахборотни кўшганида бостириб кириш содир бўлади. Хужум килувчи 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 кечиши учун ишлатилиши мумкин. Хужум килувчи тармоқдан фойдаланиш нукталарини уланиш командалари билан тўлиб-тоштиради. Натижада, бошқа фойдаланувчиларга тармоқдан фойдаланишга рұксат берилмайди.

**MITM(*man in the middle*) хужуми.** MITM хужуми юкорида тавсифланган бостириб киришларга ўхшаш. Улар турли шаклларни олишлари мумкин ва алока сеансининг конфиденциаллигини ва яхлитлигини бузиш учун ишлатилади. MITM хужумлар анчагина мураккаб, чунки уларни амалга ошириш учун тармок хусусида ба-тафсил ахборот талаоб этилади. Нияти бузук одам, одатда, тармок ресурсларидан бирининг идентификациясини бажаради. Хужум курбони уланишни бошлаганида, фирибгар уни ушлаб колади ва исталган ресурс билан уланишни тугаллайди, сўнгра ушбу ресурс билан барча уланишларни ўзининг станцияси орқали ўтказади (11.9-расм). Бунда хужум килувчи ахборотни жўнатиши,

жўнатилганини ўзгартириши ёки барча музокараларни яширинча эшлиши ва сўнгра расшифровка қилиши мумкин.



11..9-расм. МИТМ хилидаги ҳужум.

**Абонент-фирибгар.** Тармок абонентининг ишини синчилаб ўрганиб чиккан ҳужум қилувчи ўзини «тармоқ абоненти» қилиб кўрсатиб, тармоқ ва унинг хизматларидан фойдаланишга уринади. Ундан ташкари, фойдаланишда қўлланиладиган курилманинг ўғирланиши тармокка киришга етарли бўлади. Барча симсиз курилмаларнинг хавфсизлигини таъминлаш осон иш эмас, чунки улар фойдаланувчиларнинг харакатланишида кулийлик туғдириш мақсадида атайн 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 мухим реквизитларидан, масалан, аутентификация ахборотидан хабардор қиласидар. Ҳужумнинг бу хили тармоқдан фойдаланишнинг ҳақиқий нуктасини «бўғиш» мақсадида баъзида тўғридан-тўғри бўғиш билан биргаликда амалга оширилади (11.10-расм).



*11.10-расм. Фойдаланишнинг ёлғон нуктаси.*

Симли тармоқдан фойдаланувчилар хам, билмасдан тармоқни хужумга очиб бериб фойдаланишнинг ёлғон нукталарининг ўрнатилишига сабабчи бўлишлари мумкин. Баъзида фойдаланувчи, кулагайликка интилиб, симсиз алока тақдим этувчи фойдаланишнинг симсиз нукталарини ўрнатади, аммо хавфсизлик муаммосини ўйламайди. Бу нукталар 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 кандай жойда беркиниши мумкин. Бундай холда нияти бузук одами тутиш кийин, ишни судга ошириш эса ундан хам кийин.

Таъкидлаш лозимки, аксарият фирибгарлар тармоқни, уларнинг ички ресурсларига хужум килиш учун эмас, балки Internetдан текин аноним фойдаланиш учун ўрганадилар ва Internet химоясида бошка тармокларни хужумлайдилар.

**«Мижоз-мижоз» хилидаги хужумлар.** Тармокнинг барча абонентлари хужумланиши мумкин. Биринчи мувффакиятдан сўнг хужум килувчи корпоратив ёки телекоммуникацион тармокдан фойдаланиш хуқукига эга бўлади. Аксарият тармок маъмурлари хавфсизлик режимига талабни оширишга ёки шахсий тармоклараро экранларни (брандмауэрларни) ўрнатишга ётарлича эътибор бермайдилар. Шу сабабли, симсиз тармок мижозларига мувффакиятли хужумлар нияти бузук одамларга фойдаланувчиларнинг исмини ва паролини очиш, демак, бошка тармок ресурсларидан фойдаланиш имконини бериши мумкин.

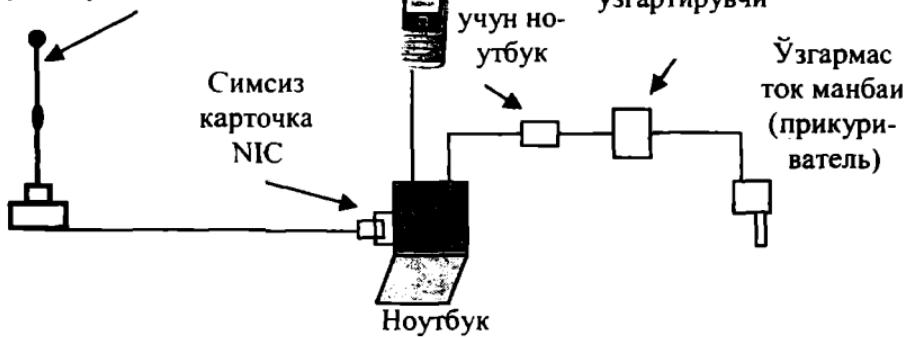
**Тармок асбоб-ускуналарига хужумлар.** Нотўғри конфигурацияланган асбоб-ускуналар хужум килувчилар учун биринчи «хўрак» хисобланади ва тармокка кейинги сукилиб киришга йўл очади. Хужумларнинг асосий обьектлари – маршрутизаторлар, узиб-улагичлар, архивларни сакловчи серверлар ва фойдаланиш серверлари.

**Махфий симсиз каналлар.** Симсиз тармок фойдаланувчилари тармокни яратиш ёки баҳолаш жараёнида яна бир омилни хисобга олишлари зарур. Симсиз фойдаланиш нуктасининг нархи паст хамда дастурий таъминот, стандарт ноутбук ва NIC-карталар асосида фойдаланиш нуктасини яратиш ётарлича осон бўлганлиги сабабли, нокоррект конфигурацияланган ёки симли тармокда ўйламасдан жойлаштирилган симсиз асбоб-ускунани зийраклик билан кузатиш талаб этилади. Бу асбоб-ускуна (11.11-расм) симли инфратузилмада жуда сезиларли «рахналар» хосил килиши мумкинки, улар тармокдан бир неча километр узоқдаги хужум килувчилар диккатини тортиши мумкин.

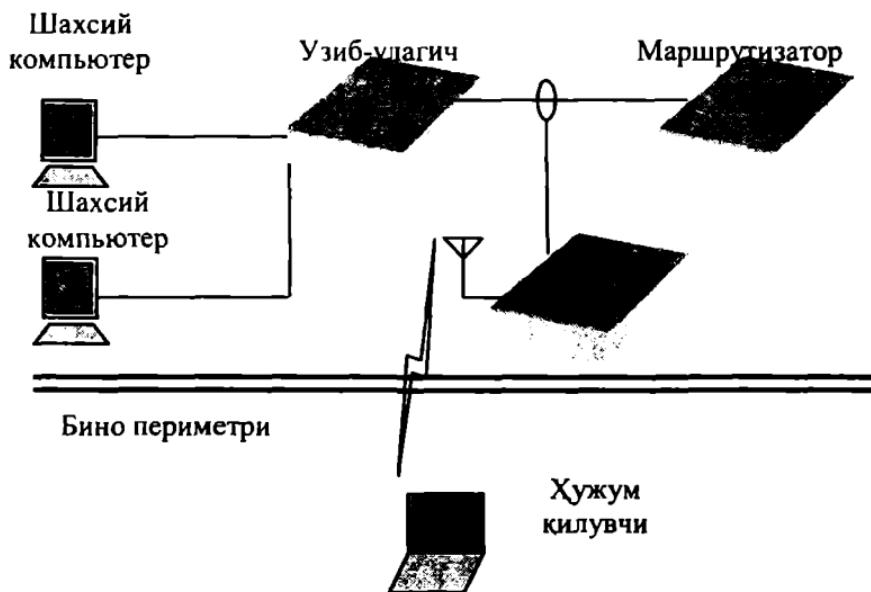
Худди шунга ўхшаш конструкция ёрдамида ўзига хос «симсиз кўприк» ўtkазиш ва фойдаланиш нукталарининг бутун занжирини гашкил килган ҳолда гармоқдан маълумотларни химояланган бино ташкарисида чиқариб олиш мумкин (11.12-расм)

## 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 тармокнинг симли тармоқдан яна бир мухим фарки фойдаланувчининг тармок билан алокани узмасдан жойини ўзгартириш қобилиятидир. Роуминг концепцияси турли симсиз алока стандартлари CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) ва симсиз Ethernet учун бир хил. TCP/IPнинг кўпгина тармок иловалари сервер ва мижоз IP-манзилларининг ўзгармаслигини талаб этади, аммо тармоқдаги роуминг жараёнида абонент албатта унинг бир жойини тарк этиб, бошқа жойига қўшилади. Симсиз тармокларда мобил IP-манзилларнинг ва бошқа роуминг механизмларининг ишлатилиши ушбу талабига асосланган.

Мобил IP-алоқанинг асосий ғояси – фойдаланувчининг турган жойини кайдлаш ва трафикни қайта йўналтириш. Абонент турган жойига боғлик бўлмаган манзил TCP/IP – уланишни мададлайди, фойдаланувчи турган жойига боғлик бўлган вактинча манзил эса локал тармок ресурслари билан уланишни таъминлайди. IP мобил тизими учун учта тартибга солувчи талаблар мавжуд: мобил узели (фойдаланувчининг симсиз курилмаси), уй агенти (уй тармоғида жойлашган сервер) ва ажнабий агент (роуминг узатилувчи тармоқда жойлашган сервер). Мобил узели янги тармокка ўтганида, у турган жойига боғлик бўлган вактинча IP-манзилни олади ва ажнабий агентда кайдланади. Сўнгра ажнабий агент уй агенти билан боғланиб мобил агентнинг ўзига боғланганилигини хабар қилади. Шу ондан бошлаб барча пакетлар ажнабий агент-роуминг оркали уй агентига йўналтирилади.

**Криптоҳимоялаш таҳдидлари.** CDMA, GSM уяли тармокларда ва симсиз Ethernet-тармоқда ахборотнинг конфиденциаллигини ва яхлитлигини таъминлаш мақсадида криптографик воситалар ишлатилади. Аммо хатоликларга йўл кўйиш коммуникациянинг бузилишига ва ахборотнинг ёмон ниятда ишлатилишига олиб келади.

WEP(Wired Equivalent Privacy – симсиз тармок даражасидаги маҳфийлик) – 802.11 хилидаги тармок хавфсизлигини таъминлаш учун яратилган криптографик механизм. WEPни татбиқ этишдаги хатоликлар ва бошқариш муаммолари уни бефойда килиб кўйди. Ушбу механизм барча фойдаланувчилар ишлатадиган ягона статик калитга эга. Internet тармоқда нияти бузук одамга бир неча соат мобайнида калитни тикилашга имкон берувчи воситалар мавжуд. Шу сабабли, WEPга аутентификация ва конфиденциаллик воситаси

сифатида ишониш мумкин эмас. Тавсифланган криптографик усуларни ишлатилгани, умуман ишлатилмаганига қараганда яхширок, аммо юкорида көлтирилгандан хужумлардан химоялашнинг бошқа усуллари зарур.

### 11.3. Симсиз тармоқлар хавфсизлиги протоколлари

**SSL/TLS протоколлари.** Ҳимояланган 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 килиш жараёнида ўзгармасдан келади. Шу сабабли, SSL кўпгина иловалар учун ишлатилиши мумкин.

SSL ўзидан кейинги TLS (Transport Layer Security – транспорт сатҳи химояси протоколи) билан Internet да кенг тарқалган хавфсизлик протоколидир. Netscape компанияси томонидан 1994 йили татбик 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 сатҳнинг транспорт протоколи) ва Wireless Transport Layer Security (WTLS – симсиз мухитда транспорт сатҳини химоялаш протоколи) учун асос вазифасини ўтайди.

SSL/TLSнинг асосий вазифаси тармоқ трафигини ёки гиперматнни узатиш протоколи HTTPни химоялашдир. SSL/TLS алока 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 таркалиши электрон

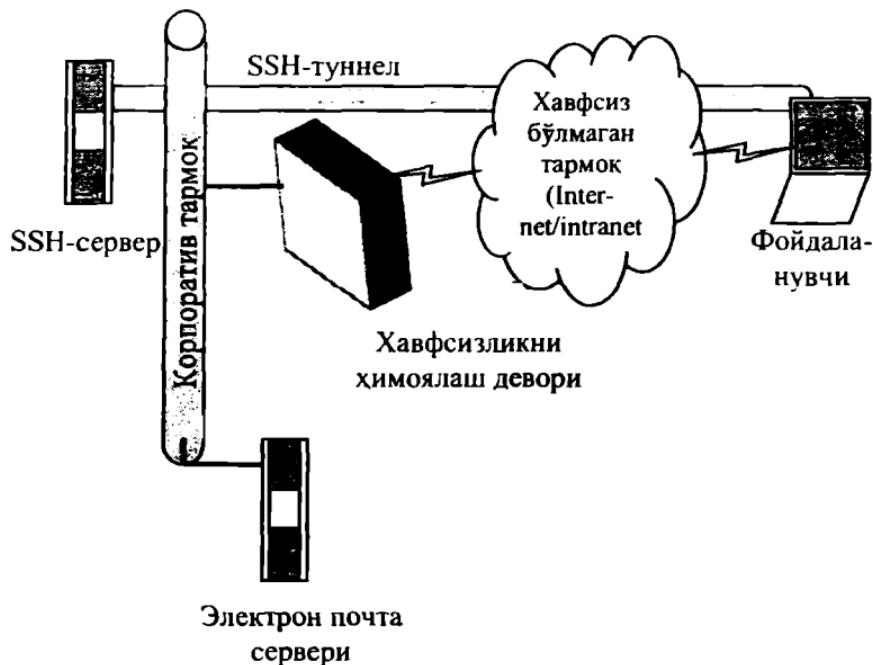
пошта, янгиликлар, Telnet ва FTP (File Transfer Protocol – файлларни узатиш протоколи) каби машхур TCP-коммуникациялар билан боғлиқ. Аксарият холларда SSL/TLS ёрдамида коммуникация учун алоҳида портлар ишлатилади.

**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 хозирда аксарият опрацион тизимларда стандарт илова хисобланади.

SSHда алоқа сеанси жараёнида маълумотларни узатиш учун симметрик калитдан фойдаланилади. Серверни, ҳам мижозни аутентификациялаш учун SSHни осонгина қайта конфигурациялаш мумкин.

Кўпинча SSH тармок хостларини бошкаришда ишлатиладиган, кўп тармкалган илова – telnet ни алмаштириш учун ишлатилади.

Баъзида ишлаб чиқарувчилар SSHни telnet ёки FTPни алмаштирувчи сифатида мададламайдилар. Бундай холларда SSHни telnet, FTP, POP (Post Office Protocol – пошта хабарлари протоколи) ёки хатто 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 хеч кандай трафик ўтказилмайди. SSH-сервернинг SSH дан терминал фойдаланишидан ташкири, портнинг қайта йўналтирилиши электрон почта трафигини SSH-серверга хавфсиз тармок 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) курилмаларида, масалан, уяли телефонларда ва чўнтақ компьютерларида ишлатилади. SSL ва WLTS бир-биридан транспорт сатхи билан фарқланади. SSL йўколган пакетларни қайта узатишда ёки ностандарт пакетларни узатишда TCP ишига ишонади. WLTSдан фойдаланувчи WAP курилмалари ўз функцияларини бажаришида TCPни кўллай олмайдилар, чунки факат UDP (user Datagram Protocol) бўйича ишлайдилар. UDP протоколи эса уланишга мўлжалланмаган, шу сабабли бу функциялар WLTSга киритилиши лозим.

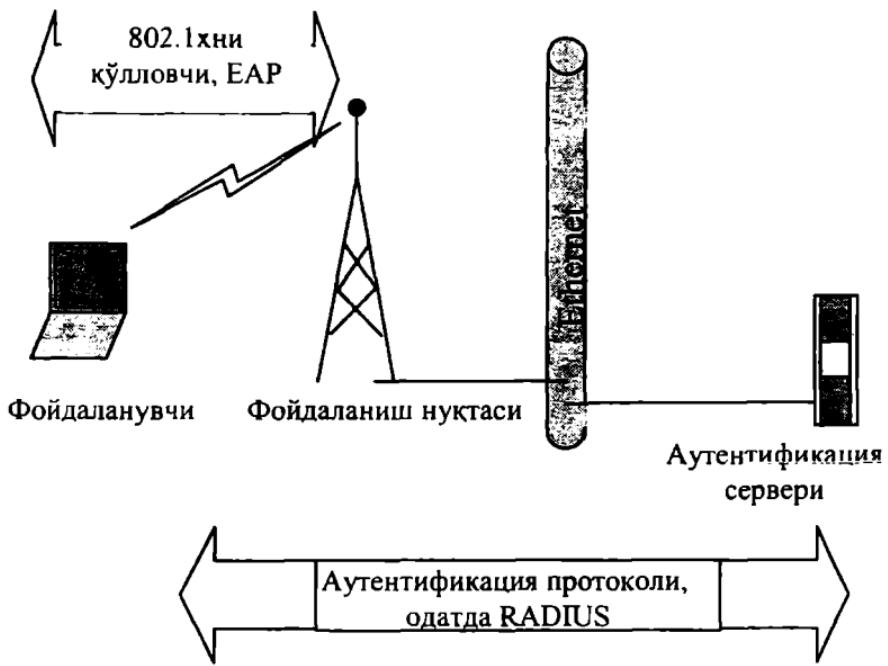
«Кўл бериб кўришиш» жараёнида куйидаги учта синф фаоллашиши мумкин:

- 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 аутентификациялади, аксарият холларда сертификатлар терминалнинг дастурий таъминотига киритилади. 3-синфда мижоз ва сервер аутентификациялади.

**802.1x протоколи.** Бу протоколнинг асосий вазифаси – аутентификациялашdir; баъзи холларда протоколдан шифрловчи калитларни ўрнатишда фойдаланиш мумкин. Уланиш ўрнатилганидан сўнг ундан факат 802.1x. трафиги ўтади, яъни DHCP (Dynamic Host Configuration Protocol – хостларни динамик конфигурациялаш протоколи), IP ва x. каби протоколларга рухсат берилмайди. Extensible Authentication Protocol (EAP) (RFC 2284) фойдаланувчиларни аутентификациялашда ишлатилади. Бошланишида EAP «нуктаникта» (PPP, Point-to-Point Protocol) протоколи ёрдамида аутенти-

фикациялашнинг баъзи муаммоларини ҳал этиш учун ишлаб чиқилған эди, аммо унинг асосий вазифаси симсиз алока муаммоларини ҳал этишга қаратилиши лозим. ЕАРнинг аутентификациялаш пакетлари фойдаланувчи маълумотларини киритган фойдаланиш нуктасига юборилади; аксарият ҳолларда бу маълумотлар фойдаланувчи исми (login) ва паролдан иборат бўлади. Фойдаланиш нуктаси тармок яратувчиси танлаган воситаларнинг бири билан фойдаланувчини идентификациялаши мумкин. Фойдаланувчи идентификацияланганидан ва шифрлаш учун канал ўрнатилганидан сўнг алока мумкин бўлади ва DHCP каби протоколларнинг ўтишига рухсат берилади (11.14-расм).

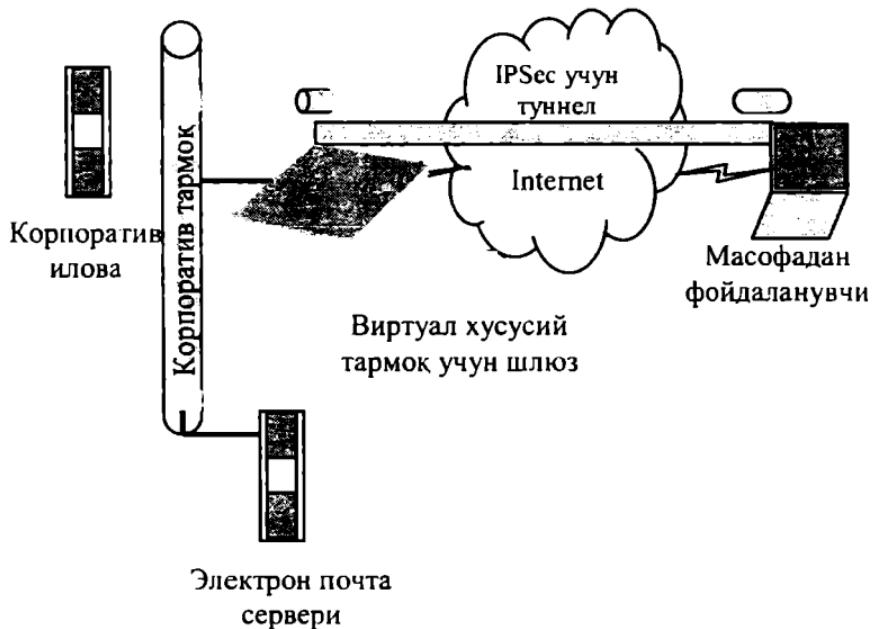


11.14-расм. 802.1x протоколининг кўриниши.

**IPSec протоколи.** Протоколлар стекида IPSec протоколи SSL/TLS, SSH ёки WLTS протоколларидан пастда жойлашган. Хавфсизликни таъминлаш IP-сатҳида ва Internet-моделда амалга оширилади. IPSec ни татбик килиш усулларидан кўп гаркалгани туниеллаш бўлиб, у битта сессияда IP-трафикни шифрлаш ва аутентификациялаш имконини беради. IPSec хозирда Internet да иш-

латилувчи аксарият виртуал хұсусий тармоқлардаги (VPN-Virtual Private Network) асосий технология ҳисобланади. IPSecнинг мослашувчанлиги ва иловалар танланишининг кенглиги сабабли. күпчилик айнан бу схемадан симсиз иловалар хавфсизлигині таъминлашда фойдаланади.

IPSecни иловаларга асосланган құлланишининг жуда күп имкониятлари мавжуд. Хавфсиз коммуникациялар учун IPSecнинг құлланиши күнинча Internet оркали масофадан фойдаланиш виртуал хұсусий тармоғи VPN билан боғылған. Қачонки умумфойдаланувчи тармоқ хұсусий гармоқ функцияларини амалға ошириш учун ишлатылса, уни VPN деб аташ мүмкін. Бундай таърифга ATM (Asynchronous Transfer Mode – узатишининг асинхрон усули), Frame Relay ва X.25 каби тармоқ технологиялари ҳам тушади, аммо аксарият одамлар Internet бүйича шифрланған канални ташкил этиш хұсусида гаі кетганида VPN атамасини ишлатышади. Корпоратив тармоқ периметри бүйича 11.15-расмда құрсатылғаннан деңгээл шлюзлар үрнатылады ва IPSec-туннел оркали шлюздан масофадан фойдаланыш амалға оширилади.



11.15-расм. IPSec VPN-туннел.

## 11.4. Симсиз қурилмалар хавфсизлиги муаммолари

Симсиз қурилмаларни түрттә категорияга ажратиш мүмкін: ноутбуклар, чүнтак компьютерлари (PDA), симсиз инфратузилма (күпприклар, фойдаланиш нұкталари ва х.) ва уяли телефонлар.

*Ноутбуклар* – корпоратив симсиз тармоқларда ва SOHO (Small Office Home Office – кичик ва уй оғислари) тармоқларида кенг гаркалған қурилма.

Физик хавфсизлик ноутбуклар учун жиғддий муаммо хисобланади. Бундай компьютерларни харид килишдаги параметрлардан бири-унинг ўлчами. Ноутбук қанчалик кичкина бўлса, у шунчалик киммат туради. Бошқа тарафдан, ноутбук қанчалик кичкина бўлса, уни ўғирлаш шунчалик осонлашади. Шифрлаш калитларининг масалан, WEP-калитлар (Wired Equivalent Privacy), дастурий калитлар, пароллар ёки шахсий калитларнинг (PGP, Pretty Good Privacy кабиллар) йўкотилиши катта муаммо хисобланади ва уни иловалар яратилиши босқичидаёқ хисобга олиш зарур. Нияти бузук одам ноутбукни ўз ихтиёрига олганидан сўнг аксарият хавфсизлик механизмлари бузилиши мумкин.

Ноутбукларнинг мобиллилиги уларнинг корпоратив тармоқлараро экранлар (брандмауэрлар) билан химояланмаган бошқа тармоқлар билан уланиш эҳтимолларини оширади. Бу Internet-уланишлар, фойдаланувчи тармоқлар, асбоб-ускуна ишлаб чиқарувчиларининг тармоғи ёки ракиблар хам жойланувчи меҳмонхона ёки кўргазмалардаги умумфойдаланувчи тармоқлар бўлиши мумкин. Бундай холларда мобил компьютерларнинг ахборот хавфсизлиги хусусида жиғддий ўйланиш лозим.

Ноутбукларнинг физик сакланишларини таъминлаш усувларидан бири-хавфсизлик кабелидан фойдаланиш. Ушбу кабел ноутбукни столга ёки бошқа йирик предметга «бойлаб» кўйишга мўлжалланган. Албатта, бу юз физиц кафолатни бермайди, аммо ҳар холда ўғрининг анчагина куч сарф килишига тўғри келади.

Ноутбукларнинг тез-тез ўғирланиши сабабли, ахборотни архивлашнинг хавфсизликни таъминлашга нисбатан мухимлиги кам эмас. Шифрлаш дастурлари файллар хавфсизлигини таъминлашда ёки каттиқ дискларда шифрланган маълумотлар ҳажмини яратища ишлатилади. Бу маълумотларни расшифровка килиш учун, одатда, паролни киритиш ёки шахсий калитларни ишлатиш талаб этилади. Барча ахборотларни шифрланган файлларда ски архивларда

сакланиши керакли файллар түпламини архив учун нусхалашни сингиллаштиради, чунки улар энди маълум жойда жойлашган бўлади.

Ўғрилар учун ноутбуклар «биринчи рақамли нишон» эканлигини фойдаланувчилар тушуниб етишлари ва уларни каровсиз колдирмасликлари зарур. Ҳатто оғисларда ноутбукни кечага колдириш мумкин эмас, чунки оғисга кўп кишилар (компания ходимлари, фаррошлар, мижозлар) ташриф буюрадилар.

Ахборотнинг чикиб кетиши ноутбук эгасининг кўп одамлар тўпланган жойларда ҳам содир бўлиши мумкин. Самолет - компания менежерлари фойдаланадиган одатдаги транспорт воситасидир. Самолётда қўшни креслодаги йўловчи ноутбук эгасинини слекаси устидан муҳим ахборотни ўқиб олиши мумкин. Ҳатто «уўй шароитидаги» ноутбуклар ҳам химояланиши зарур. Бу холда компьютернинг химояси сервер химоясидан фарқланмайди. Жуда ҳам зарур бўлмаган сервисларнинг ўчирилиши қурилма ишланини яхшилайди.

Ўзининг дастурий таъминотини ноутбукка ўрнатган нияти бузук одам хавфсизликнинг барча механизmlарини четлаб ўғиш 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 қагтик дискда ўрнатилган пароллар ўғриланган ноутбуқдан фойдаланишга тўскинлик қилиши мумкин.

Ушбу барча воситалар, афсуски, тажрибали хакер учун тўсик бўлаолмайди.

**Чўнтак компьютерлари.** PDA(Personal Digital Assistans «шахсий рақамли ёрдамчилар»)нинг кўпгина хилларидан симсиз иловалар билан ишлашда фойдаланилади. Махсус қурилган PDAларда гиббиёт, саноат ёки авиация иловалари ишга туширилади. Чўнтак компьютерлари ҳам мавжуд бўлиб, уларда симсиз алоқа учун ўрнатилган карточка, штрих кодларнинг сканери, хизмат муддати узок бўлган батарсяялар ёки магнит хошияли карталарни ўқувчи қурилма каби қўшимча қурилмалар билан биргаликда Palm OS ёки Windows SE операцион тизим ўрнатилган. Бундай компьютерлардан фойдаланиш учун махсус техник тайёргарлик талаб этилмайди. Шунга ўхшаш қурилмаларни ёки иловаларни химоялаш айниқса мураккаб масала хисобланади.

PDAдан фойдаланишга хохиш билдирган хужум килувчи учун ундаги ахборот киритиш механизмларининг барчаси нишон хисобланади. Ундан ташкари, аксарият чўнтак компьютерлари шундай ишлаб чикилганки, уларни ишлаб чикувчилари учун иловалардаги хатоликларни осонгина аниклаш йўллари таъминланган. Хатоликларни аниклашда ишлатилувчи интерфейслар нияти бузук одамлар учун ҳакикий «тешик» хизматини ўташи мумкин.

Чўнтак компьютери ишлайдиган ахборотни химоялаш учун ахборотни чўнтак компьютерида эмас, балки маълумотларнинг хавфсиз резерв базасида саклаш лозим. Яна бир вариант – JAVA тили иловасидан ёки фойдаланувчи учун маҳсус яратилган иловалардан фойдаланиш. Бу ҳолда ахборот курилмада сакланмайди, аммо, PDAнинг дисплейида акслантирилади. Бошкacha айтганда, симсиз иловалардан факат симсиз тармоқдан фойдаланиш мавжуд бўлган жойларда фойдаланиш мумкин.

Аксарият PDAларда парол ёрдамида блокировка ва разблокировка килиш имконияти мавжуд. Бу усувларга бутунлай ишонмаслик лозим, аммо улар нияти бузук одамларни вактинча тўхтатиб туриши мумкин. Ундан ташкари, PDAни блокировка килиш гизими курилмадаги иловалардан ёки ахборотдан нияти бузук одамларнинг фойдаланишни қийинлаштиради. PDAнинг зарур бўлмаган барча функцияларини ўчириб куйиш лозим, чунки ҳар бир ўчирилган киритиш механизми бўлиши мумкин бўлган хужумлар сонини камайтиради.

Чўнтак компьютерида мухим ахборотни саклаш учун шифрлашни кўллаш ва унга кўшимча сифатида манбани улаш ва экранни блокировка килиш учун пароллар ўрнатиш тавсия этилади.

**Симсиз инфратузилма.** Симсиз инфратузилма курилмалари одатда одамлар йигилган с尔да жойлаштирилади. Уларга кафелар, аэропортлар, корпоратив тадбирларни ўтказиш жойлари ва х. киради. Турли хил одамлар EAP(Extensible Authentication Protocol – аутентификациялашнинг кенгайтирулувчи протоколи) ёки WEP каби хавфсизлик воситаларини ишдан чиқариш ёки тармоқка сукилиб кириш учун тармоқ конфигурацияси хусусидаги ахборотни кўлга киритиш масадида ушбу компонентлардан фойдаланишни хоҳ-лашлари мумкин.

Симсиз инфратузилма курилмаларида тармоқни бошқариш функцияларининг хавфсизлигини таъминлаш учун улардан фойдаланишда SSH, SSL (Secure Sockets Layer) ёки SNMP3 (Simple Net-

ork Management Protocol 3 – тармокни оддий бошқариш протоколи, 3-версия) каби хавфсиз протоколлардан фойдаланиш лозим. Үндан ташкари telnet, HTTP даги түғри матн, ва SNMP (биринчи версия) каби хавфсизлик етарли даражасини мададламайдыган протоколлар ўчирилиши лозим. Хавфсиз бошқаришни таъминлаш иложи бўлмаса, фойдаланишнинг баъзи бир нукталарини кетма-кет портлар оркали бошқариш мантиқан түғри хисобланади. Фойдаланиш нукталарини юкорига кўл етмайдиган жойга маҳкамалаб кўйиш хам уларни ўғирланишдан саклади.

**Уяли телефонлар.** Уяли телефонлар учун хавфсизлик мулохазалари ноутбук ва PDAларга нисбатан келтирилган мулохазаларга ўхшаш. Курилмаларнинг ўзи ва мос дастурий таъминот учун хавфсизлик муаммоси хам ҳеч нимаси билан фарқ килмайди.

Уяли телефонлар хам бошқа симсиз курилмаларга бўладиган хужумларга дучор бўладилар. Одатда, буфернинг тўлиб-тошиши, катор форматига хужумлаш, грамматик хатоликлар ишлатилади, натижада хужум килувчи ўғирланган курилмада ўзининг дастурини ишга туширишга эришади. Мисол сифатида SMSнинг киска хабарларини кўрсатиш мумкин. Ўзининг телефони оркали SMS жўнатган фойдаланувчига хужумга дучор бўлиши ҳавфи туғилади. Бу хужум натижасида хизмат килиш тўхтатилади ёки фойдаланувчи терминалида бегонанинг командалари бажарилади.

Үндан ташкари, SIM-карталарни (Subscriber Identity Module – абонент идентификацияси модули) ишлаб чиқарувчилари курилмаларига уяли телефонга симсиз интерфейс оркали юкланилиши рухсат этиладиган кўшимча функцияларни кирига бошладилар. Мисол тарикасида Sim Toolkit ва МЕХЕни кўрсатиш мумкин. Заарли иловаларни бошқа фойдаланувчига узатишни олдини олувчи усууллар ташки хужумларга дучор бўлади. Бундай иловаларнинг можияти шундаки у нияти бузук одамга фойданувчининг манзил китобини ёки телефондаги бутун SMS рўйхатини узатиши мумкин. Баъзи ечимлар DES стандартти асосида ишлайди, аммо худди шундай DES-калитлар хар бир SIM-карталар учун ишлатилади.

Терминаллар учун парол ёки PIN-кодларни ишлатиш тавсия этилади. GSM(Global System for Mobile Communications – мобил коммуникацияларнинг глобал тизими) тармокларида 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 ракам)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 ташкари, GSM ичидаги алгоритмларга бўладиган аксарият хужумлар нияти бузук одамга фойдаланувчининг телефон ракамини ўйлаб чиқаришига (клонировка) имкон беради. Бу хужумлар одатда телефон мавжудлигини талаб килади, шу сабабли телефонни хавфсиз жойда саклаш, йўқотилган ёки ўғирланган холда тезлик билан операторга хабар бериш лозим.

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

### **12.1. Бошқаришнинг функционал масалалари**

Замонавий ахборот технологияларидан муваффакиятли фойдаланиш учун нафакат тармокларнинг ўзини, балки тармок хавфсизлиги воситаларини ҳам ишончли ва самарали бошқариш зарур. Ҳозирги вактда компаниянинг бутун инфратузилмасини камраб олувчи бошқаришнинг комплекс тизимини яратиш биринчи галдаги вазифа хисобланади. Бундай бошқариш тизими ахборот тизимининг мураккаблиги ва масштабидан қатъий назар, куйидагиларга имкон яратади:

- бутун ахборот инфратузилмасига марказлаштирилган ва оператив бошқариш таъсирни кўрсатиш;
- оператив ечимларни қабул килиш учун ахборот хавфсизлиги ҳолати хусусидаги объектив ахборотни берувчи мунтазам аудит ва кенг кўламдаги мониторинг ўтказиш;
- ахборот инфратузилмаси ривожини башоратлаш учун унинг ишлаши хусусидаги статистик маълумотларни тўйланиш.

#### **Ахборот тизимларини бошқаришнинг ITIL методологияси.**

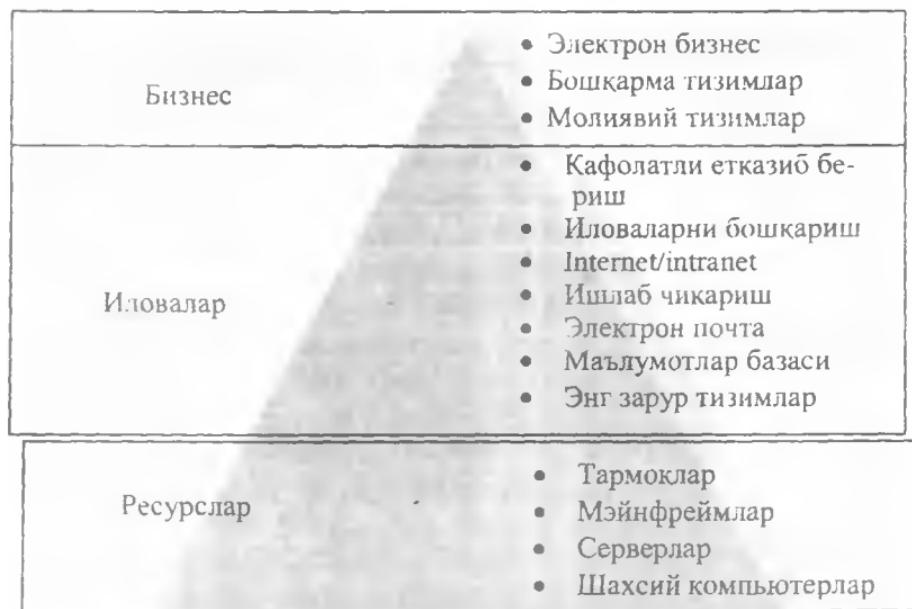
ITIL (IT Infrastructure Library) методологиясига мувофиқ ахборот тизими иккита йирик блокдан – ахборот инфрагузилмаси ва ахборот сервисларидан иборат (12.1-расм).



*12.1-расм. ITIL методологияси нуктаи назаридан ахборот тизимининг кўриниши.*

Ахборот инфратузилмаси ахборот сервислари ишловчи моддий асос, мухит хисобланади. Ахборот сервисларига Internet-сервислар, иловалар сервиси, бошқариш, ечим кабул килиш сервислари ва х. киради. Ахборот инфратузилмаси сервислар ишлашини таъминловчи техник воситалар, алоқа линиялари, муолажалар, меъёрий хужжатлар ва х. мажмуудир. Ахборот сервисларининг сифати бевосита ахборот инфратузилмаси ва уни бошқариш сифатига боғлик.

Ахборот инфратузилмасини асосида ахборот ресурслари (хисоблаш платформалари, серверлар, шахсий компьютерлар, маълумотларни узатиш тармоқлари, алоқа линиялари) ётувчи пирамида сифатига тасаввур этиш мумкин (12.2-расм).

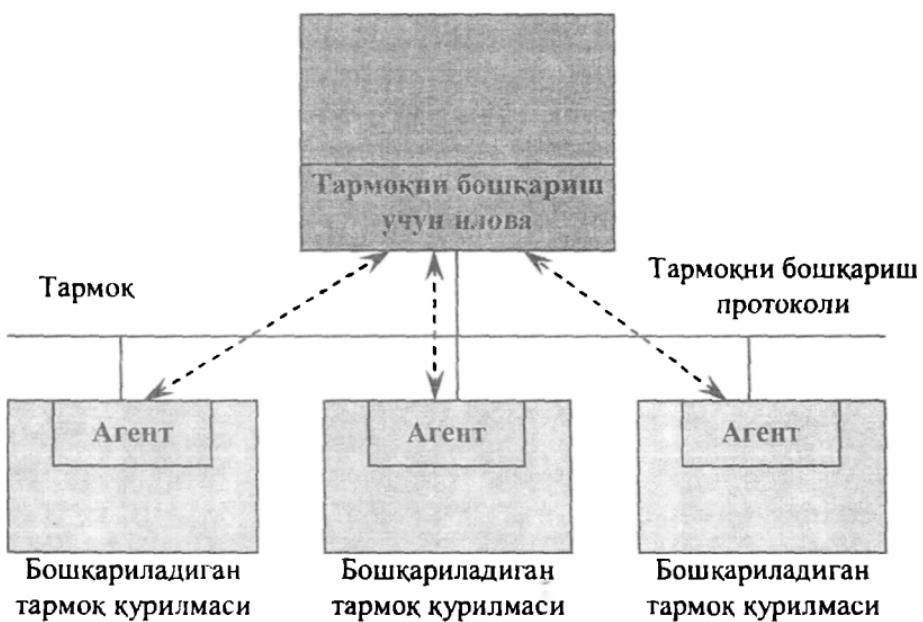


12.2-расм. Ахборот инфратузилмасини ташкил ётувчилари.

Пирамиданинг иккинчи сатхини гурли иловалар ташкил этади. Бу иловалар биринчи сатҳ ресурсларидан фойдаланиб татбикий дастур гаъмиюти, электрон почта, кафолатланган етказиш тизими, маълумотлар базаси, Web-серверлар ва х. каби муайян иловалар

ишилашини таъминлайди. Ва ниҳоят, энг юкори сатҳда бизнес ва ишлаб чикариш жараёнларининг ўтишини таъминловчи иловалар ишлайди. Иккала пастки сатҳдан фойдаланувчи бу иловалар ишлаб чикаришни бошқариш, буюртмачилар ва таъминловчи билан ўзаро алоқа, молиявий хисоб ва ечимни кабул килишни мададлаш каби бизнес – масалаларни ечишга йўналтирилган.

Умумий холда, тармоқни бошқариш тизимининг архитектураси 12.3-расмда келтирилган кўринишга эга. Тармоқни бошқариш иловаси тармоқ маъмурининг иш жойида ёки бошка компьютерда бажарилиши мумкин. Унинг вазифаси бошқарилувчи курилмаларда бажариладиган *агент* – иловалардан ёки операцион тизим сервисларидан келувчи бошқарилувчи объект хусусидаги ахборотни йиғиш.



12.3-расм. Тармоқни бошқариш тизимининг умумлаشتirilgan архитектураси.

Бундай иловаларни агентлар билан ўзаро алокаси учун одатда, SNMP (Simple Network Management Protocol) ёки CMIP (Common Management Information Protocol) протоколларидан фойдаланилди. Биринчиси, одатда, локал тармоқда ишлатилиса, иккинчиси тел-

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 курилмалардаги бузилишларни кузатиш, сабабларни аниглаш ва бартараф этиш (кўпинча автоматик тарзда), окибатларини тузатиш ва бузилишларни олдини олиш (масалан ташхислаш амалини бажариш оркали);

- компьютерларнинг ва тармоқ курилмаларининг конфигурацияланишини бошқариш (хусусан, инициализациялаш, кайта конфигурациялаш ва тармоқ курилмалари ва компьютерларни узуб қўйиш);

- фойдаланувчилар ва фойдаланувчилар груҳи томонидан тармоқ ресурсларидан фойдаланишни тартибга солиш (масалан, дискини ва бошқа квоталарни тартибга солиш);

- тармоқ курилмалари ва сервислар унумдорлиги даражасини бошқариш (тармоқ курилмалари ишлатилиши жадаллиги статистикасини ва хатоликлар частотасини йигини ва таҳлилини хамда олингандан маълумотлар асосида улар унумдорлиги даражасини сунъий гарзла ўрнатиш);

Олдиндан белгиланган ҳавфсизлик сиёсати асосида тармоқ ресурсларидан фойдаланишни назоратлашдан фойдаланиб маълумотлар ҳимоясини бошқариш ва уларни бузишга уринишлардан маъмурни хабардор этиш.

Корхона ахборот ҳавфсизлиги тизими корпоратив тармоқни бошқариш тизимининг энг мухим компоненти ҳисобланади. Корхона масштабидаги таксимланган тармоқда ахборотни ҳимоялаш воситаларини бошқарувчи тизим қуйидаги вазифаларни бажариши лозим:

- корхона тармоғи доирасида ҳавфсизлик сиёсатини бошқариш, алоҳида курилмалар ҳавфсизлигининг локал сиёсатини шакллантириш ва уни ахборотни ҳимояловчи барча курилмаларга етказиш;

- фойдаланиш обьектларини ва субъектларини конфигурациялашни бошқариш; ҳимоя қурилмалари ва дастурий таъминоти таркибини, версиясини, компонентларини бошқаришни ўз ичига олади;

– тақсимланган татбиқий тизимларга химоя сервисларини тақдим этиш, химояланган иловалар ва улар ресурсларини рўйхатга олиш. Иловаларнинг бу гурухи, 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 созлашни, логларни деталлаштириш сатхини 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 вактда ахборот олинишини таъминлайди;

– маҳсус химояланган иловалар, масалан амаллар устидан нотариал назорат ишини таъминлаш ҳамда регламентда кўзда тутилган тадбирларни (калитларни, паролларни, химоя қурилмаларини алмаштириш, смарт-каргаларни ишлаб чиқариш ва х.) мададлаш;

– иловаларнинг лойиха-инвентаризациялаш гурухи ишини таъминлаш. Иловаларнинг бу гурухи корхона тармоғига химоя воситаларини ўрнатишни, кўлланиладиган химоя воситаларини хисобга 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 алокани комплекслаш ва ташкил этиш муаммоси мавжуд.

## 12.2. Хавфсизлик воситаларини бошқариш архитектураси

Компания тақсимланган ахборот тизимида хавфсизлик сиёсатини муваффакиятли амалга ошириши учун хавфсизликни бошқариш марказлиштирилган бўлиши ва ишлатиладиган операцион тизимга ва татбиқий тизимларга боғлик бўлмаслиги лозим. Ундан ташкири, корпоратив ахборот тизимида кечувчи жараёнлар-

ни (рухсатсиз фойдаланиш, фойдаланувчилар имтиёзини ўзгариши ва х.) рўйхатга олиш тизими ягона бўлиши ва маъмурга корпоратив ахборот тизимидағи барча ўзгишларнинг тўлик 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 қуидаги хусусиятларга эга бўлган комплекс бошқариш тизимини қуришга имкон беради:

- корхонанинг барча ресурслари (хавфсизлик сиёсати объектлари) учун химоялашнинг яхлитлигини, зиддиятлик эмаслигини ва коидалар тўпламининг тўлалигини таъминловчи, барча мавжуд химоя воситаларини корхона хавфсизлиги сиёсати асосида бошқариш;
- ресурсларни гавсифловчи шахсий восигалар хамда корхонанинг бошка каталоглари билан алокаси бўйича фаоллашувчи корхона мухитининг ягона (таксимланган) каталоги оркали корхонанинг барча ресурсларини аниклаш;
- хавфсизлик сиёсатига асосланниб, ахборотни химоялашнинг локал воситаларини марказлаштирилган бошқариш;
- корхона мухитида сиёсат объектларини токенлар ва очик калитлар инфратузилмасидан фойдаланиб катъий аутентификациялаш;
- каталогда белгиланган корхона ресурсларидан ёки бутун каталог кисмларидан фойдаланишни маъмурлашнинг кенгайтирилган имкониятлари;
- хисоб-китобликни (корпоратив тармок масштабида тизимнинг таксимланган объектларининг ўзаро алокасидаги 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 РВМ (Policy Based Management) бошқариш» деганда корхона бизнес-объекти учун таърифланган коидалар тўплами тушунилади. Бу коидалар тўплами объектларнинг бизнес-соҳани тўлик камраб олишини ва ишлиатилувчи бошқариш коидаларининг зиддиятлик эмаслигини кафолатлади.

РВМ принципларига асосланган, корхона хавфсизлигини бошқаришга мүлжалланган GSM бошқариш тизими қуидаги талабларга жавоб беради:

- корхона хавфсизлиги сиёсати мантикий ва семантик боғланган, шаклланувчи, таҳрирланувчи ва таҳлилланувчи маълумотларнинг бир бутун тузилмасидан иборат;

- корхона хавфсизлиги сиёсати ягона контекстда химоянинг барча сатхлари учун химоянинг тармок сиёсати ва корхона ахборот ресурслари хавфсизлик сиёсатининг бир бугуни сифатида белгиланади;

- корхона ресурсларини ва хавфсизлик сиёсатини маъмурлашни снгиллаштириш мақсадида сиёсат параметрлари сони минималлаштирилади.

GSM бошқариш тизими хавфсизлик сиёсагининг 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 ахборог хавфсизлиги контекстида корпоратив тармок обьектлари ўзаро алоқасининг параметрларини тавсифловчи хавфсизлик қоидаларининг чекли тўпламидир.

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) обьектлар гурӯхи ёки хатто алоҳида компания кўрилиши мумкин.

Хавфсизликнинг глобал сиёсати тармоқдаги ўзаро алоқага, ҳамда тизимнинг назоратлаш ва бошқариш функцияларига таалукли бўлиши мумкин. Бажарадиган функциялари бўйича хавфсизликнинг глобал сиёсати қуидаги гурӯхларга бўлинади:

- *VPN қоидалари*. Қоидаларнинг бу гурӯхи IPSec протоколлари ёрдамида амалга оширилади;

- *пакетли фильтрлаш қоидалари*. Бу қоидалар Stateful ва Stateless хилидаги пакетли фильтрлашни таъминлайди.

- *proxy-қоидалар*. Бу қоидалар берилган татбикий протоколлар бошкарувида узатилувчи трафикни фильтрлашга жавоб беради;

- *аутентификацияланган/авторизацияланган фойдаланиш қоидалари*;

*– сигнализацияга ва ҳодисавий протоколлашга жавоб берувчи қоидалар.*

Хавфсизликнинг глобал сиёсати тармок сатхига хавфсизлик сиёсатининг мантикий яхлит ва семантик тўлиқ гавсифи бўлиб, унинг асосида алоҳида курилмалар хавфсизлигининг локал сиёсати курилиши мумкин.

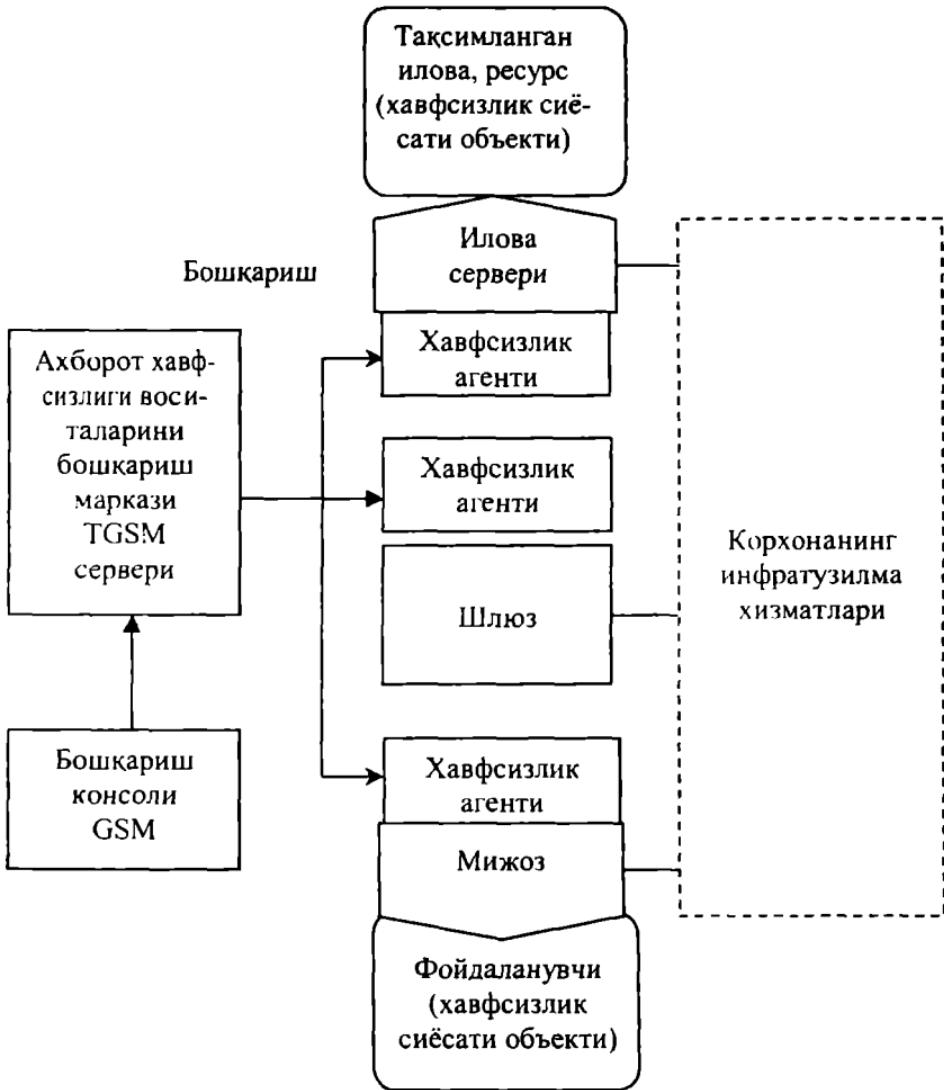
Хавфсизликнинг локал сиёсати ахборот хавфсизлигининг қандайдир сервисини амалга оширувчи ҳар қандай ҳимоялаш воситасига зарур ҳисобланади. Анъанавий ёндашишда маъмурга ҳар бир ҳимоя воситасини алоҳида созлашга ёки энг оддий созлашни узелларнинг катта сонига қайтаришга (репликациялашга) тўғри келар эди. Равшанки, бу маъмурлашнинг катта сонли ҳатолигига олиб келар ва натижада корпоратив тармокнинг ҳимояланиш даражаси жиддий пасаяр эди.

Маъмур томонидан хавфсизликнинг глобал сиёсати шакллантирилганидан сўнг бошқариш маркази унинг асосида ҳар бир ҳимоя воситаси учун автоматик тарзда ҳимоялашнинг алоҳида локал сиёсатини ҳисоблади ва мос ҳимоя воситасининг бошқариш модулига зарурий созлашларни автоматик тарзда юклайди.

Тармокда хавфсизликнинг глобал сиёсатини ва муайян курилмада хавфсизликнинг локал сиёсатини амалга ошириш қоидаларининг бир-биридан фарки шундаки, хавфсизликнинг глобал сиёсатидаги қоидалардан фойдаланиш обьектлари ва субъектлари тармок чегарасида ихтиёрий равишда таксимланиши мумкин, хавфсизликнинг локал сиёсатидаги қоидалардан эса факат тармок курилмаларидан бирининг мухити чегарасида фойдаланиш мумкин.

Ахборот хавфсизлиги воситаларини бошқариш тизимининг умумий тузилма схемаси 12.4–расмда келтирилган. Асосий хавфсизлик воситаларининг вазифалари куйидагича. Мижоз шахсий компьютерида ўрнатилган *хавфсизлик агенти* одатда, «мижоз-сервер» иловаларида мижоз сифатида катнашувчи алоҳида фойдаланувчини ҳимоялашга мўлжалланган.

Иловалар серверига ўрнатилган *хавфсизлик агенти* таъминлашга мўлжалланган иловаларнинг сервер компоненти хавфсизлигини таъминлашга мўлжалланган. Шлюз компьютерига ўрнатилган *хавфсизлик агенти* турли тармок хавфсизлиги сиёсатини мувофиқлаштириш масаласини ечган ҳолда, корхона ичида ёки корхоналар орасида тармок 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 курилмаси хавфсизлигининг локал сиёсатига трансляциялашни, химоялаш курилмасини юклашни ва тизимнинг барча агентлари холатини назоратлашни таъминлайди.*

*Бошқарши консоли маъмур (маъмурлар) иш жойини ташкил этишга мўлжалланган. GSMнинг хар бир сервери учун бир неча консоллар ўрнатилиши мумкин.*

*Хавфсизликнинг локал агенти охирги курилмада (мижозда, серверда, шлюзда) жойлаштирилувчи дастур бўлиб. қуйидаги функцияларни бажаради:*

- хавфсизлик сиёсати обьектларини аутентификациялаш, жумладан, аутентификациялашнинг турли сервисларини интеграциялаш;*
- тизимдаги фойдаланувчини ва у билан боғлик ҳодисаларни аниклаш;*
- хавфсизлик воситаларини марказлаштирилган бошқаришни ва фойдаланиш назоратини таъминлаш;*
- иловалар манфаати учун ресурсларни бошқариш, гатбикй сатҳ ресурсларидан фойдаланишни бошқаришни мададлаш;*
  - трафикни ҳимоялаш ва аутентификациялаш;*
  - графикни фильтрлаш;*
  - ҳодисавий протоколлаш, мониторинг, хавотирли сигнализация.*

*Локал агентнинг марказий элементи – хавфсизликнинг локал сиёсатининг процессори (ISP processor) хавфсизликнинг локал сиёсатини изоҳлайди ва бошка 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 кўнгина гаҳдидлар хавфсизлик маъмурининг эътиборидан четда колиши мумкин. Шунинг учун ахборот тизимларининг мунтазам аудити ва доимий мониторинги амалга оширилиши зарур.

*Ахборот тизимлари хавфсизлигининг аудити.* Аудиткорхонанинг алоҳида соҳаларини мустакил экспертизаси. Корхона аудитининг ташкил этувчиларидан бири унинг ахборот тизими аудити хисобланади. Ахборот тизимларининг аудити – ахборот тизими ҳимояланишининг жорий ҳолаги, ундаги ҳаракатлар ва хо-

дисалар хусусидаги объектив маълумотларни олиш ва баҳолаш, улар сатхининг белгиланган мезонга мослигини аникловчи тизимли жараёндир. Аудит ўтказилиши ахборот тизимининг жорий хавфсизлигини баҳолашга, хавф-хатарни баҳолашга, уларнинг ташкилот бизнес-жараёнларига таъсирини башоратлашга ва бошкаришга, ташкилот ахборот ресурслари хавфсизлигини таъминлаш масаласига асосли ёндашишга имкон беради.

Ахборот тизимлари хавфсизлигининг аудити куйидаги боскичларни ўз ичига олади:

- аудит муолажасининг бошланиши;
- аудит ахборотини йигиш;
- аудит маълумотларини тахлиллаш;
- тавсиялар ишлаб чикиш;
- хисобот тайёрлаш.

Аудит боскичларининг бажарилиш кетма-кетлиги 12.5-расмда келтирилган.

*Аудит муолажасининг бошланиши.* Аудит, бу масалада манфатдор хисобланувчи, компания раҳбарияти ташаббуси билан ўтказилади. Аудит тадбирларнинг комплекси бўлиб, унда аудитор билан бирга компаниянинг аксарият тузилмавий бўлинмаларининг вакиллари катнашади. Бу жараёнда иштирок өтвучиларининг ҳаракатлари аник мувофиқлаштирилиши шарт. Шу сабабли, аудит муолажасининг бошланиши боскичида аудит ўтказиш режасини тайёрлаш ва тасдиқлаш, аудитор хукуки ва мажбуриятини белгилаш билан боғлик ташкилий масалалар ечилиши лозим.

Аудит муолажасининг бошланиши боскичида текшириш доираси аникланиши лозим. Компаниянинг ахборот кисми тизимининг бирини конфиденциаллик нуктаи назаридан аудитга тортиб бўлмаса, иккинчисини, етарлича жиддий бўлмаганиниги сабабли, аудит доирасидан чикариш мумкин.



12.5-расм. Аудит боскичларининг бажарилиш кетма-кетлиги.

*Аудит ахборотини йигиш.* Бу боскич энг мураккаб ва узок давом этади. Бунга сабаб, ахборот тизимига керакли ҳужжатларнинг йўклиги 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 маҳсус ташкил этилган сухбат оркали, техникавий ва ташкилий-бошқариш ҳужжатларни ўрганиш йўли билан, ҳамда ихтисослаштирилган дастурий воситалар ёрдамида ахборот тизимини тадқиқлаш оркали олади.

*Аудит маълумотларини таҳлиллаш.* Таҳлиллаш ахборот тизимларининг аудитида энг масъулиятли боскич хисобланади. Таҳлиллашда ноаник, эскирган маълумотлардан фойдаланиш ножоиздир, шу сабабли маълумотларга аниқлик киритилиши ва ахбо-

ротлар жиiddий йиғилиши мумкин. Аудит маълумотларини таҳлиллашда қуидаги учта ёндашишдан фойдаланилади.

Биринчи ёндашиш хавф-хатарларни таҳлиллашга асосланади. Хавф-хатарларни таҳлиллашдан максад мавжуд хавф-хатарларни аниклаш ва улар катталигини баҳолаш (уларга сифатий ва миқдорий баҳо бериш). Ушбу ёндашиш жуда мураккаб бўлиб, кўп меҳнат сарф этилади ва аудиторнинг энг юкори малакасини талаб килади.

Иккинчи ёндашиш ахборот хавфсизлиги стандартларидан фойдаланишга асосланган. Стандартлар ахборот тизимларининг кенг синфи учун дунё амалиётини умумлаштириш натижасида шаклланган хавфсизлик талабларининг базавий гўпламини белгилайди. Бу холда аудитордан, берилган ахборот тизими учун стандарт талаблари тўпламини тўғри танлаш талаб этилади. Соддалиги ва ишончлилиги туфайли бу ёндашиш амалда кенг кўлланилади. У ресурсларнинг минимал сарфига ахборот тизими хусусида асосланган хуносалар килишга имкон беради.

Учинчи ёндашиш олдинги иккала ёндашишни комбинациялашни кўзда тутади. Ахборот тизимига кўйиладиган хавфсизликнинг базавий талаблари стандарт орқали аникланса, берилган ахборот тизими ишлашининг хусусиятларини хисобга олувчи қўшимча талаблар хавф-хатарларни таҳлиллаш асосида шакллантирилади.

*Тавсиялар ишлаб чиқши.* Таҳлиллаш натижалари тавсиялар ишлаб чиқиш учун асос бўлади. Аудитор тавсиялари муайян ва берилган ахборот тизимига кўлланиладиган, иқтисодий асосланган, исботланган (таҳлиллаш натижалари билан кувватланган) ва муҳимлик даражаси бўйича рутбалangan бўлиши шарт. Аудитнинг мунтазам ўтказилиши ахборот тизимининг барқарор ишлашини кафолатлайди. Шунинг учун профессионал аудит натижаларидан бири кейинги текширишларни ўтказиш режа-графигини шакллантиришдан иборат.

*Хисобот тайёрлаш.* Аудитор хисоботи аудит ўтказишнинг асосий ҳужжати хисобланади ва унинг сифати аудитор ишининг сифатини характерлайди.

Хисобот таркибида аудит ўтказиш мақсадининг тавсифи, текширилувчи ахборот тизимининг характеристикаси, аудит ўтказиш доираси ва ишлатилувчи усууллар бўйича кўрсатма, аудит маълумотлари таҳлилиниң натижаси, бу натижаларни умумлаштирувчи ва ахборот тизими химояланиш сатхининг 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**

Хозирда тармоқлараро экран, виртуал хусусий тармок, рухсатсиз фойдаланишдан химоялаш воситалари каби химоянинг анъанавий воситалари ишончли ва самарали ахборот хавфсизлиги тизимини куришга зарур бўлсада, етарли эмас. Чунки бу анъанавий воситалар факат хужумни блокировка килишга кодир, аммо хужумларни олдини олиш ва окибатларини аниклаш имконияти уларда мавжуд эмас.

Ушбу муаммонинг ечими асосланган ёндашиш фаол аудит технологияси ёки хавфсизликни фаол (адаптив) бошқариш технологияси номини олган. Хавфсизликни фаол бошқариш технологияси куйидаги компонентларни ўз ичига олади:

- ишчи станциялари, серверлар, маълумотлар базасини бошқарувчи тизимлар, тармок уланишлари ва Internet ва бошқа глобал тармоқларга уланиш нукталари каби ахборот тизими объекtlари химояланишини тахлилловчи ва заифликларини кидирувчи воситалар;

- хужумларни аниклаш ва тахлиллаш воситалари;

- инфратузилма ўзгаришида ёки хужумларда химоялаш воситаларини вақтнинг реал режимида созлашларни мослаштириш ва бошқариш воситалари.

Ахборот хавфсизлиги тизими мониторинги вазифаларини химояланишини тахлиллаш ва хужумларни аниклаш воситалари баъзари. Химояланишини тахлиллаш воситалари ишчи станцияларида ва серверларда, маълумотлар базасида операцион тизим химояси элементларининг созланишини тадқиклайди. Улар тармок топологиясини тадқиклайди, химояланмаган ёки ногўғри тармок уланишларини кидиради, тармоқлараро экранлар созланишини тахлиллайди. Химояланишини тахлиллаш воситаларини, уларнинг ишлаши бўйича хавфсизлик сканерлари деб хам юритишади. Тахлиллаш натижасида сканер маъмурга юборилувчи, таркибида аникланган заифликлар ва уларни йўкотиш коидалари бўлган хисботни шакллантиради. Агар сканер таркибида хавфсизлик воситалари созланишини бошқарувчи воситалар бўлса, у мустакил тарзда уларни қайта конфигурациялаши мумкин.

Ташкилотнинг замонавий инфратузилмасини хисобга олган холда айтиш мумкини, бундай сканерларнинг мавжудлиги ахборот тизимлари хавфсизлиги мониторингининг мухим элементи хисобланади. Таъкидлаш лозимки, бу воситалар химояни хужум содир бўлишидан аввал амалга оширади.

Ахборот тизими хавфсизлиги мониторингининг яна бир зарур элементи хужумларни аникловчи воситалардир. Хужумларни аниклаш корпоратив тармоқда кечувчи шубҳали харакатларни баҳолаш жараёнидир. Хужумларни аниклаш вактнинг реал режимида тармок трафигини, ҳамда операцион тизим ва иловаларнинг рўйхатга олиш журнallарини таҳлиллаш оркали амалга оширилади. Хужумларни аниклаш тизимининг компонентлари агентлар деб аталади, ва ишчи станцияларда, серверларда жойлаштирилади ёки тармокнинг қандайдир сегментини ёки бутун тармоқни коплайди. Агентлар ўзларининг ишида сканерлар каби маълум заифликлар рўйхатидан фойдаланиб, ҳодисаларни ушбу заифликлар билан таккослайди. Қандайдир узелда шубҳали фаолият аниқланганида хужумларни аниклаш тизими ушбу фаолият фаоллиги хусусидаги огохлантиришни маъмурга жўнатади. У огохлантиришни узелнинг ўзига жўнатиши ёки узел ишини блокировка килиш мумкин. Ушбу тизимнинг фарқли хусусияти – унинг бўлиб ўтган хужумларни аниклаш учун ҳодисалар журналини таҳлиллашидир.

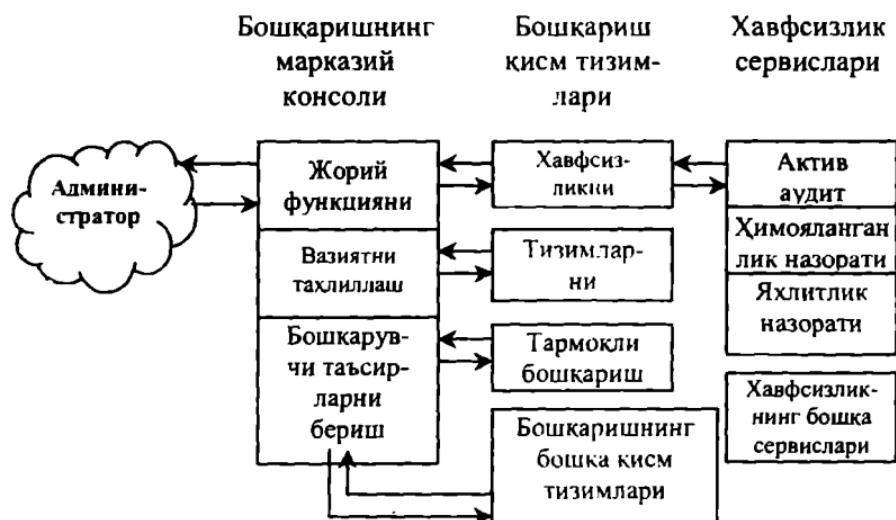
Хавфсизлик воситаларини бошқариш шакли бўйича пассив ва фаол (актив) бўлиши мумкин. Пассив бошқаришда тармокни бошқариш тизимига ёки маъмурга факат ҳабар берилса, фаол бошқаришда хужумловчи узел ёки фойдаланувчи билан мустақил тарзда сессия тугалланади.

Бундан ташқари, бу тизимнинг вазифасига тармоқдаги, иловалардаги ёки ташкилот ахборот тизимининг бошқа компонентларидаги заифликларни йўқотиш бўйича маъмурга тавсиялар ишлаб чикиш киради.

Фаол аудит тизими (мониторинги) ва умумий бошқариш ўргасида ўзаро алokane ташкил этиш мухим масалалардан хисобланади. Фаол аудит намунавий бошқариш функцияларини, яъни ахборот тизимидағи фаоллик хусусидаги маъдумотларни таҳлиллашни, жорий вазиятни акслантиришни, шубҳали фаолликка автоматик тарзда реакция кўрсатилишини бажаради. Тармокни бошқариш тизими худди шунга ўхшаш ишлайди. Фаол аудит ва умумий бошқаришни умумий ластурий-техник ва ташкилий ечим-

лардан фойдаланиб интеграциялаш максадга мувофик хисобланади. Бу интеграцияланган тизимга яхлитликни назоратлаш ҳамда ахборот тизими хатти-харакатларининг ўзига хос жихатларини кузатувчи бошқа йўналишдаги агентлар ҳам киритилиши мумкин (12.6-расм).

Бошқаришнинг марказий консоли 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 на бошқариш тизимининг интеграцияси.

Тармоқ хавфсизлигини адаптив бошқариш моделидан фойдаланиш барча таҳдидларни назоратлаш ва уларга ўз вактида реакция кўрсатиш, нафакат таҳдидларни амалга оширишга шароит яратувчи заифликларни йўкотиш, балки заифликларни пайдо бўлиш шароитларини тахлиллаш имконини беради.

## 12.4. Хавф-хатарларни таҳлиллаш ва бошқариш

Хавф-хатарларни таҳлиллаш ва бошқариш ахборот тизимидағи таҳдидлар, заифликлар ва хавф-хатарларни баҳолаш ҳамда ушбу ахборот тизими хавфсизлигининг старли даражасини таъминловчи карши чораларни аниклаш учун ишлатилади.

Хавф-хатарларни таҳлиллаш-таҳдидларни, заифликларни ва корпоратив ахборот тизими хавфсизлигига бўлиши мумкин бўлган заарларни аниклаш жараёни. Хавф-хатарларни таҳлиллашдан максад мавжуд хавф-хатарларни аниклаш ва улар меъёрини баҳолаш (уларга микдорий баҳо бериш). Хавф-хатарларни таҳлиллаш компьютер ахборот тизими хавфсизлигини текшириш бўйича тадбирни ўз ичига олади. Бу тадбирга биноан қайси ресурсларни қайси таҳдидлардан химоялаш зарурлиги ҳамда у ёки бу ресурслар қандай даражада химояга муҳтож эканлиги аникланади.

Хавф-хатарларни таҳлиллашга турли ёндашишлар мавжуд. Ёндашишни танлаш ташкилотда ахборот хавфсизлиги режимига кўйиладиган талаблар даражасига ва эътиборга олинувчи таҳдидлар характеристига (таҳдидлар таъсири спектрига) боғлик. Тарабларнинг иккита даражаси фарқланади:

- ахборот хавфсизлиги режимига минимал талаблар;
- ахборот хавфсизлиги режимига оширилган талаблар.

Ахборот хавфсизлиги режимига 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 таркалган тўплами уларнинг эҳтимоллигини баҳоламасдан кўрилади. Вируслар, асбобускуналарнинг 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 режимига оширилган талаблар, ахборот хавфсизлиги режимининг бузилиши оғир оқибатларга сабаб бўлганида ва ахборот хавфсизлиги режимига минимал талаблар етарли бўлмаганида ишлатилади.

Ахборот хавфсизлиги режимига оширилган талабларни таърифлаш учун ресурслар ахамиятини аниклаш, тадқикланувчи ахборот тизими учун долзарб бўлган таҳдидлар рўйхати билан стандарт тўпламни тўлдириш, таҳдидлар эҳтимоллигини баҳолаш ва ресурслар заифлигини аниклаш зарур.

Хавф-хатарни таҳлиллаш жараёнини қўйидаги боскичларга 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 боғлик хавф-хатарларни хисоблаш.

Ресурслар учта категорияга ахборот ресурсларига, дастурий таъминотга ва техник воситаларга (файл серверлари, ишчи станциялар, кўприклар, маршрутизаторлар ва х.) бўлинади. Ҳар бир категория ичida ресурсларни синфларга ва кисм синфларга ажратиш мумкин. Факат корпоратив ахборот тизими функционаллигини белгиловчи ва хавфсизликни таъминлаш нұқтаи назаридан муҳим бўлган ресурлар идентификацияланиши лозим.

Ресурснинг муҳимлиги (нархи) бу ресурснинг конфиденциаллиги, яхлитлиги ёки фойдаланувчанлиги бузилганида етказилган зарар микдори билан белгиланади. Ресурслар нархини баҳолашда ресурсларининг ҳар бир категорияси учун бўлиши мумкин бўлган зарар микдори белгиланади.

Намунавий хавфсизлик таҳдидларига корпоратив ахборот тизими ресурсларига локал масофадан хужумлар, табиий оғат, ходимлар хатоси, дастурий таъминотдаги хатолик ёки аппаратуранинг носозлиги сабаб бўлувчи корпоратив ахборот тизим ишидаги бузилишлар таалтуқли. Таҳдид даражаси деганда унинг амалга оширилиши эҳтимоллиги тушунилади.

Химоянинг бўшлиги корпоратив ахборот тизимидағи заифликларига сабаб бўлади. Заифликларни баҳолаш хавфсизлик

таҳдидларининг муваффакиятли амалга оширилиш эҳтимолигини аниклашни назарда тутади. Шундай қилиб, зарар етказиш эҳтимолиги таҳдидларнинг амалга оширилиши эҳтимолиги ва заифлик миқдори орқали аниқланади.

Хавф-хатар даражаси ресурс нархи, таҳдид даражаси ва заифлик миқдори асосида аниқланади. Ресурс нархи, таҳдид даражаси ва заифлик миқдори ошиши билан хавф-хатар даражаси хам ошади. Хавф-хатарлар даражасини баҳолаш асосида хавфсизлик талаблари белгиланади.

Хавф-хатарларни бошқариш масаласи, хавф-хатар даражасини мақбул миқдоргача камайтиришга имкон берувчи карши чораларни асосли танлашни ва амалга ошириш нархини баҳолашни ўз ичига олади. Табиийки, қарши чораларни амалга ошириш нархи бўлиши мумкин бўлған зарар миқдоридан кам бўлиши керак.

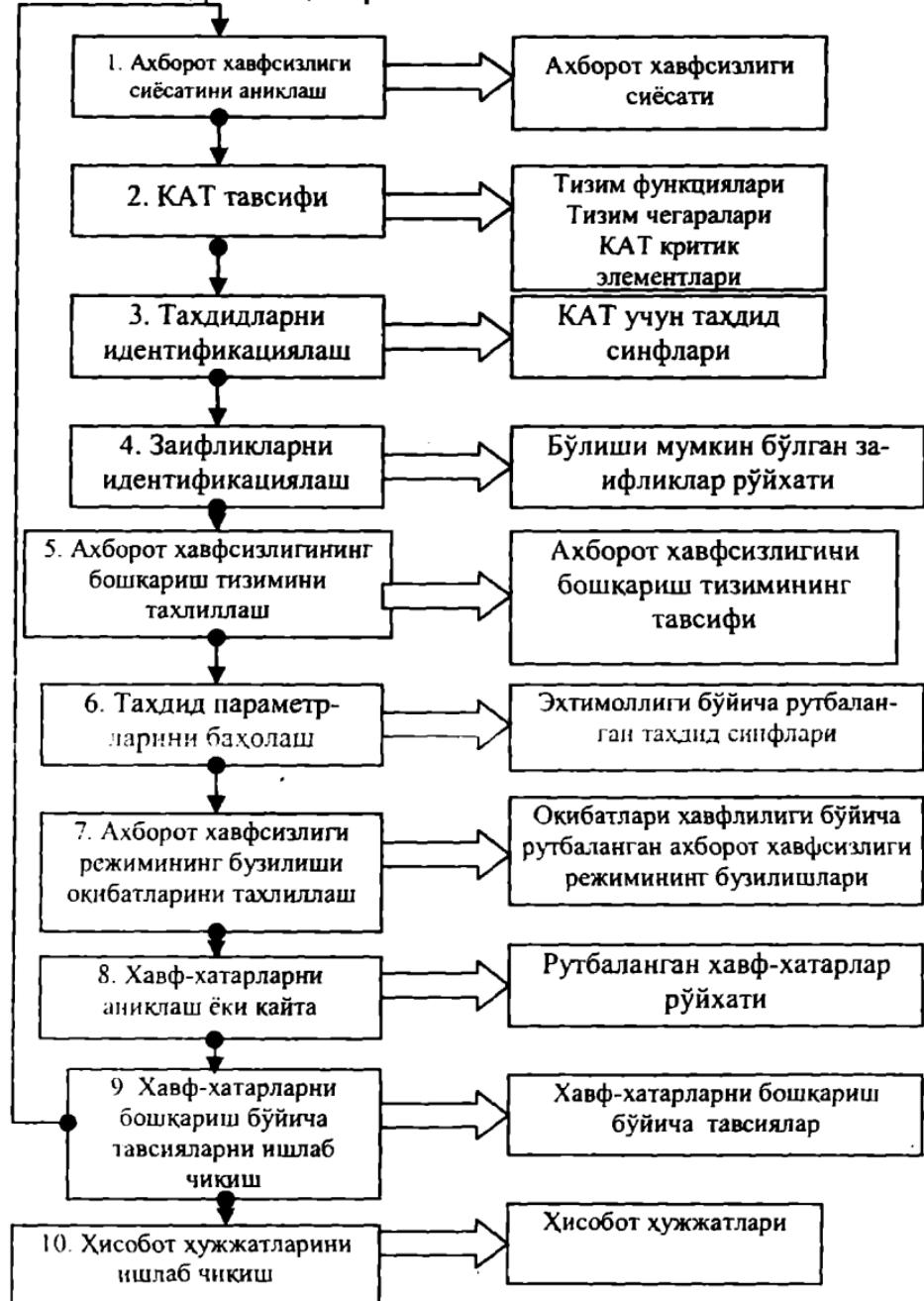
12.7-расмда хавф-хатарларни бошқариш технологиясининг босқичлари келтирилган.

*Ахборот хавфсизлиги сиёсатини аниқлаш.* Бу босқичда ахборот хавфсизлиги соҳасидаги кўдланма-хужожатлар, стандартлар, ахборот хавфсизлителгининг асосий қоидалари, хавф-хатарларни бошқаришга ёндашишлар аниқланади ҳамда карши чоралар структуризацияланади ва корпоратив ахборот тизимини сертификациялаш тартиби белгиланади.

*Корпоратив ахборот тизимини (КАТ) тавсифлаш.* Ушбу босқичда ахборот хавфсизлиги соҳасидаги ҳалқаро, 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.

**Хавф-хатарларни таҳлиллаш  
ва бошқариш боскичлари**

**Натижавий маълумотлар**



12.7-расм. Хавф-хатарларни бошқариш технологиясининг варианти.

*Таҳдидларни идентификациялаш.* Ушбу боскичда таҳдидлар рўйхати тузилади ва уларнинг даражаси баҳоланади. Бунда турли ташкилотларнинг таҳдидлар синфлари рўйхатидан хамда берилган таҳдидни амалга ошириш эҳтимоллигининг рейтинги ёки ўртача кийматидан фойдаланиш мумкин.

*Заифликларни идентификациялаш.* Ушбу боскичда берилган корпоратив ахборот тизимининг заифликлари рўйхати, уларнинг амалга оширилишидаги жоиз натижалар кўрсатилган ҳолда тузилади. Мавжуд корпоратив ахборот тизими учун рўйхатлар катор манбалардан фойдаланилиб тузилади. Бу манбаларга заифликларни тармок сканерлари, турли ташкилотларнинг заифликлар каталоги, хавф-хатарларни таҳлилловчи ихтисослаштирилган усууллар киради.

*Корпоратив ахборот тизимининг бошқариши тизимини таҳлилаш.* Ушбу боскичда бошқариш, тизими, аникланган таҳдидларга ва заифликларга жоиз бўлган таъсир нуктаи назаридан таҳлилланади.

*Таҳдидлар параметрларини баҳолаши.* Ушбу боскичда ходисага олиб келувчи заифликнинг амалга оширилиши имконияти баҳоланади. Баҳолашнинг намунавий шкаласи – бир неча рутбали (масалан, паст, ўрта, ва юқори сатҳ) сифатий (балли) шкаладир. Бундай баҳо эксперт томонидан мавжуд объектив факторларни хисобга олган ҳолда берилади.

*Ахборот хавфсизлиги режимининг бузилиши оқибатларини таҳлилаш.* Ушбу боскичда ахборот хавфсизлиги режимининг бузилиши баҳоси аникланади. Бузилиш оқибатлари молиявий йўқотишларга, обрўисизланишга, 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 баҳолаши.* Ушбу боскичда ахборот ресурслари хавфсизлигининг бузилиши хавф-хатар даражаси баҳоланади. Хавф-хатар даражаси киймати таҳдидлар, заифликлар даражасига ва бўлиши мумкин бўлган оқибатлар оғирлигига боғлик. Хавф-хатарларни баҳолашда сифатий ва микдорий усууллардан фойдаланилади. Сифатий усул ишлатилганда ахборот хавфсизлиги бузилишининг бўлиши мумкин бўлган хавф-хатарлар хавфлилиги даражаси бўйича рутбаланиши лозим. Микдорий усул ишлатилганда хавф-хатарлар микдорий шкалаларда баҳоланиши мумкин. Бу тав-

сия этилаётган карши чораларнинг нархи-самарадорлигини таҳлиллашни осонлашгиради. Аммо бу ҳолда дастлабки маълумотларни ўлчаш шкалаларига ва ишлатилаётган моделнинг адекватлигига жуда юкори талаблар куйилади. Оддий ҳолда хавф-хатарни баҳолашда иккита омил-ходиса эҳтимоллиги ва бўлиши мумкин бўлган оқибатлар оғирлиги ишлатилиши мумкин.

*Хавф-хатарларни бошқариш бўйича тавсияларни ишлаб чиқиши.* Ушбу босқичда турли сатҳлар (ташкилий, дастурий-техник) ва хавфсизликнинг алоҳида жиҳатлари бўйича структуризацияланган қарши чораларнинг комплексӣ тавсия этилиши лозим. Таклиф этилувчи карши чоралар комплекси хавф-хатарларни бошқаришнинг танланган стратегиясига биноан курилади.

*Ҳисобот ҳужжатларни ишлаб чиқиши.* Ушбу босқичда хавф-хатарларни таҳлиллаш ва бошқаришнинг барча босқичлари бўйича иш натижалари акслантирилган ҳисобот ҳужжатлари тайёрланади.

Таъкидлаш лозимки, хозирда ахборот хавф-хатарларини баҳолашни автоматлаштириш мақсадида дастурий маҳсулотлар ишлаб чикилган.

## 12.5. Ахборот хавфсизлиги тизимини қуриш методологияси

**Ахборот хавфсизлиги моделини қуриш.** Корхонадаги ахборот хавфсизлиги бўйича тадбирлар қонун чиқариш, ташкилий ва дастурий-техник ҳарактерга 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 ҳалқаро стандартларга асосланган корхона ахборот хавфсизлигининг концептуал моделидан фойдаланиш мумкин.

Куйидаги ҳалқаро стандартлар корпоратив ахборот тизими химояланишини баҳолаш мезонини ва химоялаш механизмларига кўйиладиган 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 ҳалқаро стандартларга тўла мос равишда тузилган корхона ахборот хавфсизлигининг концептуал модели 12.8-расмда келтирилган.



#### Асосий белгилашлар

→ Бошқарувчи таъсирлар

→ Табиий таъсирлар

12.8-расм. Корхона ахборот хавфсизлиги тизимининг концептуалъ модели.

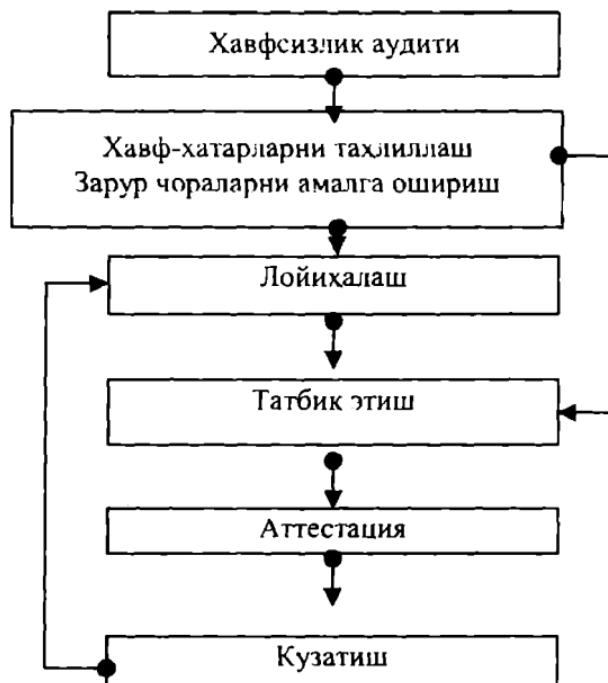
Корхона ахборот хавфсизлигининг концептуалъ моделида куидаги омиллар хисобга олинган:

– пайдо бўлиш эҳтимоллиги ва амалга оширилиш эҳтимоллиги билан характерланувчи ахборот хавфсизлиги *таҳдиidlari*;

- 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 харакатдаги субъектлари – Бузғунчи (таҳдидлар манбани ифодаловчи) ва Эга (корхона маъмури) обьект-Ресурсга қарама-карши мақсадларда таъсир киладилар. Ресурс-корхонанинг моддий ва ахборот ресурсларини ва ахборот хавфсизлиги ҳолатини ифодалайди.

**Ахборот хавфсизлиги тизимини қуриш боскичлари.** Ахборот хавфсизлиги тизимини қуриш боскичлар кўйидаги стандартлаштирилган кетма-кетликда амалга оширилади: хавфсизлик аудити; хавф-хатарларни таҳлиллаш, тизимни лойихалаш, жорий этиш, аттестациялаш ва кузатиш (12.9-расм).



12.9-расм. Ахборот хавфсизлиги тизимини қуриш боскичлари.

*Хавфсизлик аудити.* Ҳозирда «хавфсизлик аудити» тушунчаси етарлича кенг талкин этилади. Аудитнинг куйидаги кўринишлари фарқланади.

- ахборот хавфсизлигини тестли бузиш;
- экспресс-текшириш;
- тизимни аттестациялаш;
- лойиҳагача текшириш.

Ахборот хавфсизлиги тестли бузиш корпоратив ахборот тизимининг химояланиш даражасини аниклаш нуктаи назаридан самарали хисобланмайди. «Бузувчи»нинг асосий максади бир икки заификларни топиб, уларни тизимдан фойдаланишда ишлатиш. Агар «тестли бузиш» муваффакиятли чикса, ушбу муайян «бузиш»нинг мумкин бўлган сценарийси ривожини олдини олиб, заификларни кидиришда давом этиш керак. «Тестли бузиш»нинг муваффакиятсизлигини баббаравар тестланувчи тизимнинг химояланганлиги ва тестларнинг этишмаслиги каби талқин килиш мумкин.

Экспресс-текшириш доирасида. одатда, кўп вакт 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 аниклаш зарурияти туғилганда ўтказилади.

Тизимни аттестациялаш тизимнинг ахборот ресурсларининг химояланиш талабларига мослигини текшириш мақсадида амалга оширилида. Бунда ҳам ташкилий, ҳам техник жиҳатдан талаблар тўплами расмий текширилади, хавфсизлик воситаларининг амалга оширилишининг тўликлиги ва етарлилиги кўрилади.

Лойиҳагача текшириш аудитнинг энг кўп меҳнат талаб киладиган варианти хисобланади. Бундай аудит ахборот ресурслари иловаларида корхона ташкилий тузилмасини ва ходимларнинг уёки бу иловалардан фойдаланиш коидаларини тахлил этишни кўзда тутади. Сўнгра иловаларнинг ўзи тахлилланади. Ундан кейин бир сатҳдан иккинчи сатҳнинг фойдаланишдаги муайян хизматлар ҳамда ахборот алмашишга зарур бўлган хизматлар тахлилланиши лозим. Сўнгра хавфсизликнинг ўрнатилган воситаларини тахлиллаш билан тасаввур тўлдирилади.

*Хавф-хатарларни таҳлиллаш* 12.4-бўлимда батафсил кўрилган. Ахборот хавфсизлиги бузилганда лойиҳагача текшириш, хавф-

хатарларни таҳлиллаш билан биргаликда ахборот тизимидағи мавжуд хавф-хатарларни рутбалашта ва адекват чораларни ишлаб чикишга имкон беради.

*Тизимни лойиҳалаш.* Ҳимояни ташкил этиш стратегияси нұктай назаридан ресурслы ва сервисли ёндашиш фарқланади. Ресурслы ёндашишда тизим ресурслар түплами сифатида күрилади ва ахборот хавфсизлиги тизимининг компонентлари бу ресурсларга боғланади. Ресурслы ёндашиш амалга оширилганида ахборотни ҳимоялаш масаласи хизматлар тузилмасига күшімча чеклашларсиз ечилади. Бу эса бир жинсли бўлмаган тизим шароитида мумкин эмас. Сервисли ёндашишда тизим фойдаланувчиларга тақдим этилувчи хизматлар түплами каби талкин килинади. Ҳозирги вактда сервисли ёндашиш афзалрок хисобланади, чунки у тизимда амалга оширилган хизматларга боғланади ва «ортикча» хизматларни рад этиш хисобига катор таҳдидларни истисно килинишига имкон беради. Бу эса тизимни янада мантиқан асосланган тизимга айлантиради. Айнан сервис ёндашиш хавфсизликнинг замонавий стандартлари, хусусан ISO/IEC 15408 асосида ётади.

Ахборот хавфсизлиги тизимни куришнинг иккита асосий сценарийси мавжуд: маҳсулотли ва лойиҳали. Маҳсулотли сценарий (ёндашиш) доирасида аввал ҳимоя воситалари түплами танланади, уларнинг функциялари таҳлилланади, сўнгра функциялар таҳлили асосида ахборот ресурсларидан фойдаланиш сиёсати белгиланади.

Лойиҳага харажатлар нұктай назаридан маҳсулотли сценарий энг арzon хисобланади. Ундан ташқари, ечимларнинг танқислиги шароитида кўпинча маҳсулотли ёндашиш ягона хисобланади (масалан, криптографик ҳимояда факат шу ёндашиш кўлланилади).

Лойиҳали сценарийда аввал хавфсизлик сиёсати ишлаб чиқилади, унинг асосида хавфсизлик сиёсатини амалга оширишда зарур бўлган функциялар аникланади, сўнгра бу функциялар бажарилишини таъминловчи ҳимоя воситалари танланади.

Лойиҳали сценарий асосида курилган тизимлар яхширок оптимизацияланган ва аттестациянинг юкори натижаларини беради. Ушбу ёндашиш маҳсулотли ёндашишдан фарқли равища бошидан у ёки бу платформа билан боғланмаганлиги туфайли, катта гетероген тизимларни куришда афзал хисобланади. Ундан ташқари, узок муддатга мўлжалланган ечимларни таъминлайди, чунки хавфсизлик сиёсатини ўзgartирмасдан ечимларни ва ҳимоя воситаларини алмаштиришга имкон беради.

Ахборот хавфсизлиги тизими архитектурасини танлаш нуктаи назаридан обьектли, татбикий ёки аралаш ёндашишдан фойдаланилади. Объектли ёндашиш ахборот хавфсизлигини у ёки бу обьект (бўлинма, филиал, ташкилот) тузилмаси асосида яратади. Объектли ёндашишнинг кўлланиши ташкилий чораларнинг бир жинсли тўпламини мададловчи хавфсизлик механизмлари учун универсал ечимлар тўпламидан фойдаланишини кўзда гутади. Бундай ёндашишга мисол тариқасида ташки ахборот алмашиш, локал тармок, 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 тариқасида автоматлаштиришнинг алоҳида масаласи (бухгалтерия, кадрлар ва х.) учун кисм тизимларнинг химоясини кўрсатиш мумкин. Ушбу ёндашишнинг камчилиги – маъмурлаш ва ишлатиш харажатларини минималлаштириш мақсадида хавфсизликнинг турли воситаларини уйғуналаштириш зарурияти.

Аралаш ёндашиш юкорида тавсифланган иккита ёндашишни комбинациялашни кўзда тутади. Бундай ёндашиш лойихалаш босқичида кўпроқ меҳнат гаҳаб киласада, ахборот хавфсизлиги тизимини жорий этиш ва ишлатиш нархи бўйича афзалликларни бериши мумкин.

*Жорий этиши.* Жорий этиш босқичи куйидаги кетма-кет ўтказилувчи тадбирларни ўз ичига олади:

- химоя воситаларини ўрнатиш ва конфигурациялаш;
- ходимларни химоя воситалари билан ишлашга ўргатиш;
- дастлабки синовни ўтказиш;
- тажрибавий ишлатишга тошириш.

Тажрибавий ишлатиш, ахборот хавфсизлиги тизимини ишчи режимига туширишдан аввал, унинг ишлашидаги мумкин бўлган камчиликларни аниклашга ва йўкотишга имкон беради. Агар тажрибавий ишлатиш жараёнида компонентларнинг тўғри ишламаслиги фактлари аникланса, химоя воситалари созланишига ва уларнинг ишлаш режимларига ва х. тузатишлар киритилади.

*Тизимни аттестациялаш.* Ахборот хавфсизлиги тизимини ваколатли идора томонидан аттестациялаш унинг функционал

тўликлигини ва корпоратив ахборот тизими химоясининг талаб килинган даражаси таъминланганлигини тасдиқлашга имкон беради. Тизимнинг аттестацияси хавфсизлик аудитининг бир кўриниши хисобланади ва ишлатилувчи чоралар комплекси ва химоя восита-ларининг хавфсизлик даражаси талабларига мослигини баҳолаш мақсадида химояланувчи корхонани ишлатишнинг реал шароитла-рида комплекс текширишни кўзда тутади.

Аттестация натижасида хисобот ҳужжати тайёрланади ва мос-лик аттестати берилади. Бу аттестат конфиденциал ахборот билан аттестатда кўрсатилган вакт мобайнода ишлаш хукукини беради.

*Кузатиш.* Ахборот хавфсизлиги тизимининг ишга лаёкат-лигини 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 кўнкимларини талаб этади ва химояланувчи тизим эгаси – ташкилот штатидаги ахборот хавф-сизлигига жавоб берувчи ходимлар томонидан ёки ихтисослашти-рилган ташкилот ходимлари томонидан амалга оширилиши мум-кин.

Кўрилган методология коидаларидан фойдаланиш корпоратив ахборот тизимининг умумий ривожи билан бирга ривожлантири-лиши ва модификацияланиши мумкин бўлган ахборот хавфсизли-гининг самарали ва ишончли тизимини куришга имкон беради.

## **ФОЙДАЛАНИЛГАН АДАБИЁТЛАР**

1. С.С.Косимов. Ахборот технологиялари. Ўкув қўлланма. – Т., Алокачи, 2006.
2. С.К.Ғаниев, М.М. Каримов. Ҳисоблаш системалари ва тармокларида информация химояси. Олий ўкув юрт.талааб. учун ўкув қўлланма. – 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, Дэвид 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](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](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 мухофазаси. Электрон ракамли 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 ракамли имзо очик қалити 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](http://www.nasa.gov/statistics)

34. [www.security.uz](http://www.security.uz)

35. [www.cert.uz](http://www.cert.uz)

36. [www.uzinfocom.uz](http://www.uzinfocom.uz)

## Қисқартирилган сўзлар

<b>ACK</b>	Acknowledgement – тасдиқлаш
<b>AES</b>	Advanced Encryption Standard – американинг янги шифрлаш стандарти
<b>AH</b>	Authentication Header – аутентификацияловчи сарлавҳа
<b>ANS</b>	Adaptive Network Security – хавфсизликни адаптив бошқариш модели
<b>ANSI</b>	American National Standard Institute – АҚШнинг миллий стандартлаштириш институти
<b>AS</b>	Authentication Server - аутентификациялаш сервери
<b>ASA</b>	Adaptive Security Algorithm – хавфсизликнинг адаптив алгоритми
<b>ASP</b>	Applications Service Providing – серверда исъемолчидан масофа да жойлашганд иловаларга Internet ёки хусусий тармоқ орқали хизмат кўрсатиш
<b>B2B</b>	Business to Business – «бизнес-бизнес» схемаси
<b>B2C</b>	Business to Consumer - «бизнес – истеъмолчи» схемаси
<b>CA</b>	Certification Authorities – сертификациялаш маркази
<b>CEK</b>	Content Encryption Key – маълумотларни шифрлаш калити
<b>CHAP</b>	Challenge Handshake Authentication Protocol – «кўл узатиши» мувоффаси асосида аутентификациялаш протоколи
<b>DDoS</b>	Distributed Denial of Service – хизмат кўрсатишдан бош тортишга ундейдиган тақсимланган хужум
<b>DHCP</b>	Dynamic Host Configuration Protocol – хостларни динамик конфигурациялаш протоколи
<b>DNS</b>	Domain Name Server – доменли исмлар хизмати
<b>e business</b>	electronic business – электрон бизнес
<b>e commerce</b>	electronic commerce – электрон тижорат
<b>ECP</b>	Encryption Control Protocol – шифрлашни бошқариш протоколи
<b>ESP</b>	Encapsulated Security Payload – киритилган узатиладиган химоялаган маълумотлар
<b>FTP</b>	File Transfer Protocol – файлларни узатиш протоколи

<b>GSM</b>	Global System for Mobile Communications – мобиль алоқанынг глобал тизими
<b>GSP</b>	Global Security Policy – VPN учун глобал хавфсизлик сиёсати
<b>HDLC</b>	High level Data Link Control – юкори сатхадаги маълумотларни узатиш каналини бошқариш
<b>HMAC</b>	Hashing for Message Authentication – калитларни хэшлаш оркали хабарларни аутентификациялаш
<b>HTML</b>	HyperText Markup Language – Web-саҳифаларни гиперматнли белгиловчи тил
<b>HTTP</b>	HyperText Transfer Protocol – гиперматнли файлларни узатиш протоколи
<b>ICMP</b>	Internet Control Message Protocol – Internet тармогида хабарларни бошқариш протоколи
<b>IETF</b>	Internet Engineering Task Force – Internetни лойихалаш муаммолари гурухи
<b>IKE</b>	Internet Key Exchange – Internetда калитларни алмасишиш протоколи
<b>IP</b>	Internet Protocol – тармоқлараро маълумотларни алмашинишнинг Internet протоколи
<b>IPSec</b>	Internet Security Protocol – тармоқлараро маълумотларни хавфсиз алмашиниш Internet протоколи
<b>IRC</b>	Internet Relay Chat – Internet да чат-анжуманларни ташкил этиш хизмати
<b>ISO</b>	International Standards Organization – халкаро стандартлаштириш ташкилоти
<b>ISP</b>	Internet Service Provider – Internet хизматларини таъминотчиси
<b>KDC</b>	Key Distribution Center – калитларни тақсимлаш маркази
<b>KEK</b>	Key Encryption Key – калитларни шифрлаш учун калит
<b>KS</b>	Kerberos Server – kerberos тизими сервери
<b>L2F</b>	Layer2 Forwarding – иккинчи (канал) сатҳда маълумотларни узатиш протоколи
<b>L2TP</b>	Layer2 Tunneling Protocol – канал сатҳида маълумотларни туннеллаш протоколи
<b>LAC</b>	L2TP Access Concentrator – L2TP руҳсатлар концентратори
<b>LAN</b>	Local Access Network – маҳаллий тармок
<b>LCP</b>	Link Control Protocol – уланишларни бошқариш

	протоколи
<b>LDAP</b>	Lightweight Directory Access Protocol – каталоглардан фойдаланишларни соддалаштирилган протоколи
<b>LNS</b>	L2TP Network Server – L2TP тармок сервери
<b>LSP</b>	Local Security Policy - маҳаллий хавфсизлик сиёсати (мижоз учун)
<b>MAC</b>	Message Authentication Code – хабарларни аутентификациялаш коди
<b>MD</b>	Message Digest – хабарлар дайджести
<b>NAT</b>	Network Address Translation – тармок манзилларини трансляциялаш
<b>NCP</b>	Network Control Protocol – Тармокни бошқариш протоколи
<b>NIST</b>	National Institute of Standards and Technology – АҚШнинг стандартлар ва технологиялари миллий институти
<b>NNTP</b>	Network News Transfer Protocol – тармок янгиликларини узатиш протоколи
<b>OSI</b>	Open Systems Interconnection – очик тизимлар ўзаро ботликлиги
<b>OTK</b>	One Time Key – Бир маротабалик калит.
<b>P2P</b>	Peer to Peer или Partner to Partner – бизнес муносабатининг «тeng-teng» схемаси
<b>PAP</b>	Password Authentication Protocol – парол бўйича аутентификациялаш протоколи
<b>PIN</b>	Personal Identification Number – шахсий идентификация коди
<b>PKD</b>	Public Key Directory – очик калитлар каталоги
<b>PKI</b>	Public Key Infrastructure – очик калитларни бошқариш инфратузилимаси
<b>PPP</b>	Point to point Protocol – икки нуктали боғланиш протоколи
<b>PPTP</b>	Point to Point Tunneling Protocol – икки нуктали боғланиш учун туннелилаш протоколи
<b>POP</b>	Post Office Protocol – фойдаланувчи ўзига келган электрон хабарлардан фойдаланишига имкон берувчи протокол
<b>RADIUS</b>	Remote Authentication Dial In User Service – фойдаланувчиларни боғланадиган линиялар бўйича масофадан аутентификациялаш тизими
<b>RAS</b>	Remote Access Service – масофадан фойдаланаш хизмати
<b>RFC</b>	Request For Comments – изохларни сўрови

<b>RMON</b>	Remote MONitoring – тармок ускуналарини масофадан мониторинглашнинг стандарт спецификацияси
<b>RSA</b>	Rivest, Shamir, Adleman – Райвест, Шамир, Адлеман. Асимметрик криптоалгоритм
<b>SHA</b>	Secure Hash Algorithm – химояланган хэшлеш алгоритми
<b>SKIP</b>	Simple Key management for Internet Protocols – internet протоколи учун калитларни оддий бошқариш
<b>SMTP</b>	Simple Mail Transfer Protocol – электрон почтанинг оддий протоколи
<b>SNMP</b>	Simple Network Management Protocol – тармоқни бошқаришнинг оддий протоколи
<b>SPD</b>	Security Policy Database – хавфизлик қоидаларининг маълумотлар базаси
<b>TACACS</b>	Terminal Access Controller Access Control System – Масофадан фойдаланишни марказлаштирилган назоратлаш протоколи
<b>TCP</b>	Transport Control Protocol – узатишларни бошқариш протоколи
<b>TELNET</b>	Виртуал терминал протоколи – масофадаги компьютерда дастурни бажаришга мўлжалланган протокол
<b>TFN</b>	Triple Flood Net – DDoS хужумлар учун инструментал восита:ардан бири
<b>TGS</b>	Ticket Granting Server – мандатларни тарқатиш сервери
<b>TLS</b>	Transport Layer Security – транспорт сатхининг химояси
<b>UDP</b>	User Data Protocol – фойдаланувчининг маълумотларини узатиш протоколи
<b>VPN</b>	Virtual Private Network – химояланган виртуал тармок
<b>WAN</b>	Wide Area Network - глобал тармок
<b>WWW</b>	World Wide Web – Internetнинг гиперматнли ахборотлар хизмати
<b>XML</b>	Extended Mark-up Language – белгилашнинг кенгайтирилган тили
<b>МББТ</b>	Маълумотлар базасини бошқариш тизими

**АХБОРОТ ХАВФСИЗЛИГИ  
(АХБОРОТ-КОММУНИКАЦИОН ТИЗИМЛАР  
ХАВФСИЗЛИГИ)**

Тошкент – «ALOQACHI» – 2008

Мухаррир: М.Миркомилов

Тех.мухаррир: А.Мойдинов

Мусаххиҳа: Г.Каримова

Комп. сахифаловчи: Г.Арифходжаева

Босишга рухсат ётилди 00.05.2008 йил. Бичими 60x84  $\frac{1}{16}$ .

«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 шахри, А. Темур, 108-үй.

