ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технологиялар қорғауды қамтамасыз ету әдістері АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ЖЕЛІЛЕРІН ҚОРҒАУ 4-бөлім Қашықтан қол жеткізуді қорғау

Технологии информационные Методы обеспечения защиты ЗАЩИТА СЕТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ Часть 4 Защита удалённого доступа

ҚР СТ ИСО/МЭК 18028-4 - 2007

ISO/IEC 18028-4:2005(E) Information technology Security techniques. It network security. Part 4. Securing remote access (IDT)

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті (Мемстандарт)

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технологиялар

қорғауды қамтамасыз ету әдістері
АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ЖЕЛІЛЕРІН ҚОРҒАУ
4-бөлім
Қашықтан қол жеткізуді қорғау

ҚР СТ ИСО/МЭК 18028 – 4 - 2007
ISO/IEC 18028-4:2005(E) Information technology Security techniques. It network security. Part 4. Securing remote access (IDT)

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігі
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

Алғысөз

1 «Гранит» арнаулы конструкторлық-технологиялық бюросы» ЖШС 3-тармақта көрсетілген стандарттың өзінің түпнұсқалық аудармасы негізінде **ӘЗІРЛЕП ЕНГІЗДІ**

2 Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті төрағасының 2007 жылғы 24 желтоқсандағы № 691 бұйрығымен **ҚАБЫЛДАНЫП, ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 Осы стандарт ИСО/МЭК 18028-4:2005(Е) «Ақпараттық технология. Қорғау әдістері. АТ желілерін қорғау. 4-бөлім. Қашықтан қол жеткізуді қорғау». (ISO/IEC 18028-4:2005(E) «Information technology. Security techniques. IT network security. Part 4. Securing remote access») халықаралық стандартымен бірдей

4 Осы стандарт атауы ҚР СТ 1.5-2004 «Стандарттарды құруға, баяндауға, ресімдеу мен мазмұнына қойылатын жалпы талаптарына» сәйкес берілуі үшін, көрсетілген халықаралық стандарт атауына қатысты өзгертілді

5 Осы стандартта Техникалық реттеу туралы 2004 жылғы 9 қарашадағы № 603-II, Ұлттық қауіпсіздік туралы 1998 жылғы 26 маусымдағы № 233-I, Қазақстан Республикасындағы Тілдер туралы 1997 жылғы 11 шілдедегі № 151-I Қазақстан Республикасының Заң нормалары жүзеге асырылды

6 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2012 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

7 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Осы стандартқа енгізілетін өзгертулер туралы ақпарат жыл сайын шығатын «Стандарттау бойынша нормативтік құжаттар» ақпараттық сілтемесінде, ал өзгерістер мен түзетулер мәтіні – ай сайын шығатын «Стандарттау бойынша нормативтік құжаттар» ақпараттық сілтемелерінде жарияланады. Осы стандарт қайта қаралатын (өзгерту, ауыстыру) немесе жойылатын жағдайда, тиісті ақпарат ай сайын шығатын «Стандарттау бойынша нормативтік құжаттар» ақпараттық сілтемесінде жарияланатын болады

Мазмұны

Кіріспе

Ақпараттық технологияларда (АТ) ұйымдар шегіндегі сияқты, сонымен қатар, ұйымдар арасында да желілерді пайдалану қажеттігі артып келеді. Желілерді қауіпсіз пайдалану үшін, белгілі бір талаптарды орындау қажет.

Желіге арналған қашықтан қол жеткізу саласы АТ қауіпсіздігін қамтамасыз ету үшін, арнайы шаралар қолданылуын талап етеді. Осы стандартта электронды поштаны пайдаланғанда, файлдарды бергенде немесе жай қашықтан жұмыс істеу кезінде желілерге қорғалған қашықтан қол жеткізуді қамтамасыз ету бойынша нұсқаулық болады.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технологиялар ҚОРҒАУДЫ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ЖЕЛІЛЕРІН ҚОРҒАУ

4-бөлім Қашықтан қол жеткізуді қорғау

Information technology. Security techniques. IT network security. Part 4. Securing remote access.

Енгізілген күні 2009.01.01.

1 Қолданылу саласы

Осы стандартта қашықтан қол жеткізуді қауіпсіз пайдалану бойынша ұсынымдар – компьютерді басқа компьютермен немесе ортақ пайдалану желісі арқылы желімен, мысалы, Интернетпен қашықтықтан қосу әдістері, сондай-ақ осы әдістің АТ қауіпсіздігіне әсер етуі туралы мәліметтер болады. Стандарттың осы бөлімінде қашықтан қол жеткізудің әртүрлі типтері, оның ішінде қашықтан қол жеткізуге қатысты пайдаланылған хаттамалар, түпнұсқаландыру мәселелері талқыланады, сондай-ақ қашықтан қол жеткізуді қауіпсіз орнату тәсілдері туралы ілеспе ақпарат болады. Стандарттың бұл бөлімі осы қосылу түрін пайдалануды жоспарлайтын немесе ендігі пайдаланып, оны қалай қауіпсіз орнатып, онымен қалай жұмыс істеу керектігі туралы кеңесті қажет ететін желі әкімгерлері мен инженерлерге көмек үшін арналған.

2 Терминдер, анықтамалар мен қысқартулар

Осы стандартта мынадай терминдер тиісті анықтамаларымен қолданылды:

2.1 **Қол жеткізу нүктесі;** AP (Access Point)**:** Сымсыз желіден жердегі желіге қол жеткізуді қамтамасыз ететін жүйе.

2.2 **Кеңейтілген шифрлау стандарты;** AES (Advanced Encryption Standard): Ақпаратты Өңдеу бойынша Федеральдық стандартты 197 (Federal Information Processing Standard 197; FIPS 197) тиімді жүзеге асыруға мүмкіндік жасайтын, ауыспалы ұзындық кілтін пайдаланатын, симметриялық шифрлау механизмі.

2.3 **Түпнұсқаландыру** (authentication): Сәйкестендіргішпен берілген қол жеткізу субъектісінің керек-жарағын тексеру, түпнұсқаны растау. Түпнұсқаландыру қажет болғанда, пайдаланушылар белгілі нышаны (мысалы, пароль) немесе токенді иелену (мысалы, токенмен (белгімен, нышанмен), не дербес таңбасы (биометрикалық сипаттамасы) бойынша анықтап таниды. Қатаң түпнұсқаландыру дәлдік механизміне (биометрикалық сипаттамасына) немесе берілген факторлардың (көп факторлы деп аталатын түпнұсқаландыру), кем дегенде, екеуін пайдалануға негізделеді.

2.4 **Кері шақыру** (call-back)**:** Сәйкестендірудің қолданыстағы параметрлерін алғаннан кейінгі, алдын ала анықталған немесе ұсынылған орынды (немесе мекенжайын) шақыру механизмі.

Ресми басылым

2.5 **«Қосылуды сұратуды» түпнұсқаландыру хаттамасы;** CHAP (Challenge-Handshake Authentication protocol)**:** [17] анықталған қосылуларды сұрату әдісі бойынша, шақырумен алдын ала келісілген түпнұсқаландыру хаттамасы.

2.6 **Деректерді шифрлау стандарты;** DES (Data Encryption Standard): Ұзындығы 56 бит кілтті пайдаланатын, жақсы белгілі симметриялық шифрлау механизмі. Кілттің қысқа ұзындығынан ол AES стандартымен ауыстырылған, бірақ әлі күнге дейін көпше шифрлау режімінде пайдаланылады, мысалы, 3DES немесе Үш есе DES (FIPS 46-3, мұндағы Federal Information Processing Standard − ақпаратты өңдеу бойынша федеральдық стандарт).

2.7 **Қарусызданған аймақ;** ҚА (de-militarised zone - DMZ): қол жеткізу желіаралық қалқаларды пайдаланатын, арнайы саясатпен бақыланатын, бөлінген жергілікті сала немесе жергілікті желі. Бұл аймақ жалпы желі бөлігі болып табылмайды және шамалы қауіпті.

2.8 **Қызмет көрсетуде істен шығу;** DoS (Denial of Service): Мақсаты оның іс-қимылын бұзу болып табылатын, жүйеге шабуыл.

2.9 **Цифрлық абонент арнасы;** DSL (Digital Subscriber Line)**:** Жергілікті теле-коммуникациялық желілер бойынша тез қол жеткізуді қамтамасыз ететін технология [7]

2.10 **Негізгі машиналардың пішін үйлесімдерін динамикалық күйге келтіру хаттамасы;** DHCP (Dynamic Host Configuration Protocol): Іске қосуда IP-адрестеуді қамтамасыз ететін интернет-хаттама [20].

2.11 **Қапшықталмаған қауіпсіздік хаттамасы;** ESP (Encapsulation Security Protocol): IP негізделген және деректердің құпия қызметін қамтамасыз ететін хаттама. Әдетте ESP шифрлауды IP пакетіндегі деректердің ішіндегіні қорғауға арналған қауіпсіздік шарасы ретінде қамтамасыз етеді. ESP Интернет [25] стандарты болып табылады.

2.12 **Кеңейтілген түпнұсқаландыру хаттамасы** (Extensible Authentication Protocol; EAP): RADIUS қызметі қолдайтын және [23] IETF стандартталған түпнұсқаландыру хаттамасы.

2.13 **Файлдардың берілу хаттамасы;** FTP (File Transfer Protocol): Клиент пен сервер арасында файларды беруге арналған Интернет [11] стандарты (хаттама).

2.14 **IETF** (Internet Engineering Task Force)**:** Интернет техникалық стандарттарының қозғалуы мен дамуына жауапты халықаралық мамандар тобы.

2.15 **4-нұсқа хабарламаларына қол жеткізудің интернет хаттамасы** (Internet Message Access Protocol v4; IMAP4): Қашықтағы пошталық серверде орнатылған пошта жәшіктері мен пошта байланысын басқаруды және қол жеткізуді сипаттайтын электронды пошта хаттамасы ([19] анықталған).

2.16 **Жергілікті желі;** ЛВС (Local Area Network; LAN)**:** Әдеттегі (бір) ғимараттағы жергілікті желі. Шапшаң арнамен бірлескен жүйеге қосылған компьютерлер және бір-бірінен белгісіз қашықтықта орнатылған басқа құрылғылар (бөлме, ғимарат, кәсіпорын).

2.17 **Модем** (modem)**:** Цифрлық белгілерді ұқсас белгілерге (беру үшін) және ұқсас белгілерді цифрлыққа (қабылдау үшін) құрайтын аппараттық немесе бағдарламалық құрал. Мұндай типтің құралуы ұқсас байланыс желілерін пайдалану жағдайында міндетті.

2.18 **Интернетке арналған электронды поштаның көп мақсатты кеңейтілуі;** MIME (Multipurpose Internet Mail Extensions): MIME Internet электронды поштасының хабарламаларына екі еселенген деректердің (мысалы, графикалық бейнелердің) қосылу тәсілін анықтайды. Ол [18] анықталған.

2.19 **Желіге қол жеткізу сервері;** NAS (Network Access Service): Жүйе, әдеттегі қашықтағы клиенттер үшін қол жеткізуді қамтамасыз ететін компьютер.

2.20 **Бір реттік құпия белгі** (One time Password; OTP): Бір рет пайдаланылатын пароль.

2.21 **Пассивті режім;** PASV (Passive mode; PASV mode)**:** FTP бойынша қосылу режімін белгілеу режімі.

2.22 **Құпия белгіні түпнұсқаландыру хаттамасы** (Password Authentication Protocol; PAP): PPP [13] жүзеге асыруды қамтамасыз ететін, түпнұсқаландыру хаттамасы.

2.23 **Дербес цифрлық ассистент;** PDA (Personal Digital Assistant): Кейбір арнайы қызметтерді орындауға арналған, әдеттегі қолмен алып жүретін компьютер ("алақан" компьютері).

2.24 **Нүкте-нүкте хаттама;** PPP (Point-to-Point Protocol)**:** Нүкте-нүкте қосылудың сыртындағы желілік деңгейдегі ақпаратты қапшықтандырудың стандартталған әдісі [13].

2.25 **Нұсқаның пошталық хаттамасы 3;** POP3 (Post Office Protocol v3): Пошталық серверде сақталған поштаны клиенттің алуына мүмкіндік беретін, [15] анықталған электронды пошта хаттамасы.

2.26 **Жеткілікті құпиялылық деңгейі;** PGP (Pretty Good Privacy): Ашық кілттер сұлбасын пайдаланатын, жалпылама қолжетімді шифрлау бағдарламасы. Хабарлама пішіндері [16] және [26] анықталған.

2.27 **Мекемелік жеке жалғауыш** (Private Branch Exchange; PBX)**:** Жалпы қолжетімділік желілеріне қосылмаған телефон стансасы (мысалы, кеңселік АТС).**;**

2.28 **Қосылатын пайдаланушыны қашықтан түпнұсқаландыру қызметі** RADIUS (Remote Authentication Dial-In User Service): Қашықтан пайдаланушыларды түпнұсқаландыру үшін пайдаланылатын Интернет қауіпсіздігін қамтамасыз ететін хаттама [21].

2.29 **Қашықтан қол жеткізу қызметі;** RAS (Remote Access Service): Қашықтан қол жеткізуді қамтамасыз ететін аппараттық және бағдарламалық құралдар.

2.30 **Қашықтан қол жеткізу** (remote access): Жүйеге қауіпсіздік доменінен тыс, әр тараптан автоматтандырылған қол жеткізу.

2.31 **Түсініктемеге арналған сұраным;** RFC (Request for Comment): IETF ұсынған Интернет стандарттарының тобы.

2.32 **Қауіпсіздік қабығы;** SSH (Secure Shell): Қауіпсіз желімен пайдаланылатын, қашықтан қауіпсіз қосылуды қамтамасыз ететін хаттама. SSH жалпы болып табылмайды, бірақ тез арада IETF стандарты болады. SSH бастапқыда «SSH Communications Security» компаниясы әзірледі.

2.33 **Қауіпсіз сокеттер деңгейі;** SSL (Secure Sockets Layer): Клиенттерді түпнұсқаландыру, сервер, бүтіндік, құпиялылық қызметтерін қамтамасыз ететін, желілік деңгей мен қосымшалар деңгейі арасында болатын SSL хаттама. SSL «Netscape» компаниясы өңдеген және TLS негізін құрайды.

2.34 **Интернетке арналған электронды поштаны құпия/көпмақсаттылы кеңейту;** S/MIME (Security/Multipurpose Internet Mail Extensions): Бұл хаттама қауіпсіз көп мақсаттылы пошталық алмасуды қамтамасыз етеді. Оның бұрынғы 3 нұсқасы бес бөліктен тұрады: [32] және [33] хабарламаның сөз тіркесін анықтайды, ал [27], [28] және [29] хабарлама ерекшелігін, сертификатты өңдеуді және кілтті келістіру әдісін анықтайды.

2.35 **Жүйелі арнаға арналған желіаралық хаттама;** SLIP (Serial Line Internet Protocol)**:** Телефон желілерін (жүйелі желілерді) пайдаланып, деректерді беру үшін [12] анықталған дестелі хаттама.

2.36 **Қызметті орнату сәйкестендіргіші;** SSID (Set Service Identifier): Әдеттегі есімі үлгісіндегі, сымсыз қол жеткізу нүктелеріне арналған сәйкестендіргіш.

2.37 **Поштаны қайта жіберудің қарапайым хаттамасы;** SMTP (Simple Mail Transfer Protocol): Поштаны пошталық серверлерге (шығыс хабарлар) салып жіберуге арналған Интернет хаттама ([10] кеңейтулермен).

2.38 **Көліктік деңгей қауіпсіздігі хаттамасы;** TLS (Transport Layer Security): Жетілдірілген SSL ресми Интернет хаттамасы [22] болып табылады.

2.39 **Бірыңғайланған ресурс көрсеткіші;** URL (Uniform Resource Locator)**:** Web-қызметтерге арналған мекенжайлар сұлбасы.

2.40 **Үздіксіз қоректену көзі;** UPS (Uninterruptible Power Supply): Электрқоректің кернеуі кенет ажырағанда немесе кенет өзгергенде, өз құрамында қорғаныстық қамтамасыз ететін аккумуляторлар болатын құрылғы.

2.41 **Пайдаланушы датаграммасының хаттамасы;** UDP (User Datagram Protocol)**:** Қосылуды орнатусыз байланыс ұйымдастыруға арналған Желілік Интернет Хаттама [9].

2.42 **Виртуал жабық желі;** VPN (Virtual Private Network): Бөлінген ортақ желілерді пайдаланатын, яғни басқа желі құрылымынан тыс қолданылатын криптографиялық туннельдеу хаттамасына негізделген жеке желі.

2.43 **Қорғалған WiFi қол жеткізу;** WPA (WiFi Protected Access)**:** Сымсыз байланыстың құпиялылығы мен бүтіндігін қамтамасыз етуде, қауіпсіздікті жетілдіруге арналған сипаттізім, ол TKIP (temporal key implementation protocol) уақытша хаттамасын қамтиды. WEP үлгілеудің WPA болып табылады.

2.44 **Өткізгішке баламалы құпиялылық;** WEP (Wired Equivalent Privacy): Ағымды ұзындығы 128 бит шифр кілтімен шифрлауды болжайтын криптографиялық хаттама, ол сымсыз ЛВС арналған сипаттізім ішінде анықталған [8].

2.45 **Сымсыз дәлдік;** WiFi (Wireless Fidelity): Сымсыз ЛВС арналған жабдықтарда пайдаланылатын, «WiFi Alliance» фирмасы шығаратын сауда маркасы.

2.46 **Сымсыз ЛВС** (wireless LAN; WLAN)**:** Радиобайланысты пайдаланатын желі. 2,4 ГГц ауқымына сәйкес, 11 Мб/с және 54 Мб/с жылдамдығымен барынша кеңінен пайдаланылатын стандарттар IEEE 802.11b және 802.11g болып табылады.

3 Мақсат

Берілген стандарт қашықтан қол жеткізуді қорғауды ұйымдастыру мәселелерімен жұмыс жасайтын қауіпсіздік қызметінің жұмыскерлері мен желілік әкімгерлер үшін арналған. Онда қашықтан қол жеткізуді қасақана қатерлерден қорғау бойынша барабар шаралар қабылдауда, мүдделі тұлғаларға көмектесу мақсатында қол жеткізудің әртүрлі типтері мен әдістері туралы ақпарат ұсынылған.

Ол сондай-ақ үйден өз кеңсесіне қашықтан немесе саяхат уақытында қол жеткізуді пайдаланғысы келетін пайдаланушыларға көмек көрсете алады.

4 Жалпы шолу

Қашықтан қол жеткізу пайдаланушыға жергілікті компьютерден қашықтағы компьютерге немесе компьютерлік желіге қосылуға және олардың ресурстарын ЛВС тікелей қосылғандағыдай пайдалануға мүмкіндік береді. Бұндай қызмет көрсетулерді Қол жеткізудің Қашықтағы қызметі RAS деп атайды. RAS қашықтан пайдаланушылардың желілер ресурстарына қол жеткізетіндігін есіне салады.

Әдетте RAS мынадай жағдайларда пайдаланылады:

– Тұрақты дербес жұмыс стансаларын біріктіруге арналған (яғни, жекелеген жұмыскерлер үйден қашықтағы пайдаланушылар сияқты жұмыс істей алатындай);

– Мобильді компьютерлерді біріктіруге арналған (яғни, қаланың сыртында немесе іссапарлар кезінде жұмыс жасайтын қызметкерлер құрамын қолдау);

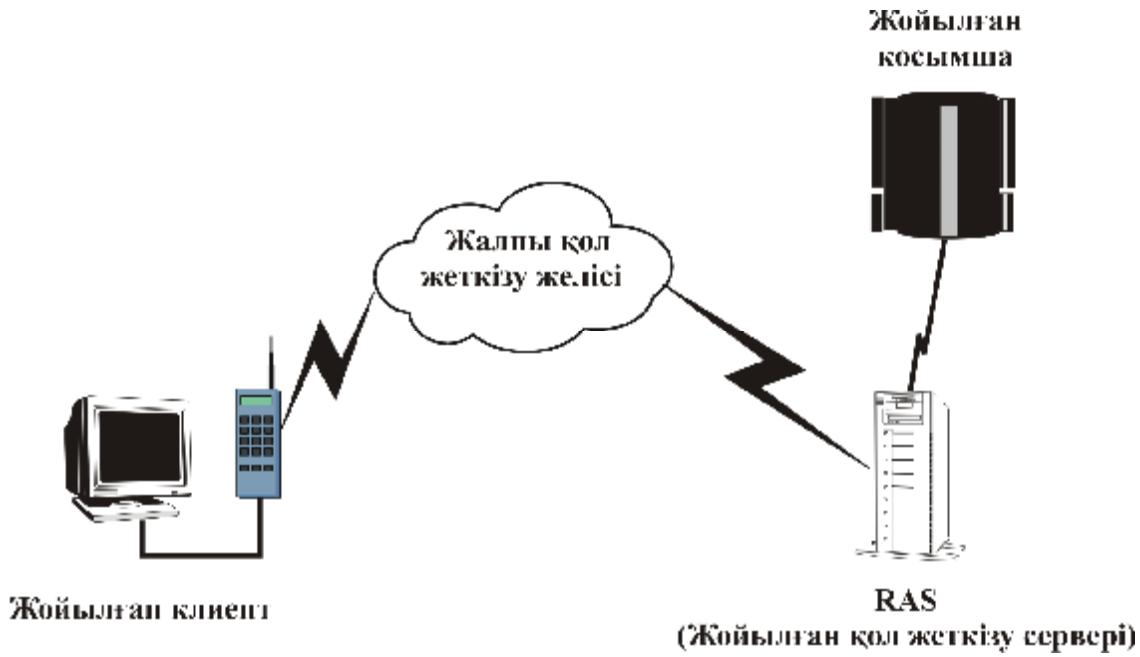
– қашықтағы бірнеше ЛВС біртұтас компьютерлік желіге біріктіруге арналған;

– қашықтағы компьютерлерге қол жеткізуді басқаруды қамтамасыз етуге арналған (яғни, қашықтан техникалық қызмет көрсету үшін).

RAS қашықтан пайдаланушылармен қарапайым байланысу тәсілін мынадай сценарийлер бойынша ұсынады: қашықтан пайдаланушы негізгі желімен байланыс орнатады, мысалы, модемді пайдаланып, телефон желісі арқылы. Бұндай тіке қосылу оның қаншалықты қажет болғандығына байланысты, ұзақ қолданылуы және қажетінше белсендірілетін жалға алынған желі ретінде қарастырылуы мүмкін. Егер DSL немесе басқа барабар технология пайдаланылатын болса, қосылудың тұрақты болуы да мүмкін.

Маңызды: Кәсіпорынға арналған қашықтан қол жеткізу әрқашан қашықтан қол жеткізу сервері арқылы қамтамасыз етілуге тиіс, компьютерлерге тікелей қол жеткізу көптеген қауіптерге кездесіп отыр, сондықтан болғызбау керек. Кәсіпорындар модемдері тек белгілі жерлерде ғана орнатылуы керек.

Қашықтан басқару ресурстары 1-суретте берілген.



1-сурет – Қашықтан басқару ресурстары

RAS қосылуын орнату әдетте 3 құрауышты қажет етеді:

1) RAS қамтамасыз ететін (яғни, RAS бағдарламалық қамтуы орнатылған) және RAS қосылуын қабылдауға дайын корпоративті желінің ішіндегі жергілікті желі құрауышы. Ол RAS сервері немесе қол жеткізу сервері ретінде белгілі.

2) RAS бағдарламалық қамтуы орнатылған және RAS қосылуын инициирлайтын қашықтағы компьютер. Ол RAS клиенті ретінде белгілі. Қашықтатылған клиенттердің жұмыс стансалары немесе мобильді компьютерлері болуы мүмкін.

3) RAS қосылуы орнатылатын коммуникациялық орта. Көптеген жағдайларда, RAS клиенті қосылуды орнату үшін телекоммуникациялық желіні пайдаланады. Мұнда қажет болатын минимум – бұл қосылуды орнатуға арналған телефон желісі және модем.

RAS архитектурасына байланысты, сервер тарапынан әртүрлі қосылу технологиялары пайдаланылуы мүмкін.

RAS клиент – сервер архитектурасы ретінде жүзеге асырылады: RAS клиенті RAS қосылуын корпоративтік желі ресурстарымен, RAS сервері орнатылған компьютер телефонының нөмірін теру жолымен автоматты орнататындай болып пішінделген болуы мүмкін.

Басқаша, пайдаланушы RAS қолмен қозғай алады. Кейбір операциялық жүйелер RAS жүйеге енгеннен кейін дереу қозғауға мүмкіндік жасайды. Клиент жүйесінің кез келген түрдегі компьютер болуы есіңізде болар (ноутбук, PDA (Personal Digital Assistant) немесе смарт-телефон).

Қосылуды орнатқаннан кейін, клиент жүйесі ішіне салынған кейбір қауіпсіздік модульдері болатын түрлі қосымшаларды пайдалана алады.

5 Қауіпсіздік талаптары

Қауіпсіздік көзқарасы тұрғысынан RAS клиенті мен RAS сервері ол уақытта осындай басқарудан тыс коммуникациялық орта ретінде және жауласатын ортада болуы мүмкін, қауіпсіздік саясатының басқаруымен қарастырылады. Қауіпсіздік механизмдері авторластырылмаған субъектілер (жеке тұлғалар немесе процестер) жасай алатын қатерлердің болуына қарамастан құрылады:

- RAS клиентіне қол жеткізуді алу;
- RAS серверіне қол жеткізуді алу;
- RAS серверіне қол жеткізуді тоскауылдау;
- RAS клиенті мен RAS сервері алмасатын ақпаратты қамту;
- Алмасу процесіндегі ақпаратты өзгерту.

Осындай қатерлермен есептесетін қауіпсіздік қызметтері құпиялылық қызметтері, қол жеткізуді басқаруды түпнұсқаландыру қызметтері болып табылады. Сондықтан RAS пайдаланғанда, мынадай қауіпсіздік элементтері қолданылады:

Түпнұсқаландыру: Қашықтан пайдаланушы RAS жүйесімен бірдей сәйкестендірілуге тиіс. Пайдаланушы сәйкестігі жергілікті желімен байланыс орнатылғанда, әр жолы түпнұсқаландыру механизмінің көмегімен орнатылуы керек. Жүйелік қол жеткізудің мағыналы мәтінінде жүйелік қол жеткізуді пайдаланушының сенімді бақылайтындығына (мысалы, қол жеткізу шектеуін белгілі бір уақытта немесе қашықтан қол жеткізу үшін рұқсат етілген нүктелерден ғана қолдану) көз жеткізу үшін, қосымша басқару механизмдері пайдаланылуы қажет.

Сапасы мен технологиясы бойынша ерекшеленетін пайдаланушылар мен процестерді түпнұсқаландырудың түрлі әдістері қолданылады. Барынша қолданылатын, бірақ сонымен қатар, барынша осалдау жері құпия белгілерді пайдалану болып табылады.

Қол жеткізуді басқару: Қашықтан пайдаланушыны түпнұсқаландырғанда, қашықтан қол жеткізу сервері пайдаланушының желімен өзара әрекетін шектеуге қабілетті болуға тиіс. Бұндайда авторластыру және авторластырылған әкімгерлер жергілікті желі ресурстары үшін анықтаған шектеулер және қашықтан пайдаланушылар үшін де, қашықтан пайдаланушыларға арналған кез келген ерекше шектеулерге қосымша әрекет етуі үшін қажет етіледі (мысалы, күннің белгілі бір уақытында қол жеткізу, бір пайдаланушыға арналған бір реттік қосылу).

Байланыс қауіпсіздігі: Жергілікті ресурстарға қол жеткізу қашықтан жүзеге асырылса, пайдаланушының деректері орнатылған RAS қосылулары арқылы берілуге тиіс. Жалпы жағдайда, байланысты қорғауға (*құпиялылық, бүтіндік, түпнұсқалылық*) қатысты жергілікті желіде қолданылатын қауіпсіздік талаптары сонымен қатар,

RAS қосылуы арқылы берілетін деректерге қолданылады.

Дегенмен, RAS кезіндегі байланысты қорғау көптеген техникалық байланыс құралдары мен жергілікті желі операторының бақылауында болады деп есептелетін хаттамалар пайдаланылып, жүзеге асырылуы мүмкін болғандықтан, әсіресе қиын.

Қол жеткізу мүмкіндігі: Қашықтан қол жеткізу жұмыс процесінің негізі болып табылғанда, RAS қолжетімділігі ерекше маңызды. Өндірістік процестердің үздіксіз ағыны толық қосылудың болмауынан немесе деректердің берілу жылдамдығының жетіспеуінен бұзылуы мүмкін.

Мұндай қатерлер баламалы немесе артық қосылуларды пайдалану жолымен белгілі деңгейге дейін азайтылуы мүмкін. Бұл, Интернет, ерекше әрбір қосылу үшін деректердің берілу жылдамдығын қажетті қамтамасыз ету жылдамдығын қамтамасыз ету кепілдігі болмаған жалпы жағдайда, байланыс ортасы ретінде пайдаланылатын жағдайларға жатады.

RAS жүйесінің клиент/сервер архитектурасы клиент те, сервер де байланыс ортасының типінен және пайдалану тәсілінен болатын ерекше қатерлердің алдында қарсы тұра алады деп тұспалдайды.

RAS клиенттерінің тұрақты болуы міндетті емес (яғни, үстел ДК), олар мобильді құралдар болуы мүмкін (мысалы, ноутбук). Дегенмен, клиенттің орналасқан орны әдетте ЛВС операторының бақылауында болмайды, клиент мобильді болғанда, ортаның қауіпсіз еместігін және арнайы қауіп-қатерлерге, жекелей алғанда, ұрлық немесе бүлдіру сияқты физикалық қауіп-қатерлерге ұшырауы мүмкін екендігін ескеру керек.

RAS серверлері әдетте қашықтан пайдаланушылар қосылатын ЛВС бөлігі болып табылады. Олар ЛВС операторының бақылауында болады және жергілікті қолданылатын қауіпсіздік шарттарымен қамтамасыз етілуі қажет. RAS серверінің негізгі міндеті тек авторластырылған пайдаланушылардың ЛВС қосылу дұрыстығын тексеру болып табылатындықтан, демек, RAS сервері ЛВС авторластырылмаған қол жеткізуді алуға бағытталған шабуылдар сәтсіздігін қамтамасыз етуге тиіс.

6 Қашықтан қол жеткізу қосылуларының түрлері

Клиент пен қашықтағы ЛВС компьютерлері арасында қосылуларды орнатудың әртүрлі тәсілдері бар:

– Қол жеткізу серверіне дейін тікелей дозвон, яғни, серверге модемнің көмегімен әдеттегі жалғастыратын байланыс телефоны желісі бойынша қосылу;

– Интернет (ISP) қызметінің провайдерінің серверіне әдеттегі жалғастыратын телефондық байланыс желісі модемнің көмегімен қосылу және бойынша Интернет арқылы қашықтағы жергілікті желіге қол жеткізу;

– Тұрақты қосылу құралдарының басқа желімен қол жеткізуі.

2-сурет қашықтан қосылулардың осы түрлерін көрсетеді: мобильдік пайдаланушы 2 ISP арқылы ЛВС қосылады, Интернет алынған деректер Интернет пен жергілікті желі арасындағы алмасуды бақылайтын желіаралық қалқа (firewall) арқылы өтеді. Мобильдік пайдаланушы 1 сымсыз ЛВС пайдаланушысы бола алады; онда RAS Қол жеткізу Нүктесі болып аталады. Қол жеткізудің осы сервері желіаралық қалқамен басқарылады.

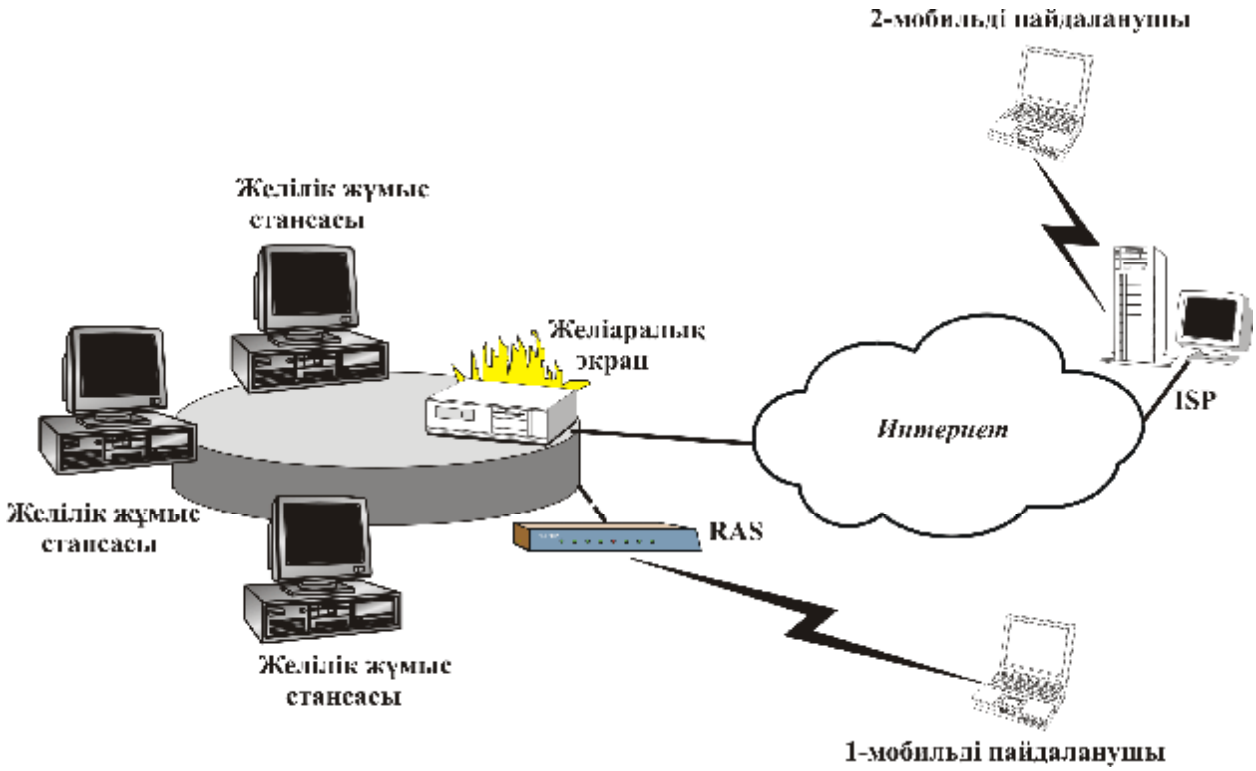
Ескертпе – Мобильдік пайдаланушылар өткізетін кең жолағы немесе сымсыз қосылулары бар жалға алған жалғастыратын телефон желісі арқылы қосылуды пайдалана алады.

«WLAN hot spot» деп аталатын жағдай (жалпы қолжетімді сымсыз ЛВС) жергілікті модемді пайдаланудың орнына, сымсыз ЛВС қол жеткізу нүктесінен жүзеге асыратын мобильдік 2-пайдаланушының көмегімен сипатталады. Бұл Интернетке жалпы қол жеткізудің сымсыз ЛВС және ISP қол жеткізу нүктесі арқылы қамтамасыз етілетінін

білдіреді.

Клиент ISP қосылу үшін пайдаланатын әртүрлі әдістер қолданылады. Клиент сымды және сымсыз технологияларды пайдалана алады. Пайдаланылатын әдістерге байланысты, қосымша қатерлер болуы мүмкін, яғни сымсыз ЛВС құпиялылықты сақтауға арналған арнайы қауіпсіздік шаралары қолданылуын талап етеді.

Бұл әдістер назарға алынуы керек ерекше тәсілдер ұсынады. Мысалы, әдеттегі жалғастыратын телефон желісі бойынша, модемнің көмегімен серверге қосылу жиынтық нөмірін білетін авторластырылған пайдаланушылар ғана қашықтан желіге қосыла алатындығына көз жеткізу үшін арналады. Алайда, дозвонның қолжетімді нөмірлерін (жүйелі іріктеу жолымен) сканерлейтін құралдар хакерлерге келетін қоңырауларды күтетін қолданыстағы белсенді модемдерді сәйкестеуге көмектеседі. Интернет қызметінің провайдерлері қашықтан пайдаланушыға арналған артықшылықты қамтамасыз етеді. Пайдаланушы қашықтағы ЛВС қосылу үшін, жергілікті ISP арқылы қосылуды пайдалана алады. Дегенмен, қосылудың осындай әдісі барынша қымбат сервермен оны арнайы пішіндеуді қажет етуі мүмкін.



2-сурет – Қашықтан қол жеткізу түрлері

7 Қашықтан қол жеткізуде қосылуларды орнату әдістері

7.1 Жалпы ережелер

Қашықтан қол жеткізуді қамтамасыз ету үшін, негізгі ұстанымдарды білу қажет. Кәсіпорын қандай жүйелер мен қандай қосымшалардың жеке пайдаланушы үшін сыртқы әлемнен қол жеткізілетін анықтауға тиіс. Қашықтан қол жеткізу түрі қашықтан пайдаланылатын қызметтермен анықталуы керек.

7.2 Жалғастырғыш қызметтерге қол жеткізу

7.2.1 Байланыстың жалпы қорғанысы

Барынша жалпылама қолданылуға ұсынылатын қол жеткізу кәсіпорын ішіндегі жалғастырғыш қызметтерге қол жеткізу болып табылады, яғни пайдаланушының өз поштасына, FTP серверіне немесе Web-серверге қол жеткізуі. D қосымшасында пошталық сервердің қауіпсіз жұмысын ұйымдастыруға арналған әрекеттер тізбесі берілген, ал Е қосымшасы Web-серверді қауіпсіз орнатуға және басқаруға көмектеседі.

Сервер мен клиент арасындағы коммуникацияларды қорғаудың мыналар сияқты түпнұсқалылықты, құпиялылық пен бүтіндікті қамтамасыз ететін әртүрлі жолдары болады:

a) SSL (қауіпсіз сокеттер деңгейі) қатысатын тараптарды (клиент пен серверді түпнұсқаландыруды) түпнұсқаландыру және осы тараптар алмасатын ақпаратты шифрлау әдісін анықтайды. SSL барлық операцияларға сүйенетін пошталар сияқты, Интернет-браузер және Web-сервер қолдайды. IETF клиент/сервер байланысын қорғау үшін, SSL және Интернет [22] стандартына негізделген көліктік деңгейді қорғау (Transport Layer Security, TLS) хаттамасын әзірледі.

b) IPsec (қауіпсіздікті қамтамасыз етуге арналған Интернет хаттамасы) берілетін ақпаратты қорғау үшін қажетті, тараптарды түпнұсқаландыру жолдарын ұсынады. IPsec сондай-ақ кілтпен басқару қызметтерін ұсынады (сондай-ақ [24] қараңыз).

c) SSH (қауіпсіздік қабықшасы) − бұл желіге қауіпсіз қашықтан кіруге және қауіпті желідегі жұмыс кезіндегі басқа құпия желілік қызмет көрсетулерге арналған хаттама. Ол қашықтан пайдаланушыны сәтті түпнұсқаландырудан соң, қауіпсіз жалғануды орнатады және бұйрықтар жиынтығы мен қызмет көрсетулерді қамтамасыз етеді (мысалы, файлдардың қауіпсіз берілуі).

Бұл әдістер қауіпсіз түпнұсқаландыруды, құпиялылық пен бүтіндеу қызметтерін қамтамасыз етеді және коммуникациялық бағдарламалық қамтуға қосымша пайдаланылуы қажет. SSL - әдетте қолжетімді Internet браузерлердің бөлігі болғандықтан, Web-поштаға қол жеткізу пайдаланушының пошталық есеп жазбасына қол жеткізу сәтіне дейін SSL байланысын орнату жолымен жеңіл қорғалуы мүмкін.

Бұл әдістер арасындағы негізгі айырмашылық SSL/TLS және IPsec әдетте желі қауіпсіздігі қызметі болып табылып, байланыстың келесі функциялары ретінде ұсынылатындығында, ал SSH қауіпсіздік қосымшасы болып табылады.

Бұл әдістер FTP-клиентті FTP-сервермен жалғау үшін, осы серверде сақталатын деректерге қол жеткізуді жүзеге асыруға мүмкіндік бере отырып қолданылатын болып табылады.

Ескертпе – Көптеген Интернет хаттамалары, мысалы терминалдық қол жеткізу мүмкіндіктерін немесе файлдардың берілуіне мүмкіндік беретін FTP қамтамасыз ететін Telnet, әдетте қарапайым мәтін сияқты құпия ақпаратты жібере отырып, түпнұсқаландырудың әлсіз механизмдерін қолдайды. Осындай хаттамаларды SSH, SSL/TLS немесе IPsec сияқты қауіпсіздік хаттамалары арқылы туннельдеу құпиялылықты ғана қамтамасыз етпей, сонымен қатар, түпнұсқаландыру процесін елеулі түрде жақсартады.

Көптеген Web-серверлер пайдаланушыны түпнұсқаландыруды қамтамасыз ету үшін, бірақ керісінше емес, пайдаланушы серверден сертификатты растауды қажет еткен кезде ғана SSL/TLS пайдаланатыны есіңізде болсын.

7.2.2 Электронды поштаны қорғау

Электронды пошта мәліметтердің құпиялылығын қамтамасыз етпейтін қызмет болып табылғанымен, серверге қол жеткізу үшін, кейбір алдын ала әрекеттерді сырттан орындау қажет. Жалпы қолданылатын тәсілмен пошталық серверге қол жеткізуді қамтамасыз ету, пайдаланушыларға өздерінің пошталық жазбаларына қол жеткізуді алуға

мүмкіндік беретін, пошталық есеп жазбаларына арналған Web-интерфейс болып табылады. Бұл әдіс браузері бар компьютердің болуын қажет етеді, яғни, кез келген қолжетімді компьютер пайдаланылуы мүмкін. Басқа жағынан, бұл әдіс пайдаланушыларға өз пошталарын толтыра салуға және жалғануды (off-line) орнатпай жауап беруге мүмкіндік бермейді.

Басқа тәсілдер өздерін пайдаланушылардың стандарттық пошталық клиенттер сияқты пайдалануына мүмкіндік береді, бірақ олар пошталық хаттамалардың шоғырлануынан, жеткілікті құпиялылықты қамтамасыз етпейді. Жалпы жағдайда, пошталық клиент пайдалану деректерін бос жолдарға толтырып, өздігінен түпнұсқалану жолымен пошталық серверге (мысалы, барлық кіріс пошталық есеп жазбаларды басқарудың қарапайым бағдарламасын пайдаланады) қол жеткізеді. Қол жеткізудің екі пошталық хаттамасы (POP3 және IMAP4) кіретін поштаға өздерін өңдейтін мынадай тәсілмен ерекшеленеді:

– POP3 барлық жаңа қолжетімді пошталық мәліметтерді толтыра салады және пайдаланушы олармен бір жердің шеңберінде жұмыс жасай алады;

– IMAP4 пайдаланушыға хаттардың тек тақырыптарын ғана толтыра салуға, содан соң өз компьютеріне қандай мәліметті толтыра салуға болатынын шешуге мүмкіндік береді.

Бұл хаттамалар өздерінде қорғау механизмдерін жеткілікті деңгейде қамтамасыз етпейтіндіктен, қатаң түпнұсқаландыру мен берілу құпиялылығы, мысалы, SSL, SSH қолданумен қосымша қамтамасыз етілуге тиіс.

Ескертпе – Сіз сондай-ақ поштаның ішіндегісін қорғай аласыз (жіберушінің мекенжайы, алушының мекенжайы мен хабарлар тақырыбының болмауына қарамастан). Негізгі сипаттайтын екі құжат − бұл құпиялылық, бүтіндік, түпнұсқалылық және авторлықтан бас тарту мүмкіндігін болдырмау қызметтерін қамтамасыз ететін PGP және S/MIME. Олардың екеуі де көптеген пошталық клиент бағдарламаларында ықпалдасуы мүмкін. Бірақ олар жіберуші мен алушының мекенжайлары ашық мәтінмен берілетіндіктен, кестені талдаудан қорғауды ұсынбайды.

Қашықтан пайдаланушыларға қолжетімді пошталық сервер тыйым салынған (TCA) желі аймағында орналастырылуға тиіс. TCA міндеті сыртқы желіні ішкі желіден желідегі әрбір компьютерден тікелей қол жеткізуге болатын компьютерлерді оқшаулау көмегімен бөлектеу болып табылады. Пошталық серверді TCA орналастыру оның сыртқы желідегі сияқты, ішкі желіден де қолжетімді екенін білдіреді. Ішкі желі үшін қатер тудыруды болдырмас үшін, мынадай шараларды орындау қажет:

Сыртқы желідегі компьютер мен TCA арқылы сыртқы желідегі компьютер арасындағы қосуды орнату мүмкін еместігі қарастырылуға тиіс. Бұған тиісті қондырғылар мен аралық компьютерлерді немесе олардың осындай бөлуді қамтамасыз етуге арналған амалдарын пішіндеумен қол жеткізілуі мүмкін.

Қолайлы пішіндеу мынадай мәселелерді қарастыруды қажет етеді:

– пошталық сервердің оны шабуылға арналған аралық машинаны пайдалануды болдырмас үшін, тек арнайы қосымшасы мен барынша азайтылған операциялық жүйесі болуы керек;

– сыртқы желіден қол жеткізу тек қатаң түрде анықталған қосымшаларға ғана рұқсат етілуі керек (анықталған IP мекенжайымен және порт нөмірімен);

– ішкі желіден қол жеткізу, сонымен қатар, анықталған мекенжайлармен және деректемелер порттарымен (қол жеткізуге рұқсат етілген ішкі желідегі компьютерлерді), сондай-ақ тағайындау мекенжайларымен шектелген болуға тиіс. Осылайша, ақпарат ағынының бағыты да шектелуі керек. Бұған маршруттауыштарды немесе желіаралық қалқаларды пайдаланып қол жеткізуге болады.

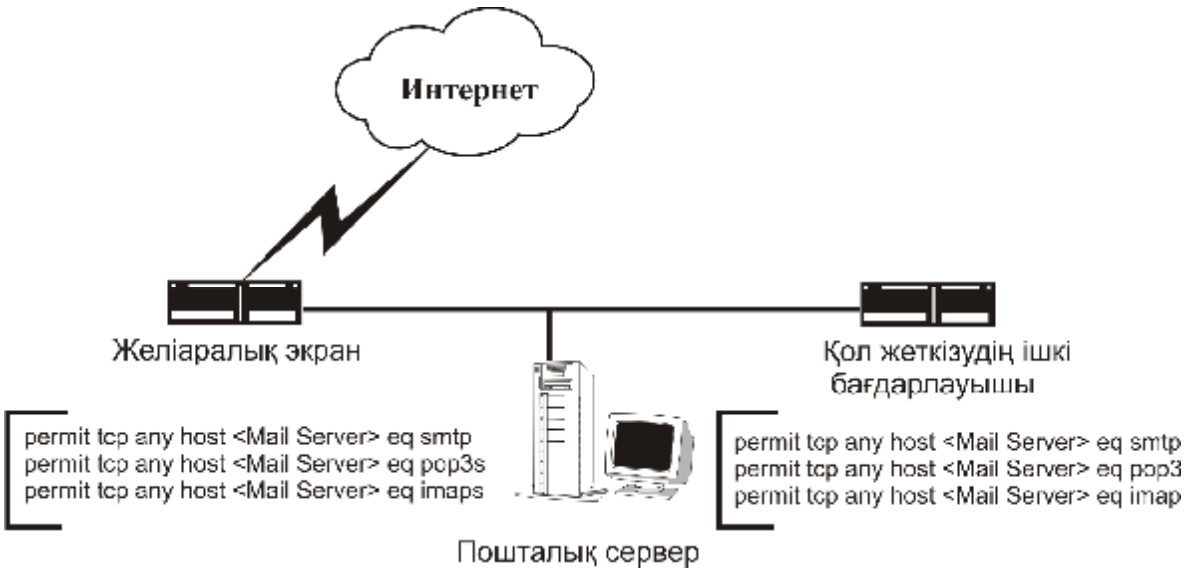
Web-серверлер сияқты басқа да коммуникациялық серверлер, сондай-ақ TCA ішінде орналастырылып, тиісінше қорғалады. 1-кестеде пошталық сервер

ТСА орналастырылғанда, пайдаланылуы мүмкін порттар нөмірлері мен хаттамалар мысалдары берілген.

1-кесте - Электрондық пошта және порттардың тиісті нөмірлері

Нөмірі	Атауы	Сипаты
22	ssh	Қауіпсіз тіркеу қабығы
25	smtp	Стандартты STMP порты TLS/SSL бірге
465	dmtps	TLS/SSL үстіндегі SMTP
143	imap	Стандартты IMAP
993	imaps	TLS/SSL үстіндегі IMAP
110	pop3	Стандартты POP3
995	pop3s	TLS/SSL үстіндегі POP3

3-кесте Интернеттің жергілікті маршруттауыштары мен ішкі желілері үшін қажетті пішімдердің айырмашылығын көрсетеді. Бұндай жағдайда пошталық серверге сырттан қол жеткізуге поштаны жіберу үшін, қарапайым SMTP пайдаланылуы мүмкін болған уақытта, TLS/SSL үстіндегі IMAP және TLS/SSL үстіндегі POP хаттамасы бойынша ғана рұқсат етіледі. Ішкі желіден қол жеткізу TLS/SSL көмегімен қосымша қорғаусыз IMAP немесе POP пайдалана отырып рұқсат етілген. Бұйрықтар шекаралық желіаралық қалқа мен ішкі маршруттауыштарға арналған қол жеткізудің қажет етілген бұйрықтар тізбесін сипаттайтын, жалған-бұйыру тілімен жазылған. Басқа барлық порттарға осы порттарға және хаттамаларға байланысты осалдықтарды болдырмас үшін, тыйым салынған.



3-кесте – Пошталық серверге ТСА шегінде қол жеткізу

Қосымша қауіпсіздік шаралары, сондай-ақ SMTP пошталық серверінің дұрыс пайдаланылмауын болдырмас үшін қолданылуы мүмкін (мысалы, сұралмаған электронды поштаның қызметін болдырмас үшін, SMTP қосылуын шектеу).

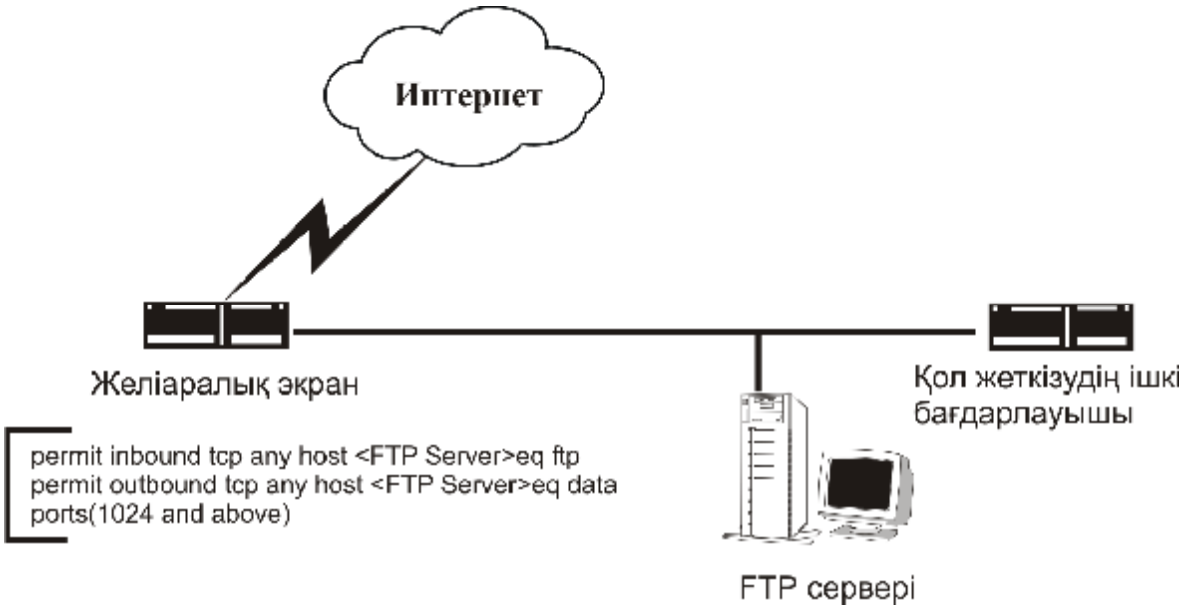
7.2.3 FTP бойынша қосуды қорғау

FTP (Файлдардың берілу хаттамасы) − бұл сервердің ТСА ішінде орналасуы мүмкін басқа қызмет. FTP екі жұмыс режімін анықтайды:

– PORT режімі (Әдеттегі немесе Активті режім сияқты да белгілі);
– PASV режімі (Пассивті режім сияқты да белгілі).

Бұл режімдер деректер арнасын орнату шарасымен ерекшеленеді: PASV режімінде бұйрықтар арнасы мен деректердің берілу арнасын FTP серверіне жүгінетін FTP клиенті орнатады; PORT режімінде - FTP клиенті бұйрықтар арнасын ашады, ал FTP сервері клиент сұранысы расталғаннан кейін, деректердің берілу арнасын ашады (толық жағдайын С қосымшасынан қараңыз). FTP пайдалануда бұйрықтар арнасын ұйымдастыруға арналған 21 порт анықталған, ал деректер арнасының порты әдетте 1024-порттан басталып, 5000-порттан аяқталатын өрісте динамикалық түрде тағайындалады.

Түптеп келгенде, PORT режімі қашықтағы клиенттер үшін FTP қызметін қамтамасыз етуде, қапшықтарды сүзгілеуге арналған желіаралық қалқаларды барынша қауіпсіз орнатуға мүмкіндік береді. TCP 21 порты ғана клиент инициирлайтын бұйрықтар арнасын орнататын қабылдау үшін ашық болуға тиіс. Келесі ұйымдастырылған деректер арнасы берілім үшін ашылады. 4-сурет ТСА, FTP сервері болатын ТСА сүзгілеуін реттеулерді көрсетеді.



4-сурет – FTP серверіне ТСА шегінде қол жеткізу

Керісінше, PASV режімін пайдаланатын FTP серверін қолдану, қарапайым желіаралық қалқалар үшін кіретін жалғануларға арналған 1024 бастап, порттардың кең өрісінің ашылуын қажет етеді. Мұндай қондырғылар желіаралық қорғауда басты қатерлерді қалдырған болар еді.

Өкінішке орай, PORT режімі деректер арнасының бөлек орнатылғандығынан, желіаралық қорғау арқылы желілік мекенжайды таратумен қатар амалдармен пайдаланыла алмайды. PASV режімі бұл шектеуді игереді, өйткені барлық арналар клиенттік жүйемен инициирланады. Тұспалданған қатерлер порттардың кең өрісі ашылған кезде желіаралық қорғаудың барынша күрделі әдістерін жүзеге асыру жолымен

төмендетілуі мүмкін: желіаралық қалқалар уақытша талап бойынша, қабылдауға арналған кіріс порттардың кең өрісінің ашылу қажетсіз, FTP арналған PASV режімін қамтамасыз ету үшін, кіріс порттардың ашылуына мүмкіндік беріп, ағымдағы жағдайдың толық бақылануын қамтамасыз етеді. Сол нәтиженің нақ өзі желіаралық қалқада арнайы прокси-құрауышты пайдалану кезінде алынуы мүмкін.

Қашықтағы клиент ұсынатын FTP мүмкіндіктерін қарастырғанда, FTP хаттамасының өзі тек базалық қауіпсіздік шараларын ғана ұсынатынын білу маңызды. Құпиялылық ұстап тұрылмайды, ал түпнұсқаландыру қызметтері тек базалық деңгейде ғана ұсынылады. Мысал ретінде, құпия белгілер шабуылдар ұйымдастыруға мүмкіндік беретін қарапайым мәтінмен беріледі.

Сондықтан FTP қызметтері, қажет болғанда, қауіпсіз туннельдеу хаттамаларының төмен жатқан деңгейі (мысалы TLS/SSL) немесе Secure FTP немесе SCP (қауіпсіз көшірмелеу) сияқты файлдарды беруге арналған жетілдірілген қосымшалар амалдарымен іске асырылуға тиіс, екеуі де SSH хаттамасында негізделген. Екі нұсқа да қатаң түпнұсқаландыру мен қызмет көрсетулер құпиялылығын қамтамасыз етуді іске асыруға мүмкіндік береді.

7.3 ЛВС ресурстарына қол жеткізу

Бұндай қол жеткізу компьютерлер мен жүйенің белгілі бір пішімінің арнайы инсталляциясын қажет етеді. Ішкі желі ресурстарына қол жеткізуді орнатқысы келетін қашықтан пайдаланушының осы желіге қатер тудыратындығынан, қашықтан қол жеткізу мынадай жағдайларды қанағаттандыруға тиіс:

Түпнұсқаландыру: қатаң түпнұсқаландыру механизмі немесе қос әсерлі түпнұсқаландыру қашықтан пайдаланушының сәйкестігі расталғанын куәландыруға тиіс.

Жүйеге қол жеткізу құқығын ұсыну (Авторластыру): сәтті түпнұсқаландырудан кейін, қашықтан пайдаланушы оған ұсынылатын, өз жұмысын орындауға мүмкіндік беретін құқыққа ие болады. Осылайша, пайдаланушы қашықтан пайдаланушының белгілі бір рөлін орындайды.

Қол жеткізуді басқару: қашықтан пайдаланушы ресурстарға немесе деректерге қол жеткізу ұсынылғанға дейін, оған ұсынылатын құқықтарға тексеріледі.

Құпиялылық, түпнұсқалық және бүтіндік: пайдаланылатын деректерге немесе ресурстарға байланысты, ұсынылатын құпиялылық, түпнұсқалық және бүтіндік қызметтерінің көмегімен байланыс қауіпсіздігі орнатылған болуға тиіс.

Осы талаптар тиісті түпнұсқаландыру механизмдерін қоса алғанда, виртуал жеке желілерге арналған қауіпсіз туннельдеу хаттамаларын пайдалану кезінде орындалатын болады.

Қашықтан пайдаланушыларға арналған түпнұсқаландырудың тиісті механизмдері, мысалы, өзінің жеке сәйкестендіру нөмірін (Personal Identification Number, PIN) енгізетін пайдаланушының қол жеткізуге ұмтылуын өткізгенде, әр жолы бірыңғай құпия белгіні қамтамасыз ететін бір реттік құпия белгі токендері (рәміздер жиынтығы) болып табылады. Бұндай токендер пайдаланушының токенге ие болғанда және сәйкесті PIN білуі керек болғанда, қос әсерлі түпнұсқаландыруды қамтамасыз етеді.

Жүйеге қол жеткізу құқығын беру (Авторластыру) қашықтан пайдаланушылар топтары тағайындауы мүмкін ерекше рөлдерді белгілейді. Топқа олар қашықтықтан орындайтын тапсырмаларды орындау үшін ғана қажетті құқықтар бөлінуге тиіс. Қашықтан пайдаланушыларға арналған қол жеткізуді шектеудің мұндай тәсілі оңай іске асырылуы мүмкін.

Қол жеткізуді басқару пайдаланылатын операциялық жүйелер ұсынатын

механизмдерді қолдайтын саясаттың көмегімен іске асырылуы мүмкін. Мысалы, пайдаланушының есеп жазбасының саясаты талап етілетін құқықтар мен шектеулерді анықтай алады. Операциялық жүйелер, сондай-ақ қашықтан пайдаланушылар үшін арнайы әзірленген топтық саясатты ұсына алады.

Хаттамалардың барынша жалпы қолданылатын жиынтығы қосылатын пайдаланушыны (RADIUS) қашықтан түпнұсқаландыру қызметі ұсынатын хаттама болып табылады. Бұл бастапқыда қашықтан қол жеткізуді жалғау үшін ғана дайындалған хаттамалар, қол жеткізуге арналған түпнұсқаландыруды, авторластыру мен есептік жазбаны желіге орталықтандыру мүмкіндігін береді, оларды VPN және түпнұсқаландырудың қатаң механизмдері қолдайды. Хаттамалар мынадай түрде жұмыс істейді:

RADIUS қызметінің клиенті (әдетте модемдік байланыс сервері түріндегі қол жеткізу сервері, VPN сервері немесе сымсыз қол жеткізу нүктесі) пайдаланушы мандатын және RADIUS хабарламасы үлгісіндегі қосылу параметрлері туралы ақпаратты RADIUS серверіне салып жібереді. RADIUS сервері түпнұсқалықты растайды және RADIUS клиентінің сұранысына рұқсат етеді және RADIUS жауап хабарламасын кері салып жібереді. RADIUS клиенттері сондай-ақ RADIUS серверіне есептік жазбалар туралы RADIUS хабарламасын салып жібереді. Қосымша, RADIUS стандарттары RADIUS прокси-қызметінің пайдаланылуын қолдайды. RADIUS прокси-қызметі − бұл мүмкін басқа RADIUS прокси-қызметтері арқылы, RADIUS клиенттері мен RADIUS серверлері арасында RADIUS хабарламасын жіберетін компьютер. RADIUS хабарламалары қол жеткізуді іске асыруға ұмтылатын клиент пен әрі қол жеткізу сервері арасында ешқашан жіберілмейді.

RADIUS хабарламалары пайдаланушы датаграммаларының хаттамасы (UDP) ретінде жолданады; UDP 1812 порты RADIUS түпнұсқаландыру хабарламалары үшін пайдаланылады, ал UDP 1813 порты RADIUS есептік жазбаларының хабарламалары үшін пайдаланылады. Тек бір RADIUS хабарламасы ғана UDP дестесіне пайдалы ақпарат ретінде қосылуы мүмкін.

[30] ұсынымы RADIUS хабарламаларының мынадай түрлерін анықтайды:

– **Қол жеткізу сұранысы.** Желіге қол жеткізу кезіндегі түпнұсқаландыру мен авторластыруды сұрау үшін RADIUS клиенті жібереді;

– **Қол жеткізуді қабылдау.** RADIUS сервері Қол жеткізу Сұранысының хабарламасына жауап ретінде жібереді. Мұндай хабарлама RADIUS клиентін қосылуға әрекет расталғанын және рұқсат берілгенін ақпараттандырады;

– **Қол жеткізудің ауытқуы.** RADIUS сервері қол жеткізу сұранысының хабарламасына жауап ретінде жібереді. Бұл хабарлама RADIUS клиентіне қосылу әрекетінің ауытқығанын хабарлайды. RADIUS сервері бұл хабарламаны не мандат түпнұсқалық болмағанда немесе қосылу әрекетіне рұқсат берілмегенде жібереді;

– **Қол жеткізуді шақыру.** RADIUS сервері Қол жеткізу Сұранысының хабарламасына жауап ретінде жібереді. Бұл хабарлама жауап күтетін RADIUS клиентінің шақыруы болып табылады.

В қосымшасында RADIUS тарату немесе Microsoft Windows 2000 операциялық жүйесінің ішіне орналастыру бойынша ұсынымдар беріледі.

7.4 Техникалық қызмет көрсетуге арналған қол жеткізу

Қашықтан қол жеткізудің бұл түрін жүйені қашықтықтан басқару қажет болғанда, жалғанатын жүйе әкімгері ұсынады. Әдетте, пайдаланушылардың бұл тобының жүйеге қол жеткізуге жоғары құқықтары болғандықтан, қол жеткізу барынша қауіпсіз түрде

орнатылуға тиіс. Сонымен қатар, қашықтықтан жүргізілетін кез келген әрекет, жүйелік қызметтерді жүйелік басқару жүргізілген кезге қарағанда, кейінірек тексерілуге тиіс.

Сондықтан қол жеткізуді қашықтан басқару қажет белгілі бір компьютерде ғана қамтамасыз ету қажет.

Бұндай жағдайда мынадай шаралар қажет етіледі:

– Қол жеткізу белгілі бір машинадағы белгілі бір есептік жазбамен ғана қамтамасыз етілуге тиіс;

– Қашықтан пайдаланушы мен әкімгер бақылауы қажет машина арасындағы байланыс SSH сияқты құралдар пайдаланылып қорғалуға тиіс;

– Пайдаланушыны түпнұсқаландыру түпнұсқаландырудың қатаң механизмдерін пайдаланумен бірге өткізілуге тиіс;

– Жүйені қашықтан басқаруға басқаруға қол жеткізуді алатын әрбір пайдаланушы қажетті шаралар мен әдістемелерді үйренуі керек;

– Әрбір әрекет тіркелуге тиіс;

– Тіркеу қашықтан басқару орындалған соң немесе техникалық қызмет көрсету үшін бөлінген уақыттың артуы жағдайындағы алғашқы мүмкіндік кезінде дереу тексерілуге тиіс.

Кері шақыру механизмі (үстеме қорғау шараларын пайдалануды қажет етеді, сондай-ақ 8.2 қараңыз) қосымша болып табылады. Осы талаптарды қолдану қашықтан қол жеткізудің атаулы түрінде болатын қатерлерді шектейді.

8 Таңдау және пішіндеу бойынша ұсынымдар

8.1 Жалпы ережелер

Осы бөлімде белгілі қауіптерге қарсы әрекет ету үшін қажет етілетін шаралар талқыланады. Әрбір ұсынылатын шара толық түсіндірілетін болады, жақтаушылар мен қарсылардың дәлелдемелері берілетін болады. Баяндау құрылымы мынадай, RAS клиентінің салалары, RAS серверлері мен RAS коммуникациялары жеке қарастырылатын болады. бірлескен шаралар соңында талқыланатын болады.

Біз егер RAS клиентіне қаншалықты шабуыл жасалса, онда RAS сервері де автоматты түрде қауіпке ұшырайтындықтан, клиент пен сервер қатерін толығымен бөлек қарастырмаймыз. Бұдан басқа, мысалы, операциялық Windows жүйесінде әрбір RAS клиенті RAS сервері сияқты жұмыс істейтіндіктен, RAS серверіне төнген қауіптің RAS клиентіне де қауіпті екенін ескеру қажет.

8.2 RAS клиентін қорғау

8.2.1 Тұрақты RAS клиенті

Тұрақты клиент алдымен физикалық қорғалуға тиіс, яғни, осындай қол жеткізу рұқсат етілген тұлғалардың ғана қол жеткізуі болатын бөлмеде болуға тиіс. Бұны үйінде қашықтан кеңсесінде жұмыс жасайтын тұлғалар қолдануы мүмкін.

Тұрақты клиент телефондық модемді, кабельдік модемді немесе DSL қосылуды пайдаланып, RAS серверімен қосыла алады. Екінші және үшінші қосылу түрі Интернетпен тұрақты қосылуды қамтамасыз ететін, жоғары жылдамдықты қосылуларды қамтамасыз етуге арналған қосымша шараларды қажет етеді. Инсталляция мен компьютерге сырттан қосылатын қол жеткізуді шектейтін, «дербес желіаралық қалқа» деп аталатын дұрыс пішін қарапайым қорғау тәсілі болып табылады.

8.2.2 Барлық RAS клиенттері

Барлық RAS клиенттері үшін компьютерді дұрыс пайдаланбауды және қауіпсіз қашықтан қосылуды қамтамасыз етуді болдырмас үшін қолданылатын бірнеше қауіпсіздік деңгейлері бар.

Бірінші орнатылған тосқауыл компьютердің өзінің аппараттық құралдары болып табылады. Компьютерді қорғаудың қарапайым тәсілі және оны дұрыс пайдаланбауды болдырмау, жүйені жүктегенге дейін пайдаланушыны сәйкестендіруді өткізетін жүктеме кезінде құпия белгіні орнату болып табылады. Бұл тосқауыл әлеуетті шабуылшылар үшін бірінші кедергі болып табылады, бірақ ол жеткілікті қорғауды қамтамасыз етпейді.

Екінші кедергі операциялық жүйе болып табылады. Шағын компьютерлер мен жұмыс стансалары үшін пайдаланушыны сәйкестендіру мен түпнұсқаландыруды қамтамасыз ететін операциялық жүйе пайдаланылуға тиіс. Мұндай қасиет қолданыстағы жүйелердің көбінде болады. Пайдаланылатын есептік жазба пайдаланушының әдеттегі есептік жазбасы болуы керек, бірақ әкімгердің есептік жазбасы емес, себебі бұл есептік жазбалар көптеген артықшылықтар береді және сондықтан компьютерді басқару үшін ғана пайдаланылуға тиіс. Сонымен қатар, құпия белгінің[1] сәйкесті сапасы міндетті түрде қамтамасыз етілуі керек екенін ескеру керек.

Егер компьютерде барлық компания мүддесін білдіретін ақпарат сақталса, онда қосымша шаралар қарастырылуға тиіс.

Операциялық жүйе үшін типтік пішімдеуге қарағанда, көбірек қауіпсіздік қамтамасыз етілуі керек. Бұл операциялық жүйенің керек емес құрауыштарының бәрі жойылатынын, ал қажетті қосымшалардың ғана инсталданғандығын білдіреді. Сонымен бірге, нақты жүйесі үшін ғана қажетті қызметтерге рұқсат етілетін желі пішімдеулері сияқты ерекшеліктермен шектеледі.

Смарт-карталарды, токен-карталарды немесе биометрикалық[2] механизмдерді пайдалану жолымен қатаң түпнұсқаландыруға қол жеткізілуге тиіс. Көп немесе қос әсерлі түпнұсқаландыру сияқты белгілі қатаң түпнұсқаландыру пайдаланушыдан ең аз дегенде, сәйкестендірудің[3] екі кезеңін өткізуді қажет етеді.

Қатты дискілерді шифрлау сақталатын ақпаратты ашудан қорғауды қамтамасыз етеді. Бұл құпиялылық қызметі қатаң алгоритмдерді міндетті түрде пайдалануға тиіс (сондай-ақ[4][4] қараңыз).

Пішімдеудің басқа маңызды мәселесі модемді пішімдеу болып табылады. Клиент модемі ол кіріс қоңырауларды қабылдамайтындай болып орнатылуға тиіс. Қосылуды пайдаланушы-клиенттің өзі ғана инициирлауы керек.

Көптеген жағдайларда қауіпсіздікті оның дұрыс пішімделуінде дербес желіаралық қалқа жақсарта алады.

Соңында, зиян таситын бағдарламалық кодпен шақырылған залалды болдырмау және шектеу үшін, вирусқа қарсы бағдарлама орнатылып, уақытылы жаңартылуы керек.

---

[1] Құпия белгімен басқару бойынша көбірек ақпаратты ИСО/МЭК 17799 табуға болады.

[2] Биометрия адамдарды физикалық немесе мінез-құлық сипаттамасы бойынша түпнұсқаландыруды білдіреді.

[3] Түпнұсқаландыру әдетте пайдаланушыдан сәйкестікті растау үшін, олар білетін (құпия белгі), неге ие болатын (токен- немесе смарт-карта) немесе не болып табылатын бірдемені (биометриялық сипаттама), не аталған іс-қимылдардың қандай да бір топтамасын ұсынуды қажет етеді.

[4] Жариялану процесінде жатыр.

8.3 RAS серверін қорғау

8.3.1 Физикалық және жергілікті орнату

RAS сервері үшін физикалық қауіпсіздік қажеттілік болып табылады. Әдетте RAS сервері кәсіпорын серверлерінің инфрақұрылымдарының бөлігі болып табылады және басқа серверлер сияқты физикалық қауіпсіздік деңгейі болуы керек. Қашықтан қызмет көрсету үшін пайдаланылатын кез келген басқа қызметтер сияқты, RAS сервері ТСА орналастырылуы керек. Авторластырылмаған физикалық қол жеткізуге қарсы қорғауға оны жабық серверлік бөлмеде орналастыру жолымен, қорек жаңылуларына қарсы – үздіксіз қорек көзін қолданумен қол жеткізіледі. Басқа қажет етілетін шаралар RAS серверін қауіпсіз орнату және пішімдеу, қауіпсіз басқару және резервтік көшірмелеу шаралары және ақпаратты қалпына келтіру болып табылады.

Дегенмен, RAS серверінің барынша тараған түрі ретінде әлі де болса, қол жеткізуді модем арқылы қамтамасыз ететін немесе ISDN телефон желісін пайдаланатын сервер қалады, әйтсе де, қол жеткізу ұйым тарапының бақылауынсыз RAS провайдерінің жергілікті қызметі арқылы іске асырылатын кезде осындай шешімдер болады. Одан арғы қол жеткізу содан кейін Интернет арқылы ұсынылады және басқарылады және желіаралық қалқалар жүйесін ұйымдастырумен шектеледі.

Осындай әдістің артықшылығы төменгі баға (қол жеткізу әдетте жергілікті қоңырау болып табылады), ал кемшілігі – клиенттің екі рет сәйкестендірілуі болып табылады: алдымен Интернет провайдерінің қызметінде, ал содан соң тағы да қашықтан орналастыру орнында.

8.3.2 RAS сервері және модем

Модем арқылы қол жеткізуді ұсынатын RAS сервері үшін, модемнің жұмысы инфрақұрылымға қосымша қатерлер әкелмейтініне кепілдік беретін кейбір шаралар қарастырылуға тиіс.

Компьютер RAS ұсынатын тапсырманы ғана орындайтындай болып үйлестірілуге, ал басқа қызметтер ескерілмеуге тиіс. Операциялық жүйе күшейтілуге және онда пайда болған барлық түзетулер мен жаңартулар жасалуға тиіс. Тек әкімшілік және қызмет көрсететін қызметкерлер құрамына ғана серверге физикалық түрде қол жеткізуге рұқсат етілген. Серверде әдеттегі пайдаланушылардың есептік жазбалары болмауы керек.

Егер RAS сервері сондай-ақ басқа қызметтерді де ұсынатын болса, онда қызметтердің топтамасының жаңа қатерлер әкелмейтіні тексеріліп, расталуы қажет. RAS серверінің пішін үйлесімін қолдауды бағдарламалық қамтуды әзірлеуші ұсынуға тиіс.

Назарға алынуға тиіс басқа да маңызды мәселелер мыналар болып табылады: деректерді резервтік көшірмелеу; жиналуға тиіс тіркелетін ақпарат; файлдарды басқару стансасына тіркеуге беру (күнделікті талдау үшін) және қиын жағдайлардағы іс-қимылдар жоспарын дайындау.

Қашықтан қол жеткізу қызметтерін белсенді ұсынуды бастағанға дейін, серверді белгілі осалдықтарға тексеру керек. Тестілер жергілікті пішін үйлесімі мен желіні қорғау тексерісін қамтуға тиіс.

Модем кіріс қоңырауларға ғана мүмкіндік беріп, бір бағыттағы пассивті жұмыс үшін үйлестірілуге тиіс. Егер мүмкін болса, пішін үйлестірілімі модемде түпнұсқаландыруды өткізуге, содан соң жадыда алдын ала сақталған нөмірге кері қоңырауды (кері шақыру сияқты да белгілі) инициирлауға мүмкіндік беруі қажет. Мұндай кері шақыру тек тұрақты клиенттермен немесе мобильді телефондар арқылы қосылған шағын компьютерлермен ғана жұмыс жасайды. Бұндайда тек белгілі мекенжайлармен ғана қосылу расталады (телефон нөмірлерімен) және мұндай тәсіл қоңырау шалған

субъектіге қоңырау құнын азайтуға мүмкіндік береді.

Қазіргі заманғы телефон жабдығы (мысалы, PBX) бастапқыда тағайындалған нөмірден басқа нөмірге қайта бағыттау кезінде, кіріс (қоңырауларды) қайта адрестеу мүмкіндігін ұсынады. Сондықтан, кері шақыру механизмдерін қосымша сақтықтармен пайдалану қажет.

Клиенттердің вирусқа қарсы бағдарламасы белгіленіп және уақытылы жаңартылуы керек.

8.3.3 Желіге қол жеткізу сервері

Егер қашықтан қол жеткізу Интернет (ISP) провайдерінің жергілікті қызметі арқылы белгіленсе, онда желіге қол жеткізу, ISP қол жеткізу ұйым тарапынан болатын тікелей бақылаудан тыс болатын болса және түпнұсқаландыру нәтижесі оған белгісіз болса, желіге қол жеткізу серверімен (NAS) бақылануға тиіс.

NAS кез келген желілік құрылғы сияқты қорғалуға тиіс, яғни ол оған физикалық қол жеткізуді авторластырылған әкімгерлер ғана алуы үшін, жабық үй-жайда сақталуы қажет. Құрылғыны басқару жергілікті қауіпсіздік саясатына сәйкес болуға тиіс: егер желіні басқару жүйесі оның барлық әрекетін бақылайтын болса, онда басқару жүйесі мен NAS арасындағы кесте не жергілікті желі ішінде іске асырылуға, не ақпарат түрін жасыру үшін туннелденуге тиіс.

8.3.4 Сымсыз қол жеткізу нүктесі

Сымсыз ЛВС арналған қол жеткізу нүктелері қашықтан қол жеткізудің типтік тәсілі болып табылмағанымен, олар желіге қол жеткізуді ұсыну үшін пайдаланылуы мүмкін. Сондықтан, басқа сымсыз технологияларына арналған қол жеткізу нүктелері ТСА орналастырылып, қорғалуға тиіс. Сымсыз қол жеткізу қауіпсіздігі туралы қосымша ақпаратты 8.5 қараңыз.

8.4 Қосылуды қорғау

8.4.1 Жалпы ескертулер

RAS клиенті мен RAS сервері арасындағы қосылу сатысының бірнеше сандарынан өтеді. Бастапқыда қосылу белгіленеді, содан кейін ол жұмыс істейді, ал пайдаланғаннан соң ол тоқтатылады. Байланыстың барлық осы сатылары қорғауды қажет етеді.

Келесі бөлім RAS клиенті мен RAS сервері арасындағы қосылуды қорғаудың түрлі сатыларын қарастырады.

8.4.2 Қосылыстарды орнату

Қауіпсіз қосылуды орнату қашықтан пайдаланушыны түпнұсқаландыруды қажет етеді. Бұл қашықтан қол жеткізу үшін пайдаланылатын арнайы хаттаманы[1] орнатқанда жүргізіледі.

Пайдаланушыны түпнұсқаландырудың сондай-ақ қауіпсіздік деңгейі бойынша ерекшеленетін әртүрлі тәсілдері қолданылады. Алғашқы екі хаттама клиент (абонент деп аталатын) пен сервер (түпнұсқаландырушы) арасында пайдаланылады, үшінші хаттама түпнұсқаландырудың қосымша сұлбаларын қамтуға мүмкіндік беретін түпнұсқаландыру серверін пайдаланады.

[1] Модемді қол жеткізу үшін бұрын тек қарапайым түпнұсқаландыруды іске асыруға ғана мүмкіндік беретін SLIP хаттамасы пайдаланылған, қазір пайдаланылатын нүкте-нүкте (PPP) хаттама барынша сенімді болып табылады және озық түпнұсқаландыруды қамтамасыз етеді.

Түпнұсқаландырудың барынша ортақ сұлбасы түпнұсқаландырушы сервер абоненттердің мандатын алатын және осы мандаттарға сүйеніп, оларға қол жеткізуге мүмкіндік беретін немесе бас тартатын байланыс орнататын екі жақты хаттама болып табылатын құпия белгілік түпнұсқаландыру хаттамасын (PAP) пайдалану болып табылады. Мандаттар ашық мәтінмен жіберіледі және әдетте, пайдаланушының сәйкестендіргішінен (ID) және құпия белгіден тұрады. Сондықтан бұл хаттама бір түрлі шабуылдарды қайталаудан қорғауды қамтамасыз етпейді.

Барынша жетілдірілген түпнұсқаландыру сұлбасы түпнұсқаландырудың «қосылу сұранымы» (CHAP) хаттамасымен ұсынылады. Ол түпнұсқаландырушы клиентке «сұраныс» жіберетін үш белгіден тұратын байланысты орнату хаттамасы болып табылады. Бұл бірегей сұраныс және жаңа жіберуде әр жолы өзгереді. Клиент өз сәйкестендіргіштерімен ID («құпия» деп аталатын) және «сұраным» параметрлерімен есептелген құпия мәнде жауап береді. Түпнұсқаландырушы нәтижені өз есептеулерімен салыстырады және мүмкіндік береді немесе қол жеткізуді қабылдамайды. Берілетін мандат хэш-алгоритм пайдаланылып шифрланады (MD5 алгоритмі барынша жиі пайдаланылатын болып табылады). CHAP сұраным қаншалықты болжанғандығына қарай, қайталанатын бір түрлі шабуылдарға қарсы қорғайды.

Барынша ортақ тәсіл 7.3 сипатталғандай, RADIUS жүзеге асырылады.

RADIUS сервері әдетте ID орталыққа бағындырып сақтайды, яғни ол қашықтан пайдаланушылардың жалпы қолжетімді құпияларын сақтайды. Егер пайдаланушы желіге қол жеткізуді алғысы келсе, ID, құпия белгі, сәйкестендірілген жүйе деректері мен қол жеткізу үшін пайдаланылатын жүйе порты болатын RADIUS серверіне «қол жеткізу сұранысын» жібереді. Құпия белгі болғанда, ол криптографиялық құралдарды пайдаланып жасырынады. RADIUS сервері сұранысқа өзі жауап бере алады немесе сұранысты басқа RADIUS серверіне жібере алады. Егер сервер сұранысқа жауап берсе, онда ол алдымен берілген деректердің дәл екендігін растауға тиіс. Дәл сәйкестендіру, кем дегенде, ID және құпия белгіден құралуға тиіс, бірақ сондай-ақ жүйелік мекенжайды және тағайындалған портты қамти алады. Егер сұраныс басқа RADIUS серверіне жіберілетін болса, онда бастапқыда жолданған сервер өзін клиент ретінде ұстайды. Осындай әдіспен қосымша түпнұсқаландыру өткізілуі мүмкін. UNIX, WINDOWS немесе NOVELL түпнұсқаландырулар үлгілер бола алады. RADIUS сервері сондай-ақ PAP немесе CHAP түпнұсқаландыру сұлбасын пайдалана алады.

Қатаң түпнұсқаландыру цифрлық сертификаттар немесе токендер пайдаланылып өткізілуі мүмкін. Түпнұсқаландырудың бұл әдісі пайдаланушының біліміне ғана емес, сонымен бірге токенге немесе сертификатқа ие болуына негізделеді, сондықтан ол қос әсерлі түпнұсқаландыру деп аталады. Сондай-ақ биометрикалық сәйкестендіру де пайдаланылуы мүмкін.

Ескертпе - Ескірген TACACS желілік қызметі және оның XTACACS және TACACS+ түрлендірулері бұрынғысынша пайдаланылады, бірақ RADIUS сияқты маңызды рөл ойнамайды.

8.4.3 Шифрланған байланыстар

Ақпаратты ұстап алу қаупі криптографияны пайдаланғанда жойылуы мүмкін. Байланыс арнасында шифрлау ұқсас шифрлау жабдығы болатын аппараттық құралдармен ғана байланысу мүмкіндігін шектейді. Мазмұнын шифрлау көп солқылдақтыққа жол береді және шифрлаудың меншікті қызметін ұсынбайтын серверлерге қосылуға мүмкіндік береді. Мұндайда шифрлаудың тиісті ақырғы нүктелерінің арасындағы байланыстың құпиялылығы қамтамасыз етіледі.

Мазмұнын шифрлау үлгісі PGP бағдарламалық қамтуын, ашық кілтті пайдалануға негізделген шифрлауды ұсынатын бағдарламалар дестесін бұндайда авторлықтан және

түпнұсқаландырудан бас тарту мүмкін еместігі сияқты қызметтерді көрсете отырып пайдалану болып табылады.

Маңызды: Шифрлау бағдарламасын пайдаланғанда, пайдаланатын кілттің жеткілікті екендігіне көз жеткізіңіз. Сонымен қатар, оларды пайдаланбас бұрын, электронды пошта арқылы алынған ашық кілттің сертификаттарының түпнұсқалығын және дұрыстығын анықтауға арналған шараларды анықтаңыз.

Қашықтан қол жеткізудегі байланыс мазмұнын қорғаудың қосымша тәсілдері виртуал жабық желілерді (VPN) пайдаланып қамтамасыз етіледі. Осындай қорғаныс түрін ұсынатын қол жетімді өнімдердің бірнеше түрі болады. Оларды қолданып, VPN ұйымы үшін стандартталған хаттамалар ғана пайдаланатындығына көз жеткізіңіз.

8.5 Сымсыз қосылыстарды қорғау

Сымсыз байланыс хаттамалары қашықтан қол жеткізудің түрлі нұсқаларында пайдаланылуы мүмкін:

– Bluetooth сияқты хаттамалар мобильді телефондардың жақын байланысы үшін, модемдер немесе қашықтан қол жеткізудің клиенттік жүйесіне кең жолақты қол жеткізудің өзге құрауыштары үшін пайдаланылады;

– IEEE 802.11 стандарттарының легінде анықталған хаттамалар сияқты сымсыз ЛВС хаттамалары қашықтан қол жеткізудің клиенттік жүйелерін жалпы қолданылатын және жеке желілерге қосу үшін пайдаланылуы мүмкін.

Осы тәріздес жағдайлардың көбінде қашықтан қол жеткізу мүмкіндіктерін ұсынатын ұйымның сымсыз байланыстың пайдаланылатын хаттамаларының пішімдерін үйлестіруге немесе реттеуге өте шектеулі ықпалы болады немесе болмайды:

Үлгі ретінде, мобильді пайдаланушы әуежайларда болатын, жалпы қолданылатын сымсыз ЛВС («hot spot» деп аталатын) қол жеткізу құралдарын пайдалана отырып, қашықтан қол жеткізудің клиенттік жүйесімен қосыла алады. Бұндай сымсыз қол жеткізудің инфрақұрылымы, әдетте, ISP тиесілі және пайдаланушылар немесе олардың ұйымдары оның пішім үйлесіміне ықпал ете алмайды.

Сымсыз хаттамалар кейбір қауіпсіздік қызметтерін ұсынғанымен, оларға қашықтан қол жеткізу саласында тұтастай сенуге болмайды. Осы себепті, егер сымсыз хаттамалар қашықтан қол жеткізу мүмкіндіктерімен бірге барлық талап етілген түпнұсқаландыру немесе құпиялылық сияқты қауіпсіздік қызметтерін байланыстыруды іске асыруға мүмкіндік берсе, 8.3 суреттелгендей барынша жоғарғы деңгейдегі хаттамалар мүмкіндігін пайдаланумен қоса жүзеге асырылуға тиіс. Қатаң түпнұсқаландыру мен құпиялылықты қамтамасыз ету үшін, IPsec немесе SSL/TLS сияқты туннельдеу хаттамаларын пайдалану ортақ тәсіл болып табылады.

Ұйым қашықтан қол жеткізу үшін сымсыз инфрақұрылымды үйлестіруі мүмкін болатын жағдайларда қол жеткізу нүктесін қауіпсіздендіру үшін, қосымша техникалық шаралар қажет етіледі. IEEE 802.11 хаттамаларының ішіне салынған AP қол жеткізуді қауіпсіздендіру үшін пайдаланылатын қазіргі заманғы үш әдіс қолданылады:

– (SSID) қызметін орнатуға сәйкестендіру;

– Жалпы қол жеткізуді басқару мекенжайларын сүзу (MAC);

– Сымсыз (WEP) немесе қорғалған қол жеткізумен WiFi (WPA) тең бағаланатын құпиялылық.

Бірақ, тіпті, барлық үш әдісті бірге пайдаланғанда да, ұйымның тиісті қауіпсіздігін әрқашан қамтамасыз ете алмайды.

SSID қол жеткізудің (AP) бір немесе бірнеше нүктелері қызмет көрсететін көптеген бірнеше шағын бағыныңқы желілердің сегменттеу механизмін білдіреді. Қол жеткізудің

әрбір нүктесі өндірушіге осы АР және мүмкін, сәйкесті АР қатысты басқа ақпаратты көрсететін SSID сәйкестендіргішінің үндемеуі бойынша белгіленген өндірушілерден келіп түседі. Осындай SSID АР-мен жұмыс жасайтын ұйым туралы және жабдықтың өзі туралы ақпарат болатын басқа SSID өзгертілуге тиіс. АР үшін ең төменгі талап радио арнасы бойынша өз SSID кең таратылатын хабарына тыйым салу болып табылады. Басқа жағынан алғанда, кез келген тыңдайтын құрылғы SSID жаза алады және дұрыс SSID шақыра отырып, АР-мен қосылуға ұмтылады. Сол себепті, кең таратылып берілмейтін SSID жазу тәсілдері бәрібір қалғанымен, кең таратылған хабар режімінде АР пішімін үйлестіруге қатаң тыйым салу ұсынылады.

SSID АР-ды сәйкестендіретін уақытта, MAC-мекенжай компьютердің желілік интерфейсін сәйкестендіреді. Желілік интерфейстің әрбір тақшасының бірегей MAC-мекенжайы болады. Сымсыз ЛВС қауіпсіздігін арттыру үшін, АР, егер бұл мүмкін болса[1], клиент компьютерлерінің дұрыстығын, олардың MAC-мекенжайларының дәл келуін талдау көмегімен сәйкестендіруге тиіс. Дегенмен, MAC-мекенжайлардың дәл келуі мүмкін, бірақ бұл сымсыз ЛВС қол жеткізуге кейбір қорғауларды қосады.

WEP құпиялылыққа, бүтіндік пен түпнұсқалыққа әсер ететін тиянақты осалдығы болуымен белгілі. Алайда ол 40 немесе 104 бит ұзындықтағы құпия кілтті пайдаланып, байланысуда шифрлауды ұсынады. Бұл кілт инициализациялаудың 24–биттік векторына қосылады, нәтижесінде кілттің ұзындығы 64 немесе 128-биттік болады. WEP хаттамасының белгілі осалдығынан, кілттер қауіпсіздікті ұлғайту үшін жиі өзгертілуге тиіс. WPA (жетілдірілген WEP) егер уақытша құпия кілттерді дұрыс ұсынуда үйлестірілген болса, осы кемшіліктерді жеңіп шығады.

Осыған қосымша «клиентті резервте ұстау» (яғни, компьютерлік MAC-мекенжайлар белгілі бір IP-мекенжайлармен байланысқан) мүмкіндігімен қоса АР ұсынатын хостарды реттеудің динамикалық пішім үйлесімдерінің хаттамасын (DHCP) пайдалану ұсынылады немесе статикалық мекенжайларды пайдалану ұсынылады.

Маршрутталмайтын IP-мекенжайларды пайдалану жағдайында, бағыныңқы желінің ішкі IP-мекенжайларын (әдетте 192.168.0.0 пайдаланады) басқа бағыныңқы желі мекенжайларына өзгертіңіз. Сондай-ақ, WAP және сымсыз маршруттауышты басқаруға арналған сымсыз қол жеткізуді оларды шабуылдаушылардың түрленуін болдырмас үшін, тыйым салыңыз.

Одан кейін, өзіңіздің сымсыз ЛВС жағдайын уақытылы бағалаңыз.

Сымсыз ЛВС қауіпсіздігі бойынша ұсынымдардың толық тізбесі F қосымшасында берілген.

8.6 Ұйымдастыру шаралары

Ұйымдастыру шаралары пайдаланушылардың, әкімгерлер мен қауіпсіздік қызметінің қызметкерлер құрамының рөлін анықтайтын, қашықтан қол жеткізу саясатын қамтуға тиіс. Сондай-ақ, осы процестерге тартылған адамдардың жауапкершілігі анықталуы керек. Қашықтан қол жеткізу саясатының үлгісі А қосымшасында беріледі.

Кейбір мобильді құрылғылар үшін (мысалы, PDA, смарт-телефон) жеткілікті техникалық қорғауды іске асыру орындалмауы мүмкін, сол себепті қатерлерге қарсы тұру бойынша қосымша ұйымдастыру шараларына қажеттілік туындауы мүмкін.

Ұйымдастыру шараларының басқа аспектілері құпиялылықты қамтамасыз ету жоспары, резервтік көшірмелеу, ақпаратты қалпына келтіру, қызметкерлер құрамын

[1] MAC-мекенжайға негізделген қол жеткізуді шектеу, үлкен сымсыз желіде немесе кейбір жұмыс жағдайында мақсатқа сәйкес болмауы мүмкін.

оқыту, пайдаланушыларды жаттықтыру және пайдаланушылардың мәселенің маңыздылығын түйсінуі болып табылады.

Осы мәселелер бойынша көбірек ақпаратты [1], [2] және [3] табуға болады.

8.7 Заңдық аспектілер

Қашықтан қол жеткізу технологияларын іске асыру қолданылатын барлық ұлттық заңдылықтарды және (немесе) нормативтік шектеулерді не талаптарды ескеріп қабылдануға тиіс.

Жобалаушылар болжанбаған салдарлар жағдайындағы техникаға сенімді болу үшін, міндетті келісім-шарттық және қол жеткізудің басқа заңдық аспектілерінің ескерілгеніне көз жеткізуі керек.

9 Қорытынды

Қашықтан қол жеткізу қызметтерін ұсыну тиісті қауіпсіздік саясатын қабылдаудан басталатын, жақсы жоспарланған тәсілді, қажетті техникалық құралдарды, сондай-ақ ұйымдастыру және заңдық шараларды пайдалануды қажет етеді.

А қосымшасы
(анықтамалық)

Алыс жердегі қол жеткізуді қорғау саясатын ұйымдастыру үлгісі

А.1 Мақсаты

Аталған саясаттың мақсаты «Компанияны» кез келген хостағы желімен қосу үшін стандарттарды анықтау. Бұл стандарттар «Компанияның» ресурстарын авторластырылмаған пайдаланудан болуы мүмкін «Компанияның» әлеуетті залалын барынша азайту үшін әзірленген. Залал компанияның құпия мәліметтерінің, интеллектілік меншіктің кемуін, компанияның қоғамдық бейнесіне, «Компанияның» ішкі жүйелеріне және т.с.с. төнетін қатерді қамтиды.

А.2 Қолданылу саласы

Бұл саясат барлық қызметкерлерге, бәсекелестерге, жабдықтаушыларға, «Компания» агенттері мен иелеріне, дербес компьютерлер иелеріне және «Компания» желісіне қосылатын жұмыс стансаларына қолданылады. Бұл саясат электронды поштаның жіберуді немесе оқуды және интернеттік Web-ресурстарды қарауды қоса алғандағы, «Компания» атынан орындалатын жұмыстар үшін пайдаланылатын қашықтан қол жеткізуге қосылуға қолданылады.

Осы саясат модемдерді, Frame Relay, ISDN, DSL, VPN, SSH, кабельдік модемдерді және т.с.с. пайдаланып, қашықтан қол жеткізуді орындауға таралады.

А.3 Саясат

А.3.1 Жалпы ережелер

1) «Компанияның» бірлескен желісіне қашықтан қол жеткізудің артықшылық құқығына ие «Компанияның» қызметкерлеріне, серіктестеріне, агенттеріне қашықтан қосылуда олардың да «Компанияның» желісіне қосылған жергілікті пайдаланушылар сияқты дәл сондай түсініктен шығатындығы үшін жауапкершілік жүктеледі;

2) Интернетке үйде пайдаланушылардың дербес компьютерлерден «Компания» желісі арқылы жалпы қол жеткізуіне, тек «Компанияның» тіклей жұмыскерлері болып табылатын қызметшілеріне ғана рұқсат етіледі. «Компания» қызметшісі отбасы мүшелерінің ешқайсысының «Компания» саясатын бұзбайтындығына, заңсыз әрекетті орындамайтындығына және қол жеткізуді бөтен іскерлік мүдделер үшін пайдаланбайтындығына жауапты. «Компания» қызметшісі егер қол жеткізу дұрыс пайдаланылмайтын болса, толық жауап береді;

3) Ақпаратты қорғаудың мынадай ережелерін RAS әдістерінің көмегімен бірлескен желіде және «Компания» желісінде пайдаланатын қол жеткізуде мұқият қараңыз:

a) Шифрлау саясатын қабылдау;

b) Виртуаль жабық желі (VPN);

c) Сымсыз байланыс ережесі;

d) Қабылданған пайдалану ережесі.

4) Тапсырыс тәртібін немесе қызмет көрсетуді ажыратуды, салыстырмалы бағаларын, ықтимал проблемалар шешімін және т.с.с. қоса алғандағы, «Компанияның» RAS қосылу аспектілеріне қатысты қосымша ақпаратты RAS Web-сайтынан табуға болады.

А.3.2 Талаптар

1) Қашықтан қауіпсіз қол жеткізу қатаң бақылануға тиіс. Бақылау бір реттік құпия белгімен немесе қатаң құпия белгілік фразадағы ашық/жабық кілттермен түпнұсқаландыру арқылы орындалатын болады. Қатаң құпия белгі фразасын жасау туралы ақпаратты Құпия белгі саясаты бөлімінен қараңыз;

2) «Компания» қызметшісі ешқашан ешкімге, тіпті өз отбасы мүшелеріне өзінің логинін немесе электронды поштасының құпия белгісін бермеуге тиіс;

3) Қашықтан қол жеткізудің артықшылық құқықтары бар «Компания» қызметшілері және оның серіктестері оларға тиесілі «Компанияның» дербес компьютерлері мен «Компанияның» бірлескен желісімен қашықтан байланысатын жұмыс стансаларының, пайдаланушының толық бақылауында болатын дербес желіні есептемегенде, бір және сол уақытта қандай да бір басқа желімен байланыспайтындығына сенімді болулары керек;

4) «Компанияның» бірлескен желісіне қашықтан қол жеткізудің артықшылық құқықтары бар «Компания» қызметшілері мен оның серіктестері ресми бизнесті жеке бизнеспен ешқашан араластырмау сенімділігіне ие болу үшін, «Компанияға» тиесілі емес электронды поштаның есептік жазбаларын (мысалы, Hotmail, Yahoo, AOL), не «Компания» шаруаларын орындау үшін өзге сыртқы ресурстарды пайдаланбауға тиіс;

5) «Компания» желісіне қол жеткізу үшін үйлестірілген ISDN желілеріне арналған бағыттар CHAP ұсынатын түпнұсқаландыру бойынша талаптардың ең төменгі деңгейіне сәйкес болуға тиіс;

6) Пайдаланушының үйдегі жабдығының пішім үйлесімін бөлек туннелдеу мақсаты үшін немесе оны екі есе қосу үшін өзгертуге тыйым салынған;

7) Frame Relay түпнұсқаландыру бойынша DLCI стандарттарында ұйғарылған талаптардың ең төменгі деңгейіне сәйкес болуға тиіс;

8) Аппараттық құралдардың стандарт емес пішім үйлесімдерін RAS қызметі құптауы керек, ал ақпараттық қауіпсіздік қызметі жабдыққа қол жеткізуге арналған үйлестіру қауіпсіздігін растауға тиіс;

9) Қашықтан қол жеткізу технологиясының көмегімен «Компанияның» ішкі желілерімен қосылатын дербес компьютерлерді қоса алғандағы, барлық хосттардың қазіргі заманғы вирусқа қарсы бағдарламаларды (осы бағдарламалар орналасатын жерге бірлескен сайт URL осында сыйғызыңыз) пайдалануы қажет. Үшінші тараппен жалғасу үшінші тарап белгілеген талаптарға сәйкес болуға тиіс;

10) «Компания» желілеріне қосу үшін пайдаланылатын жеке жабдық «Компанияға» тиесілі жабдықтарға қойылатын талаптарға сәйкес болуға тиіс;

11) «Компания» желісіне қашықтан қол жеткізу бойынша қалыптан тыс шешімдерді іске асырғысы келетін ұйымдар немесе тұлғалар алдын ала қашықтан қол жеткізу қызметінің және ақпараттық қауіпсіздік қызметінің келісімін алулары керек.

А.4 Саясатты мәжбүрлеп жүргізу

Осы саясатты бұзатын кез келген тұлға жұмыстан босатылуды қоса алғанда, тәртіптік жазаларға тартылуы мүмкін.

А.5 Терминдер мен анықтамалар

Кабельдік модем: Кейбір кабельдік компаниялар телевизиялық кабель бойынша Интернетке қол жеткізуді ұсынады.

Телевизиялық коаксиальді кабель: Бұл кабельді модеммен қосылатын коаксиал кабель, оның бойымен Интернет деректері 1,5 Мб/с артық жылдамдықпен беріледі. Қазіргі уақытта кабель кей жағдайларда ғана қолданылады.

CHAP: Түпнұсқаландырудың «қосылу сұранымы» хаттамасы − біржақты хэштеу қызметін пайдаланатын түпнұсқаландыру тәсілі.

DLCI: Деректердің берілуі кезінде қосылатын сәйкестендіргіш. Frame Relay желісінің соңғы нүктесіне берілген, үздіксіз виртуал (VPC) желісіне арналған бірегей нөмір. DLCI Frame Relay желісіндегі қол жеткізудің пайдалану арнасы ішінде әдеттегі VPC соңғы нүктені сәйкестендіреді және тек осы арнаға арналған жергілікті мәні болады.

Телефон модемі: Деректерді телефон желілері арқылы беру үшін, компьютерлердің біреуін екіншісімен қосатын шалғайдағы құрылғы. Модем телефон желілері арқылы салып жіберу үшін, компьютерлердің цифрлық деректерін ұқсас белгілерге түрлендіреді (модульдеу) және қабылданатын ұқсас белгілерді модем атауы модульдеуші/модульсіздеуіш мағынасын білдіретіндей бейнеде, желінің бір ұшында компьютер оқитын цифрлыққа (модульсіздеу) түрлендіреді.

Екі жақты қосылу: Компьютердің біреуден артық желісіне немесе желілік құрылғысына қосылу мүмкіндігі. Мысалы, жергілікті Ethernet байланыс арқылы бірлескен желімен қосылу кезінде Интернет (ISP) провайдеріне қосылуды іске асыру. Немесе үйде отырып, қашықтан қол жеткізуді ұсынатын «Компания» желісінде болып, басқа желімен қосылады, мысалы жұбайының компания желісімен. Немесе «Компаниямен» және дестелерді тағайындауына байланысты ISP қосуға арналған ISDN маршруттауышын үйлестіру қажет.

DSL: Цифрлық абоненттік арна кабельді модемдермен бәсекелесетін Интернетке жоғары жылдамдықты қол жеткізу үлгісі болып табылады. DSL стандартты телефон желілері арқылы жұмыс істейді және 2 Мб/сек дейінгі кіретін деректер ағынының жылдамдығын әрі шығатын ағынға арналған аз жылдамдық шамаларын қолдайды.

Frame Relay: ISDN жылдамдығынан бастап T1 желісінің жылдамдығына дейін қосылу жылдамдығын қадаммен өзгертуге болатын байланысу тәсілі. Frame Relay жылдамдыққа байланысты, уақытша төлемді пайдаланудың орнына белгіленген тарифтік жалақыны пайдаланады. Frame Relay кезінде телефон компаниясының желісі арқылы қосылады.

ISDN: Интегралданған қызметпен бірге цифрлық желі қызметінің екі түрі болады немесе ISDN: BRI және PRI. BRI қашықтан қол жеткізудің/үйдегі кеңселері үшін пайдаланылады. BRI 64 килобиттан екі шапшаң арнасы (128 килобитпен бірге) және белгі беретін ақпаратты беруге арналған 1D арнасы болады.

Қашықтан Қол жеткізу: Желі арқылы «Компанияның» бірлескен желісіне, «Компания» бақыламайтын құрылғыға немесе ортаға кез келген қол жеткізу.

Бөлек туннелдеу: VPN-туннель арқылы «Компанияның» бірлескен желісіне қосылу кезінде, қашықтағы құрылғыдан (ДК, PDA, WAP телефон және т.с.с.) компанияға тиесілі емес желіге (Интернет немесе үйдегі желі) бір мезгілде тікелей қол жеткізу. Виртуал жабық желі (VPN) − Интернет арқылы туннельдеу әдісімен қашықтағы желіге қол жеткізу әдісі.

В қосымшасы
(анықтамалық)

RADIUS енгізу және орнату бойынша ұсынымдар

В.1 Жалпы ережелер

Бұл қосымшада Microsoft Windows 2000 ортасында және басқа операциялық жүйелерде RADIUS-ті пайдалану бойынша ұсынымдар беріледі.

RADIUS-пен қауіпсіз жұмыс жасау үшін, Сіздің мынадай нұсқауларды қолдануыңыз қажет.

В.2 Енгізу бойынша ұсынымдар

Сервер клиенттерін немесе RADIUS прокси-серверін пайдаланғаныңызда, мынадай ұсынымдарды қолданыңыз:

RADIUS деректерінің құпиялылығын қамтамасыз ету үшін, ESP және мысалы, 3DES сияқты шифрлау алгоритмін пайдаланып, Ipsec қолданыңыз.

Бұл [31] сипатталған. Ipsec көмегімен барлық RADIUS хабарламаларын шифрлағанда, RADIUS хабарламаларының қиын өрістері (мысалы, Қол жеткізу-Сұранымы хабарламасындағы түпнұсқаландырғыш сұранысы сияқтылар) мен анықтауыштар (мысалы, пайдаланушының құпия белгісі, туннель құпия белгісі және MPPE кілтін анықтауыштар сияқтылар) қараудан қорғалады. Шабуылдаушы алдымен RADIUS хабарламасының мазмұнын талдау мүмкін болғанға дейін, ESP қорғалған RADIUS хабарламасының шифрын ашып тануға тиіс. Шабуылдаушыға кедергі жасау үшін, RADIUS серверіне қарсы оған қосылған кезде шабуылдар ұйымдастырып, IPsec сертификатына негізделген түпнұсқаландыруды қолдау ұсынылады.

Баламалы түрде немесе Ipsec пайдаланумен бірге:

1) Ұзындығы 32 он алтыдан кем болмаймын рәмізден тұратын немесе 22 пернетақта рәмізінен кем болмайтын құпия кілттерді үйлестіріп пайдалануыңыз;

2) Қол жеткізу сұранысының барлық хабарламалары үшін хабарламаны түпнұсқаландыру анықтауышын пайдалануыңыз қажет;

RADIUS клиенті үшін қол жеткізу сұранысының барлық хабарламалары үшін хабарламаны түпнұсқаландыру анықтауышын пайдалану және оны пішім үйлесіміне қосу керек. RADIUS сервері немесе прокси-сервері үшін Қол жеткізу-Сұранымы түріндегі хабарламалар үшін хабарламаны түпнұсқаландыру анықтауышын пайдалану және оны пішім үйлесіміне қосу қажет болады.

3) Сұранысты түпнұсқаландыру үшін кездейсоқ сандардың криптографиялық берік өндіргішін пайдаланыңыз.

RADIUS енгізу кезінде клиентті түпнұсқаландыруға арналған қосымша қорғауды қамтамасыз ету үшін, мынадай ұсынымдарды пайдаланыңыз:

1) Түпнұсқаландырудың қатаң әдістерін пайдаланатын EAP және ұқсас EAP хаттамаларын пайдаланыңыз;

EAP қатаң әдісінің үлгісі қол жеткізу клиентінің сертификатын және RADIUS серверін өзгертуді қажет ететін EAP-TLS болып табылады. Барлық EAP хабарламалары IPsec қорғалмаған қол жеткізу сұранысының хабарламаларын қамтамасыз ететін, хабарламаны түпнұсқаландыру анықтауышын пайдалануды қажет етеді.

2) Өзара түпнұсқаландыруды пайдаланатын, түпнұсқаландыру әдістерін

пайдаланыңыз;

Өзара түпнұсқаландыру кезінде қосылудың екі тарабы да өз әріптесін түпнұсқаландырады. Егер түпнұсқаландырудың біреуі болмай қалса, қосылу әрекеті кейінге қалдырылады. Мысалы, 2-нұсқаның EAP-TLS және MS-CHAP өзара түпнұсқаландыру әдістері болып табылады. EAP-TLS пайдаланған кезде, RADIUS сервері қол жеткізу клиентін пайдаланушы сертификатының дұрыстығын растайды, ал қол жеткізу клиенті RADIUS серверінің компьютерлік сертификатының дұрыстығын растайды. 2-нұсқаның MS-CHAP пайдаланған кезде, қол жеткізу клиенті де, қол жеткізу сервері де пайдаланушының есептік жазбасының құпия белгісін білуін растайды.

3) Егер Сіз PAP түпнұсқаландыруын қолдансаңыз, оны пайдалануды үндемей қол жеткізілетіндей етіп жасаңыз;

Мысалы, OTP/токен-карта түпнұсқаландырылған ақпаратты жіберу үшін PAP пайдаланады. Егер Сізге PAP хаттамасын пайдалану қажет болса, оны пайдалануды үндемей қол жеткізілетіндей етіп жасаңыз және ұзын құпия кілттер мен сұраныстың криптографиялық сапалы түпнұсқаландырғыштарын қолданыңыз. IEEE 802.1X PAP-ты қолдамайтындығынан, бұл жағдай тек PAP қосылуларына ғана қолданылады.

4) Егер Сіз CHAP түпнұсқаландыруын қолдансаңыз, қатаң CHAP сұранысын пайдаланыңыз;

RADIUS сұранысының түпнұсқаландырғышына ұқсас CHAP сұранысы кездейсоқ және криптографиялық сапалы болуға тиіс.

5) Егер Сіз MS-CHAP түпнұсқаландыруын қолдансаңыз, MS-CHAP сұранысына арналған жауаптар үшін, шифрлаумен ЛВС қолдайтын менеджерлерін немесе құпия белгілер өзгерісін пайдаланбаңыз.

В.3 Орнату бойынша ұсынымдар

RADIUS орнатуда, RADIUS-пен қауіпсіз жұмыс істеу үшін, мынадай ұсынымдарды орындаңыз:

Деректер құпиялылығын қамтамасыз ету үшін, барлық RADIUS хабарламалары үшін өз клиенттеріңізді және RADIUS серверін IPsec ESP және мысалы, 3DES барлық RADIUS кестелері үшін бірге пайдаланатындай етіп үйлестіріңіз.

ESP және 3DES пайдалануға арналған IPsec пішім үйлесімі қолданылатын Ipsec байланысты. Мысалы, егер Windows 2000 қол жеткізу сервері ретінде қашықтан қол жеткізуді маршруттау және қызметі үшін және Windows 2000 IAS Active Directory™ айналасындағы RADIUS сервері ретінде пайдаланатын болсаңыз, Сіздің 1812 және 1813 UDP порттарының барлық кіріс және шығыс кестелеріне арналған 3DES шифрлауымен бірге ESP пайдаланылуы үшін, ережемен қоса, тиісті жүйе жүксауытына арналған активті IPsec саясатын үйлестіруге мүмкіндігіңіз болады. Көбірек ақпарат алу үшін Windows 2000 серверіндегі «Көмек» мәзірін қара .

Баламалы түрде немесе IPsec бірге пайдаланумен, Сізге:

1) Ұзындығы 32 он алтылық белгіден немесе жоғарғы және төменгі тіркеуіштер пернетақтасының рәміздерінің кездейсоқ бірізділігінен, тыныс белгілерінің ұзындығы 22 кем болмайтын сандары мен белгілерінен тұратын берік құпия кілттерді пайдалану қажет. Мүлтіксіз жағдайда, құпия кілттер компьютермен өндірілуге тиіс;

2) RADIUS клиент-серверінің әрбір жұбы үшін, бірлескен түрлі құпия кілттерді пайдаланыңыз;

3) Қол жеткізу сұранысының хабарламасы үшін, хабарлама түпнұсқаландырғышының анықтауышын пайдаланыңыз. Әрбір RADIUS клиенті үшін оның қол жеткізу сұранысының барлық хабарламаларымен бірге түпнұсқаландыру

анықтауышын салып жіберетіндей етіп үйлестіріңіз. Әрбір RADIUS серверін әрбір RADIUS клиентінен қол жеткізу сұранысының хабарламаларындағы хабарламаны түпнұсқаландыру анықтауышын қажет ететіндей етіп үйлестіріңіз.

4) Криптографиялық қатаң сұраныс түпнұсқаландырғышын пайдаланатын RADIUS серверінің клиенттері мен прокси-серверін пайдаланыңыз.

RADIUS орнату кезінде клиенттік қол жеткізуін түпнұсқаландыруға арналған қосымша қорғауды қамтамасыз ету үшін, мынадай ұсынымдарды пайдаланыңыз:

1) Егер PAP хаттамасы қажет болмаса, оның қол жеткізу сервері мен RADIUS серверінде пайдаланылуына тыйым салыңыз. Қауіпсіз қосылулар үшін PAP пайдаланудың жалғыз қолайлы нұсқасы құпия белгінің жоғары энтропиясы болғанда және әр пайдаланғанда өзгерген кезде, бір реттік құпия белгімен және токен-картамен түпнұсқаландыруды пайдалану болып табылады. Алайда, PAP қол жеткізуі тіркелмеген клиенттерге PAP олардың қол жеткізу серверлерінен пайдалануға және пайдаланушының есептік жазбаларының қорғалмаған құпия белгілерін жіберуге мүмкіндік береді. Бір мәрте құпия белгімен және токен-картамен түпнұсқаландыру үшін, EAP немесе EAP ұқсас хаттаманы пайдалану барынша дұрыс шешім болып табылады.

2) Егер MS-CHAP пайдалану қажет болса, ЛВС менеджерінің шифрлауын пайдалануға тыйым салыңыз;

Егер Сіз Windows 2000 IAS пайдалансаңыз, HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteAccess\Policy\Allow LM Authentication IAS серверіндегі 0 тіркеуішінің кілтінің мәнін белгілеңіз.

3) EAP немесе EAP ұқсас хаттаманы қатаң түпнұсқаландыру әдісімен бірге пайдаланыңыз;

Сымсыз қол жеткізуге арналған IEEE 802.1x хаттамасын түпнұсқаландыру EAP пайдалануды қажет етеді, сондай-ақ қол жеткізудің әрбір хабарламасын қорғау үшін, хабарламаны түпнұсқаландыру анықтауышын пайдаланыңыз және PAP түпнұсқаландыруын пайдаланбаңыз.

4) EAP- TLS немесе 2-нұсқаның MS-CHAP сияқты өзара түпнұсқаландыру әдісін пайдаланыңыз.

С қосымшасы
(анықтамалық)

FTP екі режімі

FTP екі режімі болады:
- FTP PORT режімі;
- FTP PASV режімі.

С.1 FTP PORT режімі

FTP PORT режімі FTP дәстүрлі режімі болып табылады. FTP PORT қосылуды орнатқанда, іс-әрекеттер бірізділігі мынадай болуға тиіс:

1) **FTP клиенті:** Көп нөмірлер өрісіндегі дыбыс берген портты кездейсоқ ашады. (Мысал үшін, біз оларды 6000 және 6001 TCP порттары деп санаймыз);

2) **FTP клиенті:** 6000 TCP портынан FTP TCP серверінің 21 портының арнасын ашу үшін, сұраныс жібереді;

3) **FTP сервері:** 21 TCP портынан FTP клиентінің 6000 TCP портына «ОК»-ді жібереді (пәрменділік арнасы ұйымдастырылады). Осы кезде пәрменділік арнасы орнатылады;

4) **FTP клиенті**: FTP серверіне деректер сұранысын жібереді (PORT пәрмені). FTP клиенті PORT пәрменіне ол деректерді алу үшін ашқан деректер портының нөмірін қосады. Осы үлгіде FTP клиенті деректерді алу үшін, 6001 TCP портын ашты;

5) **FTP сервері:** FTP сервері PORT пәрменінде FTP клиенті көрсеткен порт арқылы FTP клиентіне кіретін *жаңа* қосылуды ашады. FTP серверінің шығыс порты 20 TCP порты болып табылады. Осы үлгіде FTP сервері өзінің меншікті 20 TCP портынан FTP клиентінің 6001 TCP портына деректер жібереді.

Осы үлгіде екі қосылу белгіленген болды: FTP клиентін инициирлаудан шығатын қосылу және FTP сервері орнатқан кіретін қосылу. PORT пәрменінде болатын ақпараттың (пәрменділік арнасы арқылы жіберілген) деректер дестесінің ішінде сақталатындығын ескеріңіз.

С.2 FTP PASV режімі

FTP жалпыға түсінікті жүзеге асыру PASV режімі немесе пассивті режім болып табылады. FTP қосылуының PASV режімі браузерлердің көпшілігінде танымал болып табылады. PASV режімінің негізгі артықшылықтарының бірі FTP клиентіне сервердің жаңадан кіретін қосылуды жасау керек еместігі болып табылады. Біз бұдан әрі көріп отырғанымыздай, бұны FTP PASV режімі барынша жақын желіаралық қалқаларға жасайды.

FTP қосылуының PASV режіміне арналған әрекеттер бірізділігі мынадай болуға тиіс:

1) **FTP клиенті:** Көп нөмірлер өрісіндегі дыбыс берген портты кездейсоқ ашады. (Мысал үшін, біз оларды 6000 және 6001 TCP порттары деп санаймыз);

2) **FTP клиенті**: 6000 TCP портынан FTP TCP серверінің 21 портының арнасын ашу үшін, сұраныс жібереді;

3) **FTP сервері**: 21 TCP портынан FTP клиентінің TCP 6000 портына «ОК»-ді жібереді (пәрменділік арнасы ұйымдастырылады). Осы кезде пәрменділік арнасы орнатылады;

4) **FTP клиенті**: FTP клиенті деректер арнасын ұйымдастыруы үшін, қосыла алатын порт нөмірін FTP сервері ашуы н сұрайтын PASV пәрменін жібереді;

5) **FTP сервері**: TCP портының нөмірін FTP клиенті деректер арнасын орнатуы үшін қосылуды инициирлай алатын пәрменділік арнасы арқылы жібереді. Осы үлгіде FTP сервері 7000 портты ашады;

6) **FTP клиенті:** FTP серверінің 7000 деректер арнасының TCP 6001 портына жауап беретін өзінің меншікті *жаңа* қосылуын ашады. Деректердің берілуі осы арна арқылы жүреді.

PASV режіміндегі барлық қосылуларды FTP клиентінің инициирлайтынын ескеріңіз. FTP серверіне FTP клиентімен жаңадан кері қосылуды жасап қажеті жоқ.

D қосымшасы
(анықтамалық)

Поштаның қауіпсіз жұмысын тексерулер тізбесі

Келесі тізбелер пошталық сервердің жұмысын үйлестіруге, жоспарлауға және қолдауға көмектеседі. Тексерулер операциялық жүйелер, пошталық бағдарламалар, сүзгілер және т.с.с. үшін берілген [6].

D.1 Пошталық сервердің операциялық жүйелерін тексерулер тізбесі

Орындау	Іс-әрекет
	Пошталық серверді үйлестіру және өрбіту
○	Пошталық сервер функцияларын анықтау
○	Сақталатын, өңделетін және пошталық сервер арқылы берілетін ақпараттар санаттарын анықтау
○	Ақпарат қауіпсіздігіне қойылатын талаптарды анықтау
○	Осы сервер үшін бөлінген хостаны анықтау
○	Осы сервер ұсынатын немесе қолдайтын желілік қызметтерді анықтау
○	Пайдаланушылар мен пайдаланушылар санаттарын анықтау және әрбір пайдаланушы санатының құқықтарын анықтау
○	Пошталық серверге арналған түпнұсқаландыру әдістерін анықтау
	Пошталық серверге арналған операциялық жүйені таңдау
○	Осалдықтың ең төменгі ұшырағыштығы
○	Авторластырудан өтіп тағайындалған пайдаланушылар үшін тек әкімгерлер құқығымен қызметін әкімшілік шектеу қабілеті
○	Авторластырылмаған тұлғаларға арналған серверде ақпаратқа қол жеткізуді ауытқыту қабілеті
○	Операциялық жүйелердің ішіне салынған сервердің қол жеткізілмейтін қызметтері мен қажет болмайтын бағдарламалық қамтуды жасау қабілеттілігі
○	Кепілдік пен сенімділіктің қолданылатын құны (кейбір сенімділік анықталған операциялық жүйелер пайдаланылып қамтамасыз етіледі)
○	Орнату, үйлестіру, техникалық қызмет көрсету үшін тәжірибелі қызметкерлер құрамының болуы және қауіпсіздік жүйесі талаптарын сақтау
	Пак-қызметтер орнату (түзету) және операциялық жүйелерді жаңарту
○	Барлық қажетті пак-қызметтерді анықтау және орнату және операциялық жүйені жаңарту
○	Барлық қажетті пак-қызметтерді анықтау және орнату және операциялық жүйелер ішіндегілерді қоса алғанда, барлық қосымшалар мен қызметтер үшін жаңарту
	Қажет емес қызметтер мен қосымшаларды жою немесе тыйым салу
○	Қажет емес қызметтер мен қосымшаларды жою немесе тыйым салу

Орындау	Іс-әрекет
	Пайдаланушыны операциялық жүйеде түпнұсқаландыруды үйлестіру
○	Пайдаланылмаған барлық есептік жазбалар мен топтарды жою немесе қол жеткізілмейтін ету
○	Активсіз есептік жазбаларды бұғаттау
○	Нақты компьютерге арналған пайдаланушылар тобын жасау
○	Нақты компьютер үшін пайдаланушылардың есептік жазбасын жасау
○	Ұйымның құпия белгілерінің саясатын тексеру (яғни, ұзындығы, күрделілігі) және тиісті құпия белгілерді орнату
○	Сәтсіз әрекеттердің шектелген санынан кейін пайдаланушыны тіркеуді кейінге қалдыру үшін компьютерді үйлестіру
○	Түпнұсқаландыруды күшейту үшін, басқа механизмдерді орнату және үйлестіру
	Операциялық жүйе қауіпсіздігін тексеру
○	Операциялық жүйені орнатқаннан кейін, оның осалдықтарын анықтау үшін тестілеу жүргізу.
○	Анықталған жаңа осалдықтар үшін операциялық жүйенің мерзімдік тексерісін (мысалы, тоқсан сайын) жүзеге асыру.

D.2 Пошталық серверді және ішіндегісінің қауіпсіздігін тексерулер тізбесі

Орындау	Іс-әрекет
	Пошталық серверді инсталляциялау
○	Бөлінген хостыны бағдарламалық қамтуды орнату
○	Ең аз талап етілетін Интернет қызметтерін орнату
○	Пак-қызметтерді және ендігі белгілі осалдықтар түзетуге арналған жаңартуларды орнату
○	Орнатылған, бірақ пошталық серверде пайдаланылмаған барлық қызметтерді жою немесе бұғаттау, (мысалы, пошта Web-ін, қашықтан басқару FTP пайдаланушы)
○	Сервердегі жабдықтаушылардан түскен барлық құжаттаманы жою.
○	Серверге тиісті қауіпсіздік үлгісін қолдану немесе сервердегі скриптты инсталдау
○	SMPT, POP және IMAP қызметтерінің дыбыс беруін бұның пошталық сервер, операциялық жүйе түрі және нұсқасы екені көрінбеуі үшін қайта үйлестіру (қажет болғанда басқаларын да)
○	Қауіпті немесе қажет емес пошталық пәрмендерді бұғаттау (мысалы, VRFY EXPN)
	Операциялық жүйені үйлестіру және пошталық серверге қол жеткізуді басқару
○	Сервер қосымшаларының есептеу ресурстарына қол жеткізуін шектеу
○	Пайдаланушылардың пошталық сервермен орындалатын қол жеткізуді басқарудың қосымша құралдары арқылы қол жеткізуін, егер қажет болса, қол жеткізуді бақылаудың барынша дәл деңгейлерін шектеу
○	Іс-әрекеттер қол жеткізуді шектеуді бақылаумен қатар, тек топтарды бірегейлендіргенде, пайдаланушыны сәйкестендіргенде ғана орындалуы үшін, пошталық сервер қосымшаларын үйлестіру

Орындау	Іс-әрекет
○	Пошталық серверді root құқығымен немесе жүйелік әкімгердің іске қоспағанына көз жеткізу
○	Хосттың операциялық жүйесін осы пошталық сервердің тіркеу файлдарын жаза алатындай, бірақ оларды оқи алмайтындай етіп үйлестіру
○	Хосттың операциялық жүйесін пошталық сервер қосымшалары жасаған уақытша файлдар қол жеткізу үшін шектеліп, қорғалған бағыныңқы директорияның тиісті үлгісінде болатындай етіп үйлестіру
○	Хосттың операциялық жүйесін пошталық сервер қосымшалары жасаған кез келген уақытша файлдарға қол жеткізу, осы файлдар жасайтын пошталық сервер процестерімен шектелетіндей етіп үйлестіру
○	Пошталық сервердің осы серверге бөлінген файлдық құрылымнан тыс файлдарды сақтай алмайтындығына көз жеткізу
○	Пошталық серверді Linux немесе Unix операциялық жүйелерін пайдаланғанда, chroot пәрменіне тыйым сала алатындай етіп үйлестіру
○	Пайдаланушылардың пошта жәшіктерін басқа қатты дискілерге немесе операциялық жүйе мен пошталық сервер қосымшасынан гөрі, қисынды бөлімдерге орнату
○	Тіркеу файлдарының жеткілікті өлшемге ие болатын жерде сақталатындығын анықтаңыз
	Зиян келтіретін салымдармен және ішіндегілерімен күрес
○	Вирустардың орталықтандырылған сканерін орнату (электронды пошта қондырғысында, желіаралық қалқада және (немесе) пошталық серверде)
○	Барлық клиенттік хосттарда вирустар сканерін орнату
○	Барлық сканерлердегі деректердің вирустық базаларын не күн сайын, не вирус жұқтыру байқалғанда жаңарту
○	Пайдаланушыларға вируспен залалданғанда туындайтын қауіптіліктерді және осы қауіптілікті азайту тәсілдерін үйрету
○	Пайдаланушыларды залалдану оқиғасы туралы құлақтандыру
○	Күмәнді хабарламаларды бұғаттау үшін, ішіндегісін сүзуді үйлестіру
○	UCE (Unsolicited Commercial E-mail), яғни спам хабарламаларын бұғаттау үшін, ішіндегісін сүзуді үйлестіру.
○	Егер қажет болса, лексикалық талдауды үйлестіру
○	Сүзудің қосымша саясатын жасау
○	Егер қажет болса, электронды поштаға арналған заңды хабарландыруды қосу
○	Пошталық серверді поштаны ашық көздерден алынған қара тізімдегі мекенжайлардан бұғаттау үшін үйлестіру
○	Егер қажет болса, пошталық серверді поштаны нақты домендерден бұғаттау үшін үйлестіру
○	Толассыз хабар таратуға арналған сервер арқылы поштаны түпнұсқаландыруды үйлестіру
○	Шифрланған түпнұсқаландыруды пайдалану үшін, пошталық серверді үйлестіру
○	Web-ке қол жеткізуді тек SSL/TLS арқылы және егер осындай қол жеткізу қажет болса ғана қолдау үшін, пошталық серверді үйлестіру

D.3 Желі инфрақұрылымын тексеру тізбесі

Орындау	Іс-әрекет
	Желілердің орналасуы
○	Пошталық сервер ішкі желіде орналасуға және пошталық қондырғымен және (немесе) желіаралық қалқамен қорғалуға тиіс немесе пошталық сервер тыйым салынған аймақта орналастырылуға тиіс
	Желіаралық қалқаның пішін үйлесімі
○	Пошталық сервер желіаралық қалқамен қорғалуға тиіс
○	Пошталық серверді, егер оған қауіп төнсе немесе ол барынша осал болса, қосымша деңгейіндегі желіаралық қалқамен қорғау қажет
○	Желіаралық қалқа Интернет пен пошталық сервер арасындағы барлық кестені бақылауға тиіс
○	Желіаралық қалқа, егер қажет болса, 25 TCP (SMPT) портын, 110 TCP (POP3) портын, 143 TCP (MAP) портын, TCP 398 (LDAP) порты мен 636 TCP (қауіпсіз LDAP) портын есептемегенде, пошталық серверге кіретін барлық кестені бұғаттауға тиіс
○	Желіаралық қалқа ((Intrusion-Detection System, IDS)күшпен кіруін байқау жүйесімен бірге) IP мекенжайларды немесе күшпен кірулерді байқау жүйелерінің хабарламасы бойынша бақыланатын желі шабуылға ұшырайтын бағыныңқы жүйелерді бұғаттауға тиіс
○	Желіаралық қалқа желі әкімгерін немесе пошталық сервер әкімгерін күдікті белсенділіктер туралы тиісті құралдар арқылы хабарландыруға тиіс
○	Желіаралық қалқа ішіндегісін (қосымшалар деңгейіндегі желіаралық қалқа) сүзуді қамтамасыз етуі керек
○	Желіаралық қалқаны қызмет көрсетуде істен шығу түріндегі шабуылдарға қарсы қорғалатындай етіп үйлестіру (Denial of Service, DoS)
○	Желіаралық қалқа өте қиын оқиғаларды тіркеуге тиіс
○	Желіаралық қалқа мен операциялық жүйеге пак-қызметтерді орнату және соңғы әрі барынша қауіпсіз деңгейдегі жаңартулар жүргізілуі қажет.
	Күшпен кіруді байқау жүйелері
○	Желілік кестені кез келген желіаралық қалқа немесе маршруттауыш (негізгі желінің) алдында бақылау үшін, IDS үйлестіру
○	Желіаралық қалқадан кейін пошталық серверге кіретін және шығатын желілік кестені бақылау үшін, IDS үйлестіру.
○	Пошталық сервердегі өте қиын файлдардың өзгеруін бақылау үшін, IDS үйлестіру (ішіне салынған құралдармен немесе файлдар бүтіндігін тексеру бағдарламасымен)
○	IDS IP мекенжайларды немесе ұйым желісін шабуылдайтын бағыныңқы жүйелерді бұғаттауға тиіс (желіаралық қалқамен бірге)
○	IDS желілік немесе пошталық әкімгерді тиісті құралдар арқылы шабуылдау арқылы құлақтандыруға тиіс
○	Көшірмеленетін портты анықтау үшін IDS үйлестіру
○	DoS-шабуылдарды байқау үшін IDS үйлестіру
○	Оқиғаларды тіркеу үшін, IDS үйлестіру
○	Мүмкіндігінше, IDS шабуылдардың жаңа сигнатураларымен жиі жаңарту қажет (негізінде апта сайын)

Орындау	Іс-әрекет
○	Пошталық серверге (орналастырылған хостта) қол жеткізетін жүйелік ресурстарды бақылау үшін, IDS үйлестіру
	Желілік жалғауыштар
○	Желілік жалғауыштарды желілік тың тыңдаудан қорғау үшін, пошталық сервер буынтықтарында пайдалану қажет
○	Желілік жалғауыштар ARP хаттамасының ұқсастыруымен және ARP сұранысының нәтижесін ауыстырумен бірге шабуылдардан қорғау үшін, жоғары қорғау режімінде үйлестірілуге тиіс
○	Желілік жалғауыштар IDS хостысы арқылы желі буынтықтарының (базалық желінің) барлық кестесін бағыттау үшін үйлестірілуі керек

D.4 Пошталық клиенттің қауіпсіздігін тексерулер тізбесі

Орындау	Іс-әрекет
	Пак-қызметтерді және пошталық клиенттерге арналған жаңартуларды орнату
○	Пошталық клиентті барынша қауіпсіз нұсқаға дейін жаңартыңыз
○	Пошталық клиентке арналған барлық қажетті пак-қызметтерді қолданыңыз
○	Браузерге арналған барлық қажетті пак-қызметтерді қолданыңыз (браузермен интегралданған пошталық клиенттер үшін (мысалы, Outlook және Netscape)
	Пошталық клиент қауіпсіздігі
○	Операциялық жүйеде пак-қызметтердің орнатылғандығына және барынша қауіпсіз деңгейге дейін жаңартылғандығына көз жеткізіңіз
○	Операциялық жүйені пошталық клиенттің жергілікті сақталған хабарламалары мен пішін үйлесімдері файлдарына тек қана тиісті пайдаланушылардың ғана қол жеткізуіне рұқсат ететіндей етіп үйлестіріңіз
○	Windows скриптарын қауіпсіздендіріңіз немесе жойып жіберіңіз (Windows хосттары үшін)
○	Орындаудан саралауға дейінгі Windows скриптарымен байланысты файлдардың үндемеуі бойынша іс-әрекетті өзгертіңіз (Windows бірге хосттар үшін ғана)
○	Операциялық жүйелердің файлдардың аттарын толық кеңейтіп көрсететіндей етіп үйлестірілгендігіне көз жеткізіңіз (Windows-пен бірге хосттар ғана)
○	Операциялық жүйенің өте қиын құрауыштарының арам ниетті кодтан қорғалғандығына көз жеткізіңіз
○	Пайдаланушының қатты дискісінде жергілікті сақталатын поштаны қорғау үшін файлдарды шифрлау жүйесін пайдаланыңыз (бұл әсіресе, тасымалданатын компьютерлер үшін маңызды)
○	Клиенттік операциялық жүйені автоматтыққа арналып белгіленген кезеңнен кейін, оны бұғаттайтындай етіп үйлестіріңіз

D.5 Пошталық серверді қауіпсіз басқаруды тексерулер тізбесі

Орындау	Іс-әрекет
	Тіркеу
○	IP стегін орнату қателерін тіркеңіз
○	Аттары мен мекенжайларын рұқсат ету проблемаларын тіркеңіз (мысалы, DNS, NIS,WINS)
○	Пошталық серверді үйлестіру қателерін тіркеңіз (мысалы, DNS сәйкес келмеуінен, жергілікті пішін үйлесімі қатесінен, деректер базасында жасырын аттардың болмауынан)
○	Файлдар мен каталогтарға қауіпсіз емес рәміздік және аппараттық байланыстардың қол жеткізуіне рұқсат ететін қолданылмайтын өзгертулерді тіркеңіз
○	Ескірген деректер базасынан жасырын аттардың пайдаланылуын тіркеңіз
○	Жүйелік ресурстар кемшіліктерін тіркеңіз (мысалы, дискілік кеңістік, жады, CPU)
○	Жасырын аттардың деректер базасын қайта құруды тіркеңіз
○	Жүйедегі тіркеулерді тіркеңіз (табысты ма, жоқ па)
○	Қауіпсіздік проблемаларын тіркеңіз (мысалы, спам)
○	Байланыс кемулерін тіркеңіз (желілік проблемалар)
○	Қателер хаттамасын тіркеңіз
○	Байланыс үзілістерін тіркеңіз
○	Байланыстың істен шығуларын тіркеңіз
○	VRFY және EXPN пәрмендерінің пайдаланылуын тіркеңіз
○	Жіберушілердің атын тіркеңіз
○	Жіберу пішіндерін тіркеңіз
○	Файлдар жүктемелерін тіркеңіз
○	Қисынсыз мекенжайларды тіркеңіз
○	Хабарламалар санағын тіркеңіз
○	Қателер туралы хабарламалар жасауды тіркеңіз
○	Сәтсіз жеткізулерді тіркеңіз (ұзақ мерзімді қателер)
○	Кейінге қалдырылған хабарламаларды тіркеңіз (қысқа мерзімді қателер)
○	Хаттамаларды бөлек (syslog) хостта тіркеуді сақтаңыз
○	Хаттамалар тіркеуін ұйымдастырушылық талаптарға сәйкес тіркеуді мұрағаттаңыз
○	Тіркеу файлдарын күнделікті талдаңыз
○	Тіркеу файлдарын апта сайын талдаңыз (барынша ұзақ мерзімді беталыстарды анықтау үшін)
○	Тіркеу файлдарын автоматтандырылған талдауға арналған аспаптар жиынтығын пайдаланыңыз
	Пошталық серверді резервтік көшірмелеу
○	Пошталық серверді резервтік көшірмелеу саясатын әзірлеңіз
○	Пошталық серверді, негізінен апта ағымында күнделікті, инкрементальды резервтік көшірмелеуді іске асырыңыз
○	Пошталық серверді бір ай ішінде апта сайын толық көшірмелеуді негізінен іске асырыңыз

Орындау	Іс-әрекет
○	Резервтік көшірмелерді мерзімінде мұрағаттаңыз
	Беделіне дақ түсіруден кейін қалпына келтіру
○	Ұйымның қауіпсіздік саясатына сәйкес жасаңыз (бұл осы ұсынымдар алдында барынша басымырақ болуға тиіс)
○	Беделіне дақ түсірілген жүйені жүйеден ажыратып, қосымша дәлелдемелерді жинау үшін, шабуыл іздерін сақтау бойынша шаралар қолданыңыз
○	Басқа жүйелердің тойтарысқа ұшырағанын белгілеу үшін, «ұқсас» хосттар туралы мәліметті зерделеңіз
○	Фирма басшылығымен, заңгерлермен және құқық қорғау органдарымен кеңесіңіз (егер сотқа жатады деп ұйғарылса, дереу құқық қорғау органдарына хабарлаңыз)
○	Күшпен кіруді талдаңыз
○	Жүйені қалпына келтіріңіз
○	Жүйені желіге қайтадан қосыңыз
○	Жүйенің қауіпсіздігіне көз жеткізу үшін тестілеңіз
○	Шабуылдаушының тағы да жүйеге немесе желіге қол жеткізуді алуға ұмтылу белгілерін анықтау үшін, жүйе және желі мониторингін өткізіңіз
○	Өткен оқиғалар бойынша құжаттарды зерделеңіз

Е қосымшасы
(анықтамалық)

Web-қызметтерді тексерулер тізбесі

Келесі тексерулер тізбесі Web-серверді жоспарлау, инсталляциялау және қауіпсіз пайдалану үшін арналған [5].

Е.1 Web-сервердің операциялық жүйелерін тексерулер тізбесі

Орындау	Іс-әрекет
	Web-сервердің пішін үйлесімін жоспарлау және өрбіту
○	Web-сервер функцияларын анықтаңыз
○	Web-сервер арқылы жүктелетін, өңделетін және берілетін ақпараттар санаттарын анықтаңыз
○	Ақпарат қауіпсіздігі бойынша талаптарды анықтаңыз
○	Web-серверде ақпараттарды жариялау әдісін анықтаңыз
○	Web-серверді инсталляциялау үшін бөлінген хостты анықтаңыз
○	Web-сервер қарастыратын немесе қолдайтын желілік қызметтерді анықтаңыз
○	Web-серверді пайдаланушылар санаттарын анықтаңыз және пайда-ланушылардың әрбір санатына арналған артықшылықтарды анықтаңыз
○	Web-сервердегі пайдаланушыны түпнұсқаландыру әдістерін анықтаңыз
	Web-серверге арналған операциялық жүйелерді таңдау белгілері
○	Осал жерлерді ашудың ең аз уақыты
○	Әкімшілік немесе түпкілікті деңгейде қызметті тек өкілетті пайдаланушының шектеу қабілеті
○	Сервердегі ақпаратқа қол жеткізуге, оның тағайындалғандардан басқалардың барлығына тыйым салу қабілеті
○	Операциялық жүйенің ішіне немесе сервердің бағдарламалық қамтуына салынуы мүмкін, міндетті емес желілік қызметтерді бұғаттау қабілеті
○	Сақтандырудың қолайлы шығындары мен жауапкершіліктері (кейбір операциялық жүйелер үшін сақтандыру шығындарын көбейту қажет)
○	Операциялық жүйені орнататын, үйлестіретін, қауіпсіздендіретін және тіркеп жіберетін тәжірибелі қызметкерлер құрамының болуы.
	Операциялық жүйеге арналған патчалар мен жаңартуларды орнату
○	Операциялық жүйеге арналған барлық қажетті патчалар мен жаңартуларды анықтаңыз және орнатыңыз
○	Операциялық жүйеге қосылған қосымшалар мен қызметтер үшін қажетті барлық патчалар мен жаңартуларды анықтап орнатыңыз
○	Міндетті емес қызмет көрсетулер мен қосымшаларды жойыңыз немесе бұғаттаңыз
○	Операциялық жүйе пайдаланушысын түпнұсқаландыруды үйлестіріңіз
○	Қажет емес есептік жазбалар мен үндемеу бойынша меңгерілген топтарды жойыңыз немесе бұғаттаңыз
○	Белсенді емес есептік жазбаларды бұғаттаңыз
○	Нақты компьютер үшін пайдаланушылар тобын құрыңыз
○	Нақты компьютер үшін пайдаланушылардың есептік жазбаларын жасаңыз

Орындау	Іс-әрекет
○	Құпия белгілерді ұйымдастыру саясатын тексеріңіз (мысалы: ұзындығы, күрделілігі) және тиісті құпия белгілерді орнатыңыз
○	Компьютерге сәтсіз әрекеттердің шектеулі санынан кейін тыйым салу үшін үйлестіру
○	Түпнұсқаландыруды күшейту үшін, басқа қауіпсіздік механизмдерін орнатып үйлестіріңіз
	Операциялық жүйе қауіпсіздігін тексерулер
○	Осал жерлерін анықтау үшін, инсталляциядан соң операциялық жүйені тестілеңіз
○	Осал жерлерді жаңадан анықтау үшін, операциялық жүйені мерзімімен тестілеуді өткізіңіз (мысалы: тоқсан сайын)

Е.2 Web-серверді қауіпсіз орнату және үйлестіру бойынша іс-әрекеттер тізбесі

Орындау	Іс-әрекет
	Web-серверді қауіпсіз орнату
○	Сервердің бағдарламалық қамтуын бөлек хостта орнатыңыз
○	Интернеттің ең аз қажет етілетін қызмет көрсетулерін орнатыңыз
○	Белгілі осал жерлерді түзету үшін, патчаларды немесе жаңартуларды орнатыңыз
○	Web ішіндегісі үшін физикалық дискіні немесе қисынды бөлімді арнайы бөліңіз (операциялық жүйе мен сервер қосымшаларынан бөліп алыңыз)
○	Web-сервермен орнатылған, бірақ қажет болмайтын барлық қызмет көрсетулерді жойыңыз немесе бұғаттаңыз (мысалы, gopher, FTP және қашықтан басқару)
○	Құжаттардың барлық үлгілерін, скриптарды (макростар) және орындалатын кодты жойыңыз
○	Серверден жабдықтаушылардың барлық құжаттарын жойыңыз
○	Қолайлы қауіпсіздік үлгісін қолданыңыз немесе қажетті скриптарды (макростарды) инсталдаңыз
○	Бұның Web-сервер екенін, операциялық жүйе түрі мен нұсқасын хабарламау үшін, HTTP қызметінің (егер қажет болса, басқаларды да) тақырыбын қайта үйлестіріңіз
	Web-сервер хостының операциялық жүйесіне қол жеткізуді басқаруды үйлестіру
○	Web-тегі файлдардың ішіндегісін оқуға болатындай, бірақ Web-сервер процестері қызметтерінің көмегімен жазбайтындай етіп үйлестіріңіз
○	Web-сервердің қызмет көрсететін процестері каталогтарға ашық Web ішіндегісі сақталатын каталогтарды жаза алмайтындай етіп үйлестіріңіз
○	Web-серверді басқару үшін сенім көрсетілген процестер ғана, Web ішіндегі файлдарды жаза алатындай етіп үйлестіріңіз
○	Web қосымшасы Web-сервердің тіркелген файлдарын жаза алатындай, бірақ тіркеу файлдарын Web-сервер қосымшасы оқи алмайтындай етіп үйлестіріңіз
○	Web-сервердің қосымшалары жасаған уақытша файлдарды белгілі бір және сәйкесінше қорғалған шағын каталогтарға топтандырылатындай етіп үйлестіріңіз

Орындау	Іс-әрекет
○	Web-сервер қосымшалары жасаған уақытша файлдардың кез келгеніне қол жеткізу үшін,осы файлдар жасаған Web қызметінің процестерімен шектелетіндей етіп үйлестіріңіз
○	Web ішіндегісін Web операциялық жүйесі мен қосымшасынан гөрі, басқа жинақтаушыға (қатты дискіге немесе қисынды бөлімге) орнатыңыз
○	Егер Web серверіне жүктеуге рұқсат етілсе, осы мақсат үшін бөлінген қатты дискінің тиісті шектелген кеңістігі болатындай етіп үйлестіріңіз
○	Тіркеу файлдарының жеткілікті өлшемге ие болатын орында сақталатындығына көз жеткізіңіз
	Web ішіндегісіне арналған қауіпсіз каталогтың пішін үйлесімі
○	Қатты дискіде жеке жинақтауыш немесе Web үшін қисынды бөлім бөліңіз және кестені қосып, бірақ скриптар мен басқа бағдарламалардан басқа, Web серверге арналған шағын каталогтармен байланысқан бірыңғай файлдарды орнатыңыз
○	Web-сервердің ішіндегісінің бөлігі ретінде орындалатын, барлық сыртқы скриптар немесе бағдарламалар үшін ғана жеке каталог бөліңіз (мысалы, CGI, ASP)
○	Әкімшілік есептік жазба басқаруымен ғана болатын скриптардың орындалуын бұғаттаңыз. Бұл әрекет авторластыру скриптары болатын жеке каталогқа қол жеткізуді жасау және басқару үшін орындалады
○	Компьютер үшін пайдаланушылар тобын құрыңыз
○	Аппаратураға немесе рәміздерге қысқа байланыстарды пайдалануды бұғаттаңыз (Windows жапсырмалары сияқтыларды).
○	Web-ке қол жеткізудің толық үлгісін анықтаңыз. Барлық бумаларды анықтаңыз және Web сервер шегінде қандай құжаттардың қол жеткізу бойынша шектелетіні, қандайы (және кімге) қолжетімді болатындығын белгілеңіз
○	Ұйымның құпия белгілер саясатын тексеріңіз (мысалы: ұзындығы, күрделілігі) және тиісті құпия белгілерді орнатыңыз
○	Егер мүмкін болса, robots.txt файлын пайдаланыңыз
	Файлдың бүтіндігін тексерулерді пайдалану
○	Web-сервер пішін үйлесімдерінің файлдарын, Web құпия белгілер файлдары мен ішіндегісін қорғау үшін, файлдардың бүтіндігін тексеруді белгілеңіз
○	Файлдар бүтіндігін тексеру жиынтықтарын ішіндегісін жақсартқан немесе өзгерткен кезде, әр жолы жаңартыңыз
○	Тексеру жиынтығын жазбадан қорғалған тасушыда сақтаңыз
○	Тексеру жиынтықтарын уақытылы салыстырып отырыңыз

Е.3 Web ішіндегісін тексерулер тізбесі

Орындау	Іс-әрекет
	Ақпараттың келесі түрінің ешқайсысына немесе ашық Web-сервер арқылы қол жеткізілмейтіндігіне көз жеткізіңіз
○	Құпия немесе өте қиын жазбалар
○	Қызметкерлер құрамына арналған ішкі ережелер мен шаралар
○	Құпия немесе жеке ақпарат
○	Тергеу жүргізу жазбалары

Орындау	Іс-әрекет
○	Қаржылық жазбалар (ендігі жарияланғандардан басқа)
○	Физикалық және ақпараттық қауіпсіздікті ұйымдастыру шаралары
○	Ақпараттық жүйе желілері мен инфрақұрылымын ұйымдастыру туралы ақпарат
○	Меншік иесінің жазбаша рұқсатынсыз, авторлық құқықпен қорғалатын материал
○	Қауіпсіздік шараларының түрлерін орнында көрсететін құпиялар немесе қауіпсіздік саясаты
	Жалпы қолжетімді Web ішіндегісін құптауға арналған жалпы ұйымдастырылып тіркелген, формальды саясатты орнатыңыз
○	Web-те жариялануға тиіс ақпаратты анықтаңыз
○	Белгілі мақсатқа арналған аудиторияны анықтаңыз
○	Ақпаратты жариялаудың ықтимал теріс нәтижелерін анықтаңыз
○	Осы нақты ақпаратты жасауға және жариялауға кімнің жауапты болатындығын анықтаңыз
○	Web-те жариялау үшін пайдаланылатын мәнерлер мен пішіндерге арналған басты ұстанымдарды анықтаңыз
○	Өте қиын деректерді басқару және оларды тарату/жариялау бойынша ақпаратты қолайлы қарауды қамтамасыз етіңіз (өте қиын ақпаратты қоса алғанда)
○	Қол жеткізу және қауіпсіздікті басқару ережесін анықтаңыз
○	Web ішіндегісінің шығыс коды ішінде болатын ақпарат бойынша басшылықты құрыңыз
	Web пайдаланушысына арналған құпиялылық бойынша түсініктер
○	Жарияланған құпиялылық саясаты
○	Пайдаланушының анық рұқсатынсыз, жеке деректер жинауға тыйым салу
○	"Тұрақты" Куки-файлдарды (ағылшынша cookies) пайдалануға тыйым салу
○	Егер сеанстық куки-файлдар пайдаланылса, олар жарияланған құпиялылық саясатында айқын анықталуға тиіс
	Клиент жағындағы белсенді құрамның қауіпсіздігін қамтамасыз ету бойынша түсініктер
○	Оны тек бұл өте қажет болғанда ғана пайдаланыңыз
○	Үндемеу бойынша әрекеттерді пайдаланушының арнайы рұқсатынсыз пайдаланбаңыз
○	Клиент жағындағы өте жоғары қауіпті белсенді құрамды пайдаланбаңыз
○	Баламалары мүмкін болғанда, оларды пайдаланыңыз (мысалы: PDF пішінімен қатар қарапайым мәтінді)
	Сервер жағындағы белсенді құрамның қауіпсіздігін қамтамсыз ету бойынша түсініктер
○	Коды түсінуде қарапайымдылыққа және тиімділікке ұмтылыңыз
○	Файлдарды оқу және жазу бойынша шектеулер енгізіңіз
○	Басқа бағдарламалармен өзара қатынасты шектеңіз немесе болдырмаңыз (мысалы, sendmail)
○	«Suid» пайдаланушысының артықшылықтарымен жұмысты пайдаланбаңыз

Орындау	Іс-әрекет
○	Анық берілген жол аттарын пайдаланыңыз (яғни, жолдың аты ауыстырылады деп есептемеңіз)
○	Жазу және орындау артықшылықтарымен болатын каталогтарды болдырмаңыз
○	Орындалатын барлық файлдарды жеке бумаларға салыңыз
○	SSI-ді бұғаттаңыз
○	Пайдаланушыны енгізетіннің бәрін тексеріңіз
○	Динамикалық жасалған беттер қауіпті метарәміздер тудырмауға тиіс
○	Кодтау рәміздерінің жиынтығы әрбір бет үшін анық белгіленуге тиіс
○	Пайдаланушы деректері кодтаудың осы сұлбасына арналған арнайы рәміздеріне тиісті байттық бірізділіктердің болуымен көшірмеленуге тиіс
○	Куктар кез келген арнайы рәміздердің болуымен зерделенуі керек
○	Шифрлау механизмін скриптардың үлгілері арқылы енгізілген құпия белгілерді шифрлау үшін пайдаланыңыз
○	Пайдаланушының атымен және құпия белгісімен шектелген Web қосымшалары үшін, қосымшадағы Web беттерінің ешқайсысы кіруді тіркеудің тиісті процесі арқылы өтпейінше, қолжетімді болуға тиісті емес
○	Скриптардың барлық үлгілерін жойыңыз
○	Үшінші тараптың ешқандай скриптары немесе орындалатын коды шығыс кодты тексермей қолданылмауға тиіс

Е.4 Web-түпнұсқаландыру және шифрлау технологиясын тексерулер тізбесі

Орындау	Іс-әрекет
	Web-түпнұсқаландыру және шифрлау технологиясы
○	Ең аз қорғауды қажет ететін және шағын, айқын анықталған аудиториясы бар Web ресурстары үшін, мекенжайға негізделген түпнұсқаландыруды үйлестіріңіз
○	Қосымша қорғауды қажет ететін, бірақ шағын, айқын анықталған аудиториясы бар Web ресурстары үшін, қорғаудың екінші желісі сияқты мекенжайға негізделген түпнұсқаландыруды үйлестіріңіз
○	Ең аз қорғауды қажет ететін, бірақ айқын анықталған аудиториясы жоқ Web ресурстары үшін, негізгі немесе жеке (дұрысырақ) түпнұсқаландыруды үйлестіріңіз
○	Іздестіру жүйелерінің арам ниетті роботтарынан қорғауды қажет ететін Web ресурастары үшін, негізгі немесе жеке (дұрысырақ) түпнұсқаландыруды үйлестіріңіз
○	Ең көп қорғауды қажет ететін Web ресурстары үшін, SSL/TLS үйлестіріңіз
	SSL/TLS құрама пішіні
○	Ең аз түпнұсқаландыруды қажет ететін, бірақ шифрлауды қажет ететін пішін үйлесімдері үшін, меншікті сертификат пайдаланылады
○	Серверде түпнұсқаландыру мен шифрлауды қажет ететін пішін үйлесімдері үшін, үшінші тарап шығарған сертификат пайдаланылады

Орындау	Іс-әрекет
○	Клиентті орташа деңгейде түпнұсқаландыруды қажет ететін пішін үйлесімдері үшін, серверді пайдаланушының атын және SSL/TLS арқылы құпия белгіні сұрайтындай етіп үйлестіріңіз
○	Клиентті жоғары деңгейде түпнұсқаландыруды қажет ететін пішін үйлесімдері үшін, серверді клиенттің сертификатын SSL/TLS арқылы сұрайтындай етіп үйлестіріңіз
○	Орташа шифрлау деңгейін қажет ететін ұйымдар үшін, DES пайдалануға болады
○	Жоғары шифрлау деңгейі қажет болатын ұйымдар үшін, RC4 (жоғары) немесе 3DES (өте жоғары) пайдалану қажет
○	Web-сервер сертификатын бақылау үшін, файлдар бүтіндігін тексеруді үйлестіріңіз
○	Егер Web-серверде тек SSL/TLS ғана пайдаланылуға тиіс болса, қол жеткізудің 80 TCP порты арқылы бұғатталатындығына көз жеткізіңіз
○	Егер кестенің Web-сервердегі ең көп бөлігі кодталған SSL/TLS арқылы өтетін болса, Web-серверде тиісті тіркеу механизмінің қолданылатындығына көз жеткізіңіз (кодталған SSL/TLS сеанстарына қарсы желілік қамтудың нәтижесіз болатындығынан)

Е.5 Желі инфрақұрылымын тексеру тізбесі

Орындау	Іс-әрекет
	Желіні орналастыру
○	Web-сервер ТСА-ға немесе одан тысқары орналастырылуға тиіс, бұл жағдайда оның желіаралық қалқамен қорғалуы керек
○	ТСА желіаралық қалқаның үшінші (немесе одан көп) интерфейсіне қосылмауға тиіс
	Желіаралық қалқаның пішім үйлесімі
○	Web-сервер желіаралық қалқамен қорғалған
○	Web-сервер, егер барынша жрғары қатерге кез болса немесе ол барынша осал болса, қолданбалы деңгейдегі желіаралық қалқамен қорғалған
○	Желіаралық қалқа Интернет және Web-сервер арасындағы барлық кестені бақылайды
○	Желіаралық қалқа 80 TCP (http) порты және (немесе) 443 (HTTPS) басқа, Web-сервердегі барлық кіретін кестені бұғаттайды
○	Желіаралық қалқа жеке IP мекенжайларын немесе IDS одан ұйым желісі шабуылдайтынын хабарлайтын бағыныңқы жүйелерін бұғаттайды (IDS-пен бірге)
○	Желіаралық қалқа желі немесе Web әкімгерін күдікті белсенділік туралы хабарландырады
○	Желіаралық қалқа ішіндегісін сүзуді қамтамасыз етеді
○	Желіаралық қалқа қызмет көрсетулерді шабуылдан қорғау үшін үйлестірілген
○	Желіаралық қалқа URL сұраныстарындағы бұзылған немесе белгілі шабуылдарды табады
○	Желіаралық қалқа өте қиын оқиғаларды тіркейді

Орындау	Іс-әрекет
○	Желіаралық қалқа және оның операциялық жүйелері ең жаңа нұсқаға немесе барынша қауіпсіз деңгейге дейін жаңартылған
	Күшпен кіруді байқау жүйелері (IDS)
○	Хостта орналастырылған IDS, SSL/TLS артық жұмыс істейтін Web-серверлер үшін пайдаланылады
○	IDS-ті кез келген желіаралық қалқа немесе маршруттауыш сүзгі алдында желілік кесте бақылай алатындай етіп үйлестіріңіз (желі негізінде)
○	IDS-ті желіаралық қалқадан кейін, Web-серверге және одан кейін желілік кесте бақылай алатындай етіп үйлестіріңіз
○	IDS-ті Web-сервердегі өте қиын файлдардағы өзгерістерді тексере алатындай етіп үйлестіріңіз (ішіне салынған құралдармен немесе файлдардың бүтіндігін тексеру бағдарламасымен)
○	IDS желіаралық қалқамен бірге, жеке IP мекенжайларын немесе ұйым желісін шабуылдайтын бағыныңқы желілер арқылы бұғаттайды
○	IDS шабуыл туралы желілік немесе Web-әкімгерді хабарландырады
○	IDS-ті порттарды көшірмелеу әрекеттерін байқайтындай етіп үйлестіріңіз
○	IDS-ті DoS шабуылдарды байқайтындай етіп үйлестіріңіз
○	IDS-ті URL қалыпты құрылымның бұзылған сұранымдарын байқайтындай етіп үйлестіріңіз
○	IDS-ті оқиғаларды тіркеу үшін үйлестіріңіз
○	IDS-ті жаңа шабуыл сигнатураларымен жиірек жаңартыңыз (апта сайын жаңарту ұсынылады)
○	IDS-ті Web-сервердің хостында қол жеткізілетін жүйелік ресурстарын бақылау үшін үйлестіріңіз (хостта)
	Желілік маршруттауыштар
○	Желілік маршруттауыштар Web-сервердің желілік буынтығында желілік тың тыңдаудан қорғау үшін пайдаланылады
○	Желілік маршруттауыштарды жоғары қауіпсіздік режімінде ARP және жарамсыз ARP ауыстыруды ұқсастыратын шабуылдарды бейтараптандыру үшін үйлестіріңіз
○	Желілік маршруттауыштарды барлық желілік кестені IDS хосты арқылы бағыттайтындай етіп үйлестіріңіз (желі негізін)

Е.6 Web-серверді қауіпсіз басқаруды тексерулер тізбесі

Орындау	Іс-әрекет
	Тіркеу
○	Берілімдер тіркеуін сақтау үшін, құрамдастырылған пішінді пайдаланыңыз немесе ақпараттың берілімдерді тіркеуге арналған стандарт пішін болып табылатын, тіркеудің құрамдастырылған пішіні болып сипатталатындай етіп қолдан үйлестіріңіз
○	Егер құрамдастырылған тіркеу пішінін пайдалану мүмкін болмаса, тіркеуді өңдеушінің немесе тіркеу агентінің жұмысына рұқсат етіңіз
○	Жалғыз физикалық Web-сервердің бөлігі болуы мүмкін әртүрлі виртуал Web-сайттарды тіркеу файлдары үшін, әртүрлі аттарды белгілеңіз
○	Пайдаланушыны қашықтан сәйкестендіруді [14] анықталғандай етіп пайдаланыңыз

Орындау	Іс-әрекет
○	Тіркеуді бөлек хостта сақтаңыз
○	Тіркеу файлдарын ұйым ережесіне сәйкес мұрағаттаңыз
○	Тіркеу файлдарын күнделікті талдаңыз
○	Тіркеу файлдарын апта сайын талдаңыз (барынша ұзақ мерзімді бағыттарды анықтау үшін)
○	Тіркеу файлдарын талдауды автоматтандыруға арналған арнайы құралдар жиынтығын пайдаланыңыз
	Web-сервердің резервтік көшірмелеуі
○	Web-сервердің резервтік көшірмелеу саясатын әзірлеңіз
○	Web-сервердің инкрементальды резервтік көшірмесін апта ішінде күнделікті жасаңыз
○	Web-сервердің толық резервтік көшірмесін бір ай мерзімде апта сайын жасаңыз
○	Көшірмелерді мезгілімен мұрағаттаңыз
○	Web-сайттың (тар) негізгі көшірмесін алыңыз
	Беделіне дақ түсіруден кейін қалпына келтірілген
○	Ұйымның қауіпсіздік саясатына жүгініңіз (ол осында берілген ұсынымдардан артығырақ болуға тиіс)
○	Беделіне дақ түсірілген жүйелерді желіден ажыратыңыз немесе бұл қосымша дәлелдер жинауға көмектесетіндіктен, шабуылдар ізін сақтау бойынша шаралар қолданыңыз
○	Басқа жүйелердің шабуылға ұшырағанын белгілеу үшін, «ұқсас» хостар туралы мәліметтерді зерделеңіз
○	Ұйым басшылығымен, заңгерлермен және құқық қорғау органдарымен кеңесіңіз (егер сотқа тартылады деп болжанса, дереу құқық қорғау органдарымен байланысыңыз)
○	Күшпен кіруді талдаңыз
○	Жүйені қалпына келтіріңіз
○	Жүйені желіге қосыңыз
○	Жүйенің қауіпсіздігіне көз жеткізу үшін, оны тестілеңіз
○	Шабуылдаушының жүйеге немесе желіге тағы да қол жеткізгісі келетін белгілерін анықтау үшін, жүйе және желі мониторингін өткізіңіз
○	Өткен оқиғалар бойынша құжаттарды зерделеңіз
	Қауіпсіздікті тексеру
○	Web-сервердегі және қолдайтын желідегі осал жерлерді мерзімімен көшірмелеңіз
○	Тестілеуді бастағанға дейін, осалдықтарды іздеу сканерін жаңартыңыз
○	Осалдықтарды іздейтін сканермен табылған кез келген кемшіліктерді жойыңыз
	Қашықтан басқару және ішіндегісін жаңарту
○	Түпнұсқаландырудың күшті механизмін пайдаланыңыз (мысалы, кілттер жұбын - ашық/жеке, қос әсерлі түпнұсқаландыруды)
○	Нақты IP мекенжайлары мен ішкі желілері бар Web-сервер ішіндегісін қашықтан басқару немесе түрлендіру үшін пайдаланылуы мүмкін хосттарды шектеңіз
○	Қауіпсіз хаттамаларды пайдаланыңыз (мысалы, қауіпсіз қабықты, HTTPS)

Орындау	Іс-әрекет
○	Тұжырымдамада ішіндегісін қашықтан басқару мен жаңартуда аздаған артықшылықтарды қабылдауға көндіріңіз (яғни, есептік жазбаларды қашықтан басқару/жаңарту үшін, қол жеткізу құқығын барынша азайтуға тырысыңыз)
○	Утилиталарды немесе қашықтан басқаруға арналған қосымшаларды пайдаланғанда, үндемеу бойынша ішіне салынған барлық есептік жазбаларды немесе құпия белгілерді өзгертіңіз
○	Интернеттен немесе желіаралық қалқа арқылы қашықтан басқаруға жол бермеңіз
○	Web-сервер үшін немесе керісінше, ішкі желіден алынатын файлдарды жалпы қолжетімді жасамаңыз

F қосымшасы
(анықтамалық)

Сымсыз ЛВС қауіпсіздігін тексерулер тізбесі

Орындау	Іс-әрекет
○	Ұйымның сымсыз технологияны пайдалануға бағытталған қауіпсіздік саясатын әзірлеңіз
○	Желідегі пайдаланушылардың компьютер қауіпсіздігі ережесі туралы толық хабардар екендігіне көз жеткізіңіз
○	Қорғауды қажет ететін ұйым қаупінің шамасын түсіне отырып, қауіпті бағалауды орындау
○	NIC және IP клиентін ішіне салынған бағдарламалық қамтудың соңғы қолжетімді деңгейге дейін жаңартылғанына (сатып алғанға дейін) көз жеткізіңіз
○	Сымсыз желінің ағымдағы қауіпсіз жай-күйін (сымсыз ЛВС 802.11 хаттамасына қол жеткізудің тіркелмеген нүктелерінің болмауы туралы растауды қоса алғанда) толық түсіну үшін, жан-жақты қауіпсіздік бағалауын жүйелі орындаңыз
○	Ғимараттың немесе ұйым құрылымының периметрі бойынша ішкі шекараны қорғау болатындығына көз жеткізіңіз
○	Ұйымның сымсыз желісін жабу аймағын өлшеу және белгілеу үшін, орталықтандырылған зерттеу жүргізіңіз
○	802.11 желісінің және қол жеткізу нүктелерінің барлық жабдықтарын толық түгендеуді өткізіңіз
○	Тәжірибелі жолмен сымсыз қамту шекараларын дәл анықтау үшін, қол жеткізу нүктелерін алып тастау шекараларын тексеріңіз
○	Ықтимал кедергілердің алдын алу үшін, кез келген басқа көрші сымсыз желілерден жиілігі бойынша қол жеткізу арналарының өзгеше болуын тексеріңіз (кем дегенде бес арнаны)
○	Құрылым ішіндегі қол жеткізу нүктелерін сыртқы қабырғалар мен терезелерден аулақ орналастырыңыз
○	Қол жеткізу нүктесінің орналасу орны авторластырылмаған физикалық қол жеткізуді және пайдаланушылардың айла-амалдарын болдырмас үшін, қорғалған аумақтарда болуға тиіс
○	Қол жеткізу нүктелерінің олар пайдаланбайтын уақыт мерзімінде сөндірілгендігіне көз жеткізіңіз
○	Қол жеткізу нүктелеріндегі түсіру қызметтерінің қажет болғанда ғана және тек қызметкерлердің өкілетті топтары ғана пайдалана алатындығына көз жеткізіңіз
○	Қол жеткізу нүктелерін реттеулерді, егер түсіру функциясы пайдаланылса, қауіпсіздіктің соңғы параметрлеріне келтіріңіз
○	Қол жеткізу нүктесіндегі ішіне салынған SSID ойлап табуға қиын мәнге өзгертіңіз
○	"Кең таратылатын SSID берілімне" SSID клиенті қол жеткізудің жіберілген нүктесіне дәл сәйкес келуі үшін тыйым салыңыз

Орындау	Іс-әрекет
○	Рәміздік SSID жолында ұйым атының (бөлімше, бөлім, көше және т.с.с.) немесе өнім атауының болмауын тексеріңіз
○	Қол жеткізу нүктелерінің кең таратылатын маягына тыйым салыңыз
○	Үндемеу бойынша ішіне салынған барлық параметрлердің өзгергендігін тексеріп, көз жеткізіңіз
○	Қол жеткізу нүктелеріндегі барлық қауіпті және мәнсіз хаттамаларды бұғаттаңыз
○	Шифрланған түпнұсқаландыруды және WEP/WPA мүмкіндіктерін қоса алғандағы, сымсыз ЛВС өнімінің барлық қауіпсіздік функцияларын кірістіріңіз
○	Шифрлау кілтінің ұзындығының 128 биттен кем еместігіне көз жеткізіңіз
○	Құпия кілттердің мезгіл-мезгіл барынша қауіпсіз бірегей кілттерге ауыстырылатындығына көз жеткізіңіз
○	Өткізгіш инфрақұрылым мен сымсыз желі арасында дұрыс үйлестірілген желіаралық қалқа орнатыңыз (қол жеткізу нүктелерінде немесе қол жеткізу нүктелерінің HUB)
○	Барлық сымсыз клиенттерге вирусқа қарсы бағдарламалық қамту мен дербес желіаралық қалқа орнатыңыз
○	MAC-мекенжайлар бойынша қол жеткізуді басқару тізімдерін пайдаланыңыз
○	Сымсыз коммуникациялар үшін, IPsec негізделетін виртуал жабық желі (VPN) технологиясын пайдаланыңыз
○	Пайдаланатын шифрлаудың желі өткізгіштігі мен компьютерлер процессорларының жылдамдығы қаншалықты мүмкіндік берсе, соншалықты күшті екендігіне көз жеткізіңіз
○	Қол жеткізудің барлық нүктелерінің күшті басқару құпия белгілерінің барлығына және барлық құпия белгілердің уақытылы өзгеретіндігіне көз жеткізіңіз
○	802.11 арналған «ad hoc (қалай бар)» режімінің бұғатталғандығына көз жеткізіңіз
○	Мүмкіндігінше, желідегі статикалық IP мекенжайларды пайдаланыңыз
○	DHCP "клиентті резервте ұстау" функциясымен бірге пайдаланыңыз
○	Қол жеткізу нүктелерін басқару интерфейстері үшін, пайдаланушыны түпнұсқаландыру механизмдерін кірістіріңіз
○	Қол жеткізу нүктелеріне арналған кестенің бөлініп қорғалған, өткізгіш бағыныңқы желіде болатындығына көз жеткізіңіз

Қосымша
(анықтамалық)

Библиография

[1] ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security —Part 4: Selection of safeguards

[2] ISO/IEC TR 13335-5:2001, Information technology — Guidelines for the management of IT Security —Part 5: Management guidance on network security

[3] ISO/IEC 17799:2000, Information technology — Code of practice for information security management

[4] ISO/IEC 18033-3, IT security techniques — Encryption algorithms — Part 3: Block ciphers7)

[5] NIST Special Publication 800-44: 2002 Guidelines on Securing Public Web Servers

[6] NIST Special Publication 800-45: 2002 Guidelines on Electronic Mail Security

[7] NIST Special Publication 800-46: 2002 Security for Telecommuting and Broadband Communications

[8] NIST Special Publication 800-48: 2002 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices

[9] IETF RFC 768 User Datagram Protocol (1980)

[10] IETF RFC 821 Simple Mail Transfer Protocol (1982)

[11] IETF RFC 959 File Transfer Protocol (1985)

[12] IETF RFC 1055 Nonstandard for transmission of IP datagrams over serial lines: SLIP (1988)

[13] IETF RFC 1334 PPP Authentication Protocol (1992)

[14] IETF RFC 1413 Identification Protocol (1993)

[15] IETF RFC 1939 Post Office Protocol – Version 3 (1996)

[16] IETF RFC 1991 PGP Message Exchange Formats (1996)

[17] IETF RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP) (1996)

[18] IETF RFC 2045 to IETF RFC 2049 Multipurpose Internet Mail Extensions (MIME) (1996)

[19] IETF RFC 2060 Internet Message Access Protocol - Version 4rev1 (1996)

[20] IETF RFC 2131 Dynamic Host Configuration Protocol (1997)

[21] IETF RFC 2139 RADIUS Accounting (1997)

[22] IETF RFC 2246 The TLS Protocol Version 1.0 (1999)

[23] IETF RFC 2284 PPP Extensible Authentication Protocol (EAP) (1998)

[24] IETF RFC 2401 Security Architecture for the Internet Protocol (1998)

[25] IETF RFC 2406 IP Encapsulating Security Payload (ESP) (1998)

[26] IETF RFC 2440 Open PGP Message Format (1998)

[27] IETF RFC 2631 Diffie-Hellman Key Agreement Method (1999)

[28] IETF RFC 2632 S/MIME Version 3 Certificate Handling (1999)

[29] IETF RFC 2633 S/MIME Version 3 Message Specification (1999)

[30] IETF RFC 2865 Remote Authentication Dial In User Service (RADIUS) (2000)

[31] IETF RFC 3162 RADIUS and IPv6 (2001)

[32] IETF RFC 3369 Cryptographic Message Syntax (CMS) (2002)

[33] IETF RFC 3370 Cryptographic Message Syntax (CMS) Algorithms (2002)

ӘОЖ 681.3 **МСЖ** 35.040

Түйінді сөздер: ақпараттық технологиялар, алыс жерден қол жеткізу, қорғалатын ақпарат, түпнұсқаландыру, қол жеткізуді басқару, қол жеткізу нүктесі, жергілікті желі

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Технологии информационные

Методы обеспечения защиты
ЗАЩИТА СЕТИ Информационных технологий

Часть 4
Защита удалённого доступа

СТ РК ИСО/МЭК 18028 – 4 - 2007
ISO/IEC 18028-4:2005(E) Information technology Security techniques.
It network security. Part 4. Securing remote access (IDT)

Издание официальное

Комитет по техническому регулированию и метрологии
Министерства индустрии и торговли Республики Казахстан
(Госстандарт)

Астана

Предисловие

1 ПОДГОТОВЛЕН И ВНЕСЕН ТОО «Специальное конструкторско-технологическое бюро «Гранит» на основе собственного аутентичного перевода стандарта, указанного в пункте 3.

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ приказом председателя Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 24 декабря 2007 г. № 691

3 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 18028-4:2005(E) «Информационная технология. Методы защиты. Защита сети ИТ. Часть 4. Защита удаленного доступа». (ISO/IEC 18028-4:2005(E) «Information technology. Security techniques. IT network security. Part 4. Securing remote access»)

4 Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с СТ РК 1.5-2004 «Общие требования к построению, изложению, оформлению и содержанию стандартов»

5 В настоящем стандарте реализованы нормы законов Республики Казахстан О техническом регулировании от 09.11.2004 г. № 603-II, О национальной безопасности от 26.06.98г. № 233-I, О языках в Республике Казахстан от 11.07.97 г. № 151-I

6 СРОК ПЕРВОЙ ПРОВЕРКИ 2012 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

7 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Нормативные документы по стандартизации», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Нормативные документы по стандартизации». В случае пересмотра (изменения, замены) или отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячно издаваемом информационном указателе «Нормативные документы по стандартизации»

Содержание

Введение

В Информационных технологиях (ИТ) увеличивается потребность в использовании сетей как в пределах организаций, так и между организациями. Для безопасного использования сетей необходимо выполнять определенные требования.

Область удаленного доступа к сети требует применения специальных мер, чтобы обеспечить безопасность ИТ. Настоящий стандарт содержит руководство по обеспечению защищенного удаленного доступа к сетям, при использовании электронной почты, передачи файлов или просто при удаленной работе.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Технологии информационные

МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ. ЗАЩИТА СЕТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 4
Защита удалённого доступа

Information technology. Security techniques. IT network security. Part 4. Securing remote access.

Дата введения 2009.01.01

1 Область применения

Настоящий стандарт содержит рекомендации по безопасному использованию удалённого доступа – метода дистанционного соединения компьютера с другим компьютером или с сетью через сеть общего пользования, например Интернет, а также сведения о влиянии этого метода на безопасность ИТ. В данной части стандарта обсуждаются различные типы удалённого доступа, в том числе, используемые протоколы, вопросы аутентификации, относящиеся к удалённому доступу, а также содержится сопутствующая информация о способах безопасной установки удалённого доступа. Данная часть стандарта предназначена для помощи администраторам сетей и инженерам, которые планируют использовать этот вид соединения или уже используют его и нуждаются в совете, как установить его безопасно и работать с ним.

2 Термины, определения и сокращения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1 **Точка доступа;** AP (Access Point)**:** Система, обеспечивающая доступ из беспроводной сети к наземной сети.

2.2 **Расширенный стандарт шифрования;** AES (Advanced Encryption Standard): Симметричный механизм шифрования, использующий ключ переменной длины, позволяющий эффективную реализацию Федерального Стандарта по Обработке Информации 197 (Federal Information Processing Standard 197; FIPS 197).

2.3 **Аутентификация** (authentication): Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. При необходимости аутентификации пользователи распознаются по известному признаку (например, паролю), или по владению (например, токеном (знаком, символом), или по персональному признаку (биометрической характеристике). Строгая аутентификация основывается на точном механизме (биометрической характеристике), или на использовании, по меньшей мере, двух из приведённых факторов (так называемая много-факторная аутентификация).

Издание официальное

2.4 **Обратный вызов** (call-back)**:** Механизм вызова предварительно определённого или предложенного места (или адреса) после получения действительных параметров идентификации.

2.5 **Протокол аутентификации «запрос соединения»;** CHAP (Challenge-Handshake Authentication protocol)**:** Протокол аутентификации с предварительным согласованием вызова по методу запроса соединения, определяемый в [17].

2.6 **Стандарт шифрования данных;** DES (Data Encryption Standard): Хорошо известный симметричный механизм шифрования, использующий ключ длиной 56 бит. Из-за короткой длины ключа он был заменен стандартом AES, но пока все ещё используется в режиме множественного шифрования, например, 3DES или Тройной DES (FIPS 46-3, где Federal Information Processing Standard − Федеральный стандарт по обработке информации).

2.7 **Демилитаризованная зона;** ДМЗ (de-militarised zone - DMZ): Выделенная локальная область или местная сеть, доступ в которую контролируется специальной политикой, использующей межсетевые экраны. Эта зона не является частью общей сети и менее опасна.

2.8 **Отказ в обслуживании;** DoS (Denial of Service): Атака на систему, целью которой является нарушение её функциональности.

2.9 **Цифровой абонентский канал;** DSL (Digital Subscriber Line)**:** Технология, обеспечивающая быстрый доступ по местным телекоммуникационным сетям [7].

2.10 **Протокол динамической настройки конфигурации хостов;** DHCP (Dynamic Host Configuration Protocol): Интернет-протокол, обеспечивающий IP-адресацию при запуске [20].

2.11 **Капсулированный протокол безопасности;** ESP (Encapsulation Security Protocol): Протокол, основанный на IP и обеспечивающий конфиденциальное обслуживание данных. Обычно ESP обеспечивает шифрование как процедуру безопасности для защиты содержимого данных IP пакета. ESP является стандартом Интернет [25].

2.12 **Расширенный протокол аутентификации** (Extensible Authentication Protocol; EAP): Протокол аутентификации, поддерживаемый службой RADIUS и стандартизированный IETF в [23].

2.13 **Протокол передачи файлов;** FTP (File Transfer Protocol): Стандарт (протокол) Интернет [11] для передачи файлов между клиентом и сервером.

2.14 **IETF** (Internet Engineering Task Force)**:** Группа международных специалистов, ответственная за продвижение и развитие технических стандартов Интернет.

2.15 **Интернет протокол доступа к сообщениям версии 4** (Internet Message Access Protocol v4; IMAP4): Протокол электронной почты, который описывает доступ и администрирование почтовой связи и почтовых ящиков, расположенных на удалённом почтовом сервере (определено в [19]).

2.16 **Локальная сеть;** ЛВС (Local Area Network; LAN)**:** Местная сеть, обычно в (одном) здании. Соединенные в совместную сеть скоростным каналом компьютеры и другие устройства, расположенные на незначительном удалении один от другого (комната, здание, предприятие).

2.17 **Модем** (modem)**:** Аппаратное или программное средство, преобразующее цифровые сигналы в аналоговые (для передачи) и аналоговые сигналы в цифровые (для приема). Преобразования такого типа обязательны в случае использования аналоговых линий связи.

2.18 **Многоцелевые расширения электронной почты для Интернет;** MIME (Multipurpose Internet Mail Extensions): MIME определяет способ присоединения к

сообщениям электронной почты Internet двоичных данных (например графических образов). Он определен в [18].

2.19 **Сервер доступа в сеть;** NAS (Network Access Service): Система, обычно компьютер, который обеспечивает доступ в инфраструктуру для удалённых клиентов.

2.20 **Одноразовый пароль** (One time Password; OTP): Пароль, используемый один раз.

2.21 **Пассивный режим;** PASV (Passive mode; PASV mode)**:** Режим установления соединения по FTP.

2.22 **Протокол аутентификации пароля** (Password Authentication Protocol; PAP): Протокол аутентификации, обеспечивающий реализацию PPP [13].

2.23 **Персональный цифровой ассистент;** PDA (Personal Digital Assistant): Обычно носимый в руках компьютер ("налодонный" компьютер), предназначенный для выполнения некоторых специальных функций.

2.24 **Протокол точка-точка;** PPP (Point-to-Point Protocol)**:** Стандартный метод инкапсулирования информации сетевого уровня, поверх соединения точка-точка [13].

2.25 **Почтовый протокол версии 3;** POP3 (Post Office Protocol v3): Протокол электронной почты, определяемый в [15], который позволяет клиенту получить почту, сохранённую на почтовом сервере.

2.26 **Достаточный уровень конфиденциальности;** PGP (Pretty Good Privacy): Общедоступная программа шифрования, использующая схему с открытыми ключами. Форматы сообщений определены в [16] и [26].

2.27 **Частный учрежденческий коммутатор** (Private Branch Exchange; PBX)**:** Телефонная станция, не включенная в общедоступные сети (например, офисная АТС).**;**

2.28 **Служба удалённой аутентификации подключающегося пользователя** RADIUS (Remote Authentication Dial-In User Service): Протокол обеспечения безопасности в Интернет, используемый для аутентификации удалённых пользователей [21].

2.29 **Сервис удалённого доступа;** RAS (Remote Access Service): Аппаратные и программные средства для обеспечения удалённого доступа.

2.30 **Удаленный доступ** (remote access): Авторизованный доступ к системе со стороны вне безопасного домена.

2.31 **Запрос для комментария;** RFC (Request for Comment): Серия стандартов Интернет, предложенных IETF.

2.32 **Оболочка безопасности;** SSH (Secure Shell): Протокол, который обеспечивает безопасное удалённое подключение, используемое небезопасной сетью. SSH не является общим, но скоро станет стандартом IETF. SSH был первоначально разработан компанией «SSH Communications Security».

2.33 **Уровень безопасных сокетов;** SSL (Secure Sockets Layer): SSL протокол, находящийся между сетевым уровнем и уровнем приложений, который обеспечивает услуги аутентификации клиентов, сервера, целостности, конфиденциальности. SSL был разработан компанией «Netscape» и составляет основу TLS.

2.34 **Конфиденциальные/Многоцелевые расширения электронной почты для Интернет;** S/MIME (Security/Multipurpose Internet Mail Extensions): Этот протокол обеспечивает безопасный многоцелевой почтовый обмен. Его нынешняя версия 3 состоит из пяти частей: [32] и [33] определяют синтаксис сообщения, а [27], [28] и [29] определяют спецификацию сообщения, обработку сертификата и метод согласования ключа.

2.35 **Межсетевой протокол для последовательного канала;** SLIP (Serial Line Internet Protocol)**:** Пакетный протокол, определенный в [12], для передачи данных с использованием телефонных линий (последовательных линий).

2.36 **Идентификатор установки сервиса;** SSID (Set Service Identifier)**:** Идентификатор для точек беспроводного доступа, обычно в форме имени.

2.37 **Простой протокол пересылки почты;** SMTP (Simple Mail Transfer Protocol): Протокол Интернет ([10] с расширениями) для посылки почты на почтовые сервера (исходящие сообщения).

2.38 **Протокол безопасности транспортного уровня;** TLS (Transport Layer Security): Усовершенствованный SSL, является официальным протоколом Интернет [22].

2.39 **Унифицированный указатель ресурса;** URL (Uniform Resource Locator)**:** Схема адресов для Web-сервисов.

2.40 **Источник бесперебойного питания;** UPS (Uninterruptible Power Supply): Устройство, имеющее в своём составе аккумуляторы, обеспечивающее защиту изделий при скачках или внезапном отключении напряжения электропитания.

2.41 **Протокол датаграмм пользователя;** UDP (User Datagram Protocol)**:** Сетевой Интернет Протокол для организации связи без установления соединения [9].

2.42 **Виртуальная закрытая сеть;** VPN (Virtual Private Network): Частная сеть, использующая разделённые общие сети, т.е. сеть, основанная на протоколе криптографического туннелирования, функционирующая поверх инфраструктуры другой сети.

2.43 **Защищённый доступ WiFi;** WPA (WiFi Protected Access)**:** Спецификация для усовершенствования безопасности при обеспечении конфиденциальности и целостности беспроводной связи, она включает временный протокол TKIP (temporal key implementation protocol) . WPA является модернизацией WEP.

2.44 **Конфиденциальность, эквивалентная проводной;** WEP (Wired Equivalent Privacy): Криптографический протокол, предполагающий шифрование потока с ключом шифра длиной 128 бит, он определён внутри спецификации на беспроводные ЛВС [8].

2.45 **Точность без проводов;** WiFi (Wireless Fidelity): Торговая марка продвигаемая фирмой «WiFi Alliance», используемая в оборудовании для беспроводных ЛВС.

2.46 **Беспроводная ЛВС** (wireless LAN; WLAN)**:** Сеть, использующая радиосвязь. Наиболее широко используемыми стандартами являются IEEE 802.11b и 802.11g, со скоростями 11 Мб/с и 54 Мб/с соответственно, диапазона 2,4 ГГц.

3 Цель

Данный стандарт предназначен для сетевых администраторов и работников службы безопасности, имеющих дело с вопросами организации защиты удалённого доступа. В нём представлена информация о различных типах и методах удалённого доступа с целью помощи заинтересованным лицам в принятии адекватных мер по защите удалённого доступа от преднамеренных угроз.

Он может также помочь пользователям, которые намерены использовать удалённый доступ в свой офис из дома или во время путешествий.

4 Общий обзор

Удалённый доступ позволяет пользователю подключиться с локального компьютера к удалённому компьютеру или компьютерной сети и использовать их ресурсы так, как при непосредственном подключении к ЛВС. Такие услуги называют Сервисом Удалённого Доступа RAS. RAS подразумевает, что удалённым пользователям могут быть доступны ресурсы сети.

Обычно RAS используется в следующих ситуациях:

– для объединения персональных стационарных рабочих станций (т.е. так, чтобы отдельные работники могли работать из дома как удаленные пользователи);

– для объединения мобильных компьютеров (т.е. поддержать персонал, работающий вне города или во время деловых поездок);

– для объединения нескольких удаленных ЛВС в единую корпоративную сеть;

– для обеспечения управления доступом к удалённым компьютерам (т.е. для удалённого технического обслуживания).

RAS предлагает простой способ связи с удалёнными пользователями по следующим сценариям: удалённый пользователь устанавливает соединение с главной сетью, например, через телефонную сеть, используя модем. Такое прямое соединение может существовать так долго, насколько оно необходимо, и может рассматриваться как арендованная линия, которая активизируется по мере необходимости. Соединение может быть и постоянным, если используется DSL или другая адекватная технология.

Важно: Удалённый доступ для предприятия должен всегда обеспечиваться через сервер удалённого доступа, прямой доступ к компьютерам сопряжен со многими рисками и поэтому должен быть исключен. Модемы предприятия должны быть расположены только в определённых местах.

Ресурсы удаленного доступа приведены на рисунке 1.

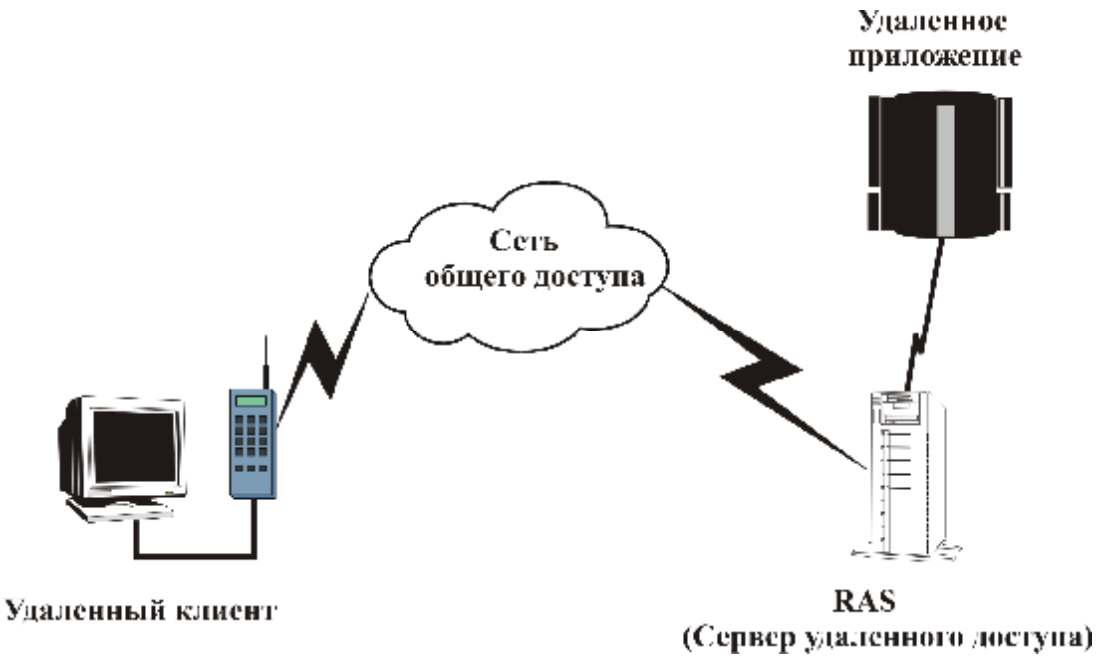


Рисунок 1 – Ресурсы удаленного доступа

Установление соединения RAS обычно требует 3-х компонентов:

1) Компонент локальной сети внутри корпоративной сети, который обеспечивает RAS (т.е. установлено программное обеспечение RAS) и который готов принять соединения RAS. Оно известно как сервер RAS или сервер доступа.

2) Удалённый компьютер, на котором установлено программное обеспечение RAS, и который инициирует соединение RAS. Он известен как клиент RAS. Удалённые клиенты могут быть рабочими станциями или мобильными компьютерами.

3) Коммуникационная среда, по которой устанавливается соединение RAS.

В большинстве случаев клиент RAS использует телекоммуникационную сеть для установления соединения. Минимум, что здесь требуется – это телефонная линия и модем для установления соединения. В зависимости от архитектуры RAS со стороны сервера могут быть использованы различные технологии соединения.

RAS реализуется как архитектура клиент–сервер: клиент RAS может быть конфигурирован так, что он автоматически устанавливает RAS соединение с ресурсами корпоративной сети путём набора номера телефона компьютера, на котором установлен сервер RAS.

Иначе, пользователь может инициировать RAS вручную. Некоторые операционные системы позволяют инициировать RAS немедленно после входа в систему. Помните, что клиентская система может быть компьютером любого вида (ноутбук, PDA (Personal Digital Assistant) или смарт-телефон).

После установления соединения клиентская система может использовать различные приложения, некоторые из которых могут иметь встроенные модули безопасности.

5 Требования безопасности

С точки зрения безопасности клиент RAS и сервер RAS рассматриваются находящимися под управлением политики безопасности, в то время как коммуникационная среда рассматривается как находящаяся вне такого управления и возможно даже находящаяся во враждебной среде. Механизмы безопасности строятся исходя из наличия рисков, что неавторизованные субъекты (индивидуумы или процессы) могут:

- получить доступ к клиенту RAS;
- получить доступ к серверу RAS;
- блокировать доступ к серверу RAS;
- перехватить информацию, которой обмениваются клиент RAS и сервер RAS;
- модифицировать информацию в процессе обмена.

Сервисами безопасности, считающимися с этими рисками, являются сервисы конфиденциальности, сервисы аутентификации управления доступом. Поэтому при использовании RAS применяются следующие элементы безопасности:

Аутентификация: Удалённый пользователь должен быть однозначно идентифицирован системой RAS. Идентичность пользователя должна быть установлена посредством механизма аутентификации каждый раз, когда устанавливается соединение с локальной сетью. В контексте системного доступа должны быть использованы дополнительные управляющие механизмы, чтобы удостовериться, что системный доступ удалённым пользователем надёжно контролируется (например, применение ограничения доступ**а** только в определённое время или только из точек, разрешённых для удалённого доступа).

Существуют различные методы аутентификации пользователей и процессов, отличающиеся по качеству и технологии. Наиболее употребительным, но также и наиболее уязвимым, является использование паролей.

Управление доступом: Когда удалённый пользователь аутентифицирован, сервер удалённого доступа должен быть способен ограничить взаимодействие пользователя с сетью. При этом требуется, чтобы авторизации и ограничения, которые определены для ресурсов локальной сети авторизованными администраторами, также действовали и для удалённых пользователей в дополнение к любым специфическим ограничениям для удаленных пользователей (например, доступ в определённое время дня, одно соединение для одного пользователя).

Безопасность связи: Когда доступ к локальным ресурсам осуществляется удалённо, данные пользователя должны передаваться через установленное соединение RAS. В общем случае, требования безопасности, которые применяются в локальной сети по отношению к защите связи (*конфиденциальность*, *целостность*, *аутентичность*), должны также применяться для данных, передаваемых через соединения RAS.

Однако, защита связи при RAS особенно критична, так как связь может осуществляться с использованием множества технических средств связи и протоколов, которые не могут считаться находящимися под контролем оператора локальной сети.

Возможность доступа: Когда удалённый доступ является основой рабочего процесса, доступность RAS особенно важна. Непрерывный поток производственных процессов может быть нарушен полным отсутствием соединения или недостаточностью скорости передачи данных.

Такой риск может быть до определённой степени уменьшен путём использования альтернативных или избыточных соединений. Это, в особенности, относится к тем случаям, когда Интернет используется как среда связи, хотя, в общем случае, нет гарантий обеспечения необходимой скорости передачи данных для каждого соединения.

Архитектура клиент/сервер системы RAS подразумевает, что оба − и клиент и сервер − предстают перед специфическими рисками из-за типа среды связи и способа использования.

Клиенты RAS не обязательно должны быть стационарными (т.е. настольный ПК), они могут быть мобильными приборами (например, ноутбук). Однако местоположение клиента обычно не будет находиться под контролем оператора ЛВС, так что, в особенности, когда клиент мобильный, следует считаться с тем, что среда небезопасна и подвержена специфическим угрозам, в частности физическим угрозам, таким как кража или повреждение.

Серверы RAS обычно являются частью ЛВС, к которым подсоединяются удалённые пользователи. Они находятся под контролем оператора ЛВС и могут быть обеспечены условиями безопасности, которые применяются локально. Поскольку основной задачей сервера RAS является проверка достоверности подсоединения к ЛВС только авторизованных пользователей, следовательно, сервер RAS должен обеспечивать провал атак, направленных на получение неавторизованного доступа к ЛВС.

6 Типы соединений удаленного доступа

Существуют различные способы установления соединения между клиентом и компьютерами в удалённой ЛВС:

- непосредственный дозвон до сервера доступа, т.е. подключение к серверу с помощью модема по обычной коммутируемой телефонной линии связи;
- подключение с помощью модема по обычной коммутируемой телефонной линии связи к серверу провайдера услуг Интернет (ISP) и доступ в удалённую локальную сеть через Интернет;
- доступ средствами постоянного соединения с другой сетью.

Рисунок 2 показывает эти типы удалённых соединений: мобильный пользователь 2 соединяется с ЛВС через ISP, данные из Интернет проходят через межсетевой экран (firewall), который контролирует обмен между Интернет и локальной сетью. Мобильный пользователь 1 может быть пользователем беспроводной ЛВС; тогда RAS называется Точкой Доступа. Этот сервер доступа также управляется межсетевым экраном.

Примечание - Мобильные пользователи могут использовать соединение через коммутируемую телефонную сеть, арендованную линию с широкой полосой пропускания или беспроводные соединения.

Ситуация с так называемым «WLAN hot spot» (общедоступной беспроводной ЛВС) описывается с помощью мобильного пользователя 2, осуществляющего доступ из точки доступа беспроводной ЛВС вместо использования локального модема. Это означает, что общий доступ к Интернет обеспечивается через точку доступа беспроводной ЛВС и ISP.

Существуют различные методы, которые клиент может использовать для соединения с ISP. Клиент может использовать проводные или беспроводные технологии. В зависимости от используемых методов могут иметь место дополнительные риски, т.е. беспроводная ЛВС требует, чтобы были применены специальные меры безопасности для сохранения конфиденциальности.

Эти методы предлагают специфические приемы, которые должны быть приняты во внимание. Например, подключение к серверу с помощью модема по обычной коммутируемой телефонной линии связи предназначается, чтобы удостовериться, что только авторизованные пользователи, которые знают номер набора, могут удалённо подсоединиться к сети. Однако инструменты сканирования доступных номеров дозвона (путем последовательного перебора) помогают хакерам идентифицировать существующие активные модемы, ожидающие входящих звонков. Провайдеры услуг Интернет обеспечивают преимущество для удалённого пользователя. Пользователь может использовать подключение через локального ISP для соединения с удалённой ЛВС. Тем не менее, такой метод соединения может потребовать использования более дорогого сервера и специального его конфигурирования.

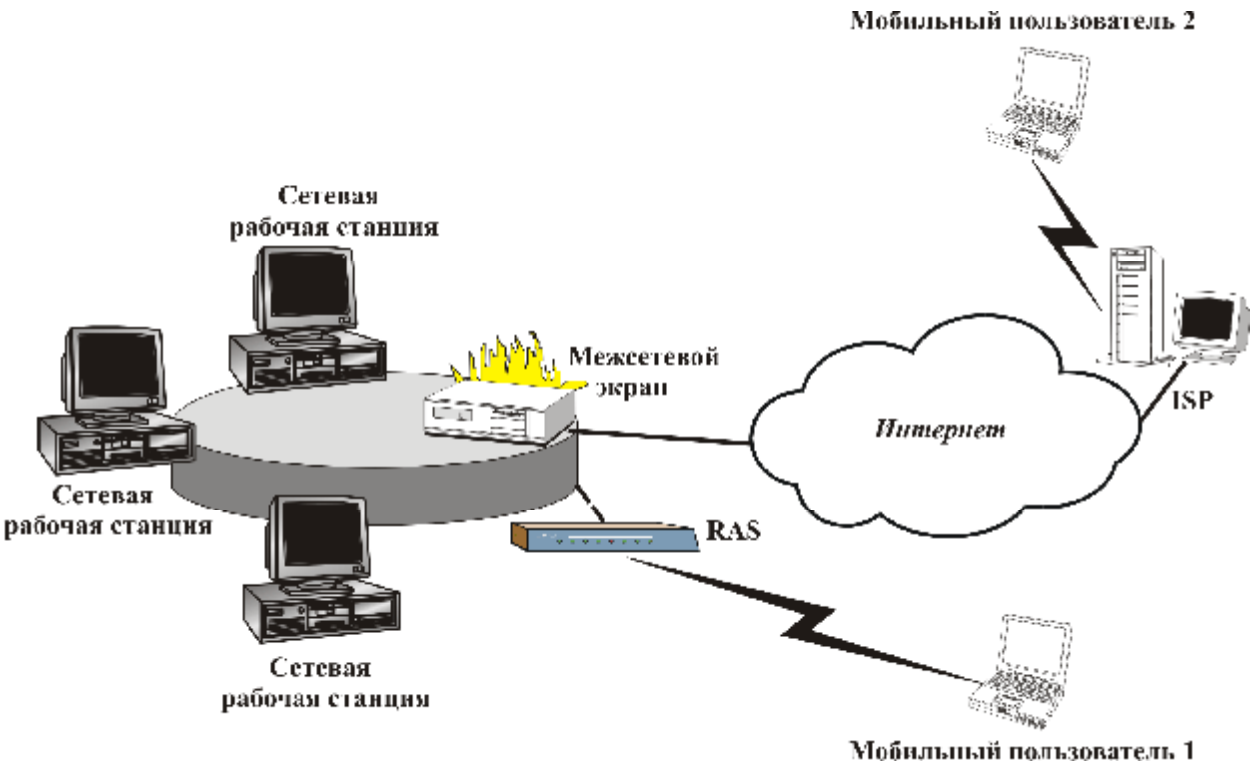


Рисунок 2 – Типы удаленного доступа

7 Методы установления соединения при удаленном доступе

7.1 Общие положения

Для обеспечения удалённого доступа необходимо знать основные принципы. Предприятие должно определиться, какие системы и какие приложения могут быть доступны из внешнего мира для отдельного пользователя. Тип удалённого доступа должен быть определён сервисами, которые используются удалённо.

7.2 Доступ к коммуникационным серверам

7.2.1 Общая защита связи

Наиболее общеупотребительным предоставляемым доступом является доступ к коммуникационным службам внутри предприятия, т.е. доступ пользователя к своей почте, к серверу FTP или к Web-серверу. В Приложении D приведены перечни действий для организации работы безопасного почтового сервера, а Приложение E поможет безопасно установить и администрировать Web-сервер.

Существуют различные пути защиты коммуникаций между сервером и клиентом, обеспечивающие аутентичность, конфиденциальность и целостность, такие как:

a) SSL (уровень безопасных сокетов) определяет метод аутентификации общающихся сторон (аутентификацию клиента и сервера) и шифрование информации, которой обмениваются эти стороны. SSL поддерживается Интернет-браузером и Web-сервером так же, как и почти всеми операционными системами. IETF разработала для защиты связи клиент/сервер протокол защиты транспортного уровня (Transport Layer Security, TLS), который основан на SSL и на стандарте Интернет [22].

b) IPsec (протокол Интернет для обеспечения безопасности) предлагает пути аутентификации сторон, необходимые для защиты передаваемой информации. IPsec также предлагает функции управления ключом (см. также [24]).

c) SSH (оболочка безопасности) − это протокол для безопасного удаленного входа в сеть и другие конфиденциальные сетевые сервисы при работе в небезопасной сети. Он устанавливает безопасное соединение после успешной аутентификации удаленного пользователя и обеспечивает набор команд и сервисов (например, безопасная передача файлов).

Эти методы обеспечивают безопасную аутентификацию, конфиденциальность и услуги целостности и должны быть использованы дополнительно к коммуникационному программному обеспечению. Из-за того, что SSL - часть обычно доступных Internet браузеров, доступ к Web-почте может легко быть защищен путём установления SSL связи до момента доступа к почтовой учётной записи пользователя.

Основное отличие между этими методами состоит в том, что SSL/TLS и IPsec обычно предоставляются как последующие функции связи, являясь услугой безопасности сети, а SSH является приложением безопасности.

Эти методы являются применимыми для соединения FTP-клиента с FTP-сервером, позволяя осуществить доступ к данным, сохраняемым на этом сервере.

Примечание - Многие протоколы Интернет, например Telnet, обеспечивающий возможности терминального доступа или FTP, позволяющий передачу файлов, поддерживают слабые механизмы аутентификации, обычно посылая парольную информацию как простой текст. Туннелирование таких протоколов через протоколы безопасности такие как SSH, SSL/TLS или IPsec обеспечивает не только конфиденциальность, но также значительное улучшает процесс аутентификации.

Заметьте, что многие Web-серверы используют SSL/TLS только для обеспечения аутентификации пользователя, но не наоборот, когда пользователь требует подтвердить сертификат от сервера.

7.2.2 Защита электронной почты

Хотя электронная почта является услугой, которая не обеспечивает конфиденциальности собщений, для достижения сервера извне необходимо выполнить некоторые предварительные действия. Общеупотребительным способом обеспечить доступ к почтовому серверу является Web-интерфейс к почтовым учётным записям, что позволяет пользователям получать доступ к своим почтовым записям. Этот метод требует наличия компьютера с браузером, т.е. может быть использован любой доступный компьютер. С другой стороны, этот метод не пользоволяет пользователям загружать свою почту и отвечать без установления соединения (off-line).

Другие подходы позволяют пользователям использовать себя как стандартных почтовых клиентов, но они не обеспечивают достаточной конфиденциальности из-за концепции почтовых протоколов. В общем случае, почтовый клиент достигает почтового сервера (например, использует обычную программу администрирования всех входящих почтовых учётных записей) путем самостоятельной аутентификации, заполненяя данные пользователя в пустых полях. Два почтовых протокола доступа (POP3 и IMAP4) отличаются способом, которым они обрабатывают входящую почту:

– POP3 загружает все новые доступные почтовые сообщения и пользователь может работать с ними локально;

– IMAP4 позволяет пользователю загрузить только заголовки писем, а затем решить, какое сообщение загрузить в свой компьютер.

Из-за того, что эти протоколы сами по себе не обеспечивают механизмов защиты в достаточной степени, строгая аутентификация и конфиденциальность передачи должны обеспечиваться дополнительно, например применением SSL, SSH.

Примечание - Вы можете также защитить содержимое почты (за исключением адреса отправителя, адреса получателя и темы сообщения). Две основных спецификации − это PGP и S/MIME, которые обеспечивают услуги конфиденциальности, целостности, аутентичности и невозможности отказа от авторства. Обе они могут быть интегрированы во многие почтовые клиентские программы. Но они не предоставляют защиту от анализа трафика, потому что адреса отправителя и получателя передаются открытым текстом.

Почтовый сервер, доступный удалённым пользователям, должен быть расположен в демилитаризованной зоне (ДМЗ) сети. Задачей ДМЗ является отделить внешнюю сеть от внутренней посредством изоляции компьютеров, к которым имеется прямой доступ, от каждого компьютера сети. Размещение почтового сервера в ДМЗ означает, что он доступен как из внешней сети, так и из внутренней. Чтобы избежать возникновения риска для внутренней сети, необходимо выполнить следующие меры:

Должна быть предусмотрена невозможность установить соединение между компьютером внешней сети и компьютером внутренней сети через ДМЗ. Это может быть достигнуто конфигурированием соответствующих шлюзов и промежуточных компьютеров или их комбинацией для обеспечения такого разделения.

Подходящая конфигурация требует предусмотреть следующие вопросы:

– почтовый сервер должен иметь только специальное приложение и минимизированную операционную систему, во избежание использования его как промежуточную машину для атак;

– доступ из внешней сети должен быть разрешён только к строго определённым приложениям (определённым IP адресом и номером порта);

– доступ из внутренней сети должен быть также ограничен определёнными адресами и портами источников (тех компьютеров во внутренней сети, которым доступ разрешен), а также адресами назначения. Таким образом, направление потока информации также должно быть ограничено. Это может быть достигнуто использованием маршрутизаторов или межсетевых экранов.

Другие коммуникационные сервера, такие как Web-сервера, также могут быть расположены внутри ДМЗ и соответственно защищены. В таблице 1 приведены примеры номеров портов и протоколов, которые могут использоваться, когда почтовый сервер расположен в ДМЗ.

Таблица 1 - Электронная почта и соответствующие номера портов

Номер	Название	Описание
22	ssh	Безопасная оболочка регистрации
25	smtp	Стандартный STMP порт с TLS/SSL
465	dmtps	SMTP над TLS/SSL
143	imap	Стандартный IMAP
993	imaps	IMAP над TLS/SSL
110	pop3	Стандартный POP3
995	pop3s	POP3 над TLS/SSL

Рисунок 3 показывает различие конфигураций, необходимых для локальных маршрутизаторов Интернета и внутренней сети. В этом случае доступ к почтовому серверу извне разрешён только по протоколу IMAP поверх TLS/SSL и POP поверх TLS/SSL, в то время как для отправки почты может быть использован обычный SMTP. Из внутренней сети доступ разрешён, используя IMAP или POP без дополнительной защиты с помощью TLS/SSL. Команды написаны псевдо-командным языком, описывающим перечень требуемых команд доступа для граничного межсетевого экрана и внутреннего маршрутизатора. Все другие порты запрещёны, чтобы избежать уязвимостей, связанных с этими портами и протоколами.

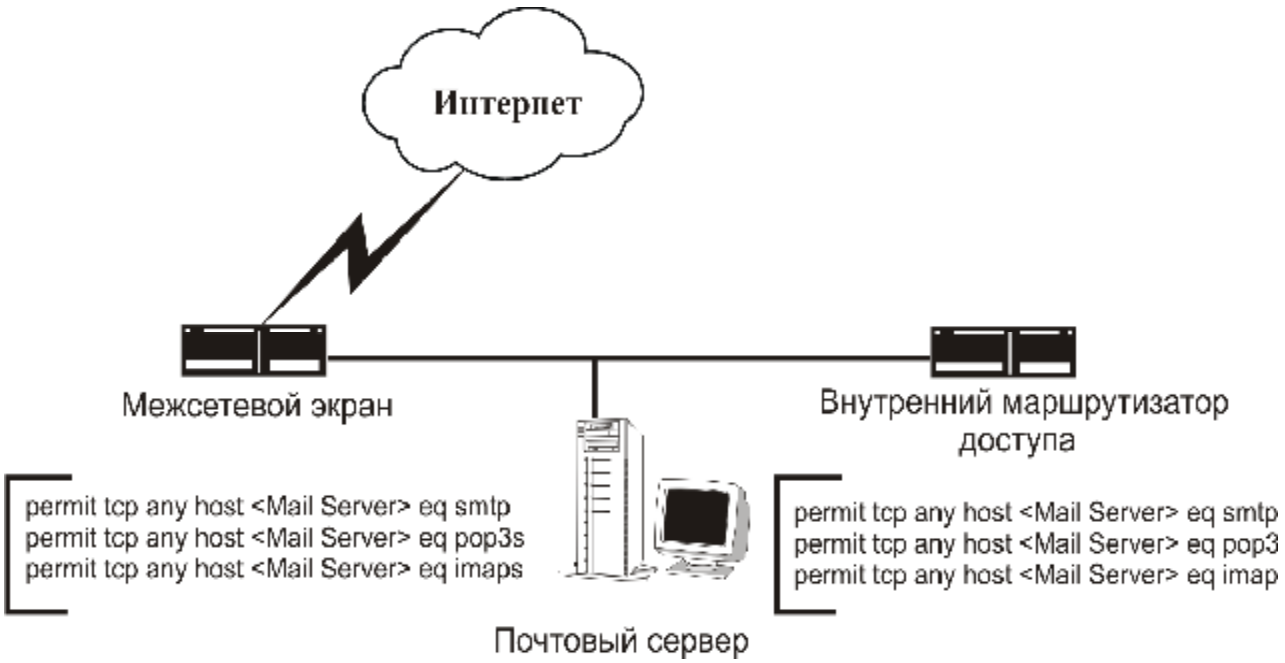


Рисунок 3 – Доступ к почтовому серверу в пределах ДМЗ

Дополнительные меры безопасности также могут быть применены, чтобы избежать неправильное использование почтового сервера SMTP (например, ограничение соединений SMTP, чтобы избежать обслуживания незапрашиваемой электронной почты).

7.2.3 Защита подключения по FTP

FTP (Протокол передачи файлов) − это другой сервис, при котором сервер может быть расположен внутри ДМЗ. FTP определяет два режима работы:

- режим PORT (известный также как Обычный или Активный режим);
- режим PASV (известный также как Пассивный режим).

Эти режимы отличаются процедурой установления канала данных: в режиме PASV канал команд и канал передачи данных устанавливается клиентом FTP, обращающимся к серверу FTP; в режиме PORT - клиент FTP открывает канал команд, а сервер FTP, после подтверждения запроса клиента, открывает канал передачи данных (подробно см. в приложении С). При использовании FTP определён 21 порт для организации канала команд, а порт канала данных назначается динамически из диапазона, обычно начинающегося от порта 1024 и заканчивающегося портом 5000.

В принципе режим PORT позволяет более безопасную установку межсетевого экрана для фильтрации пакетов, при обеспечении сервиса FTP для удалённых клиентов. Только порт 21 TCP должен быть открытым для приема, чтобы установить инициируемый клиентом канал команд. В последующем организованный канал данных открывается для передачи. Рисунок 4 показывает настройки фильтрации в ДМЗ, содержащей сервер FTP.

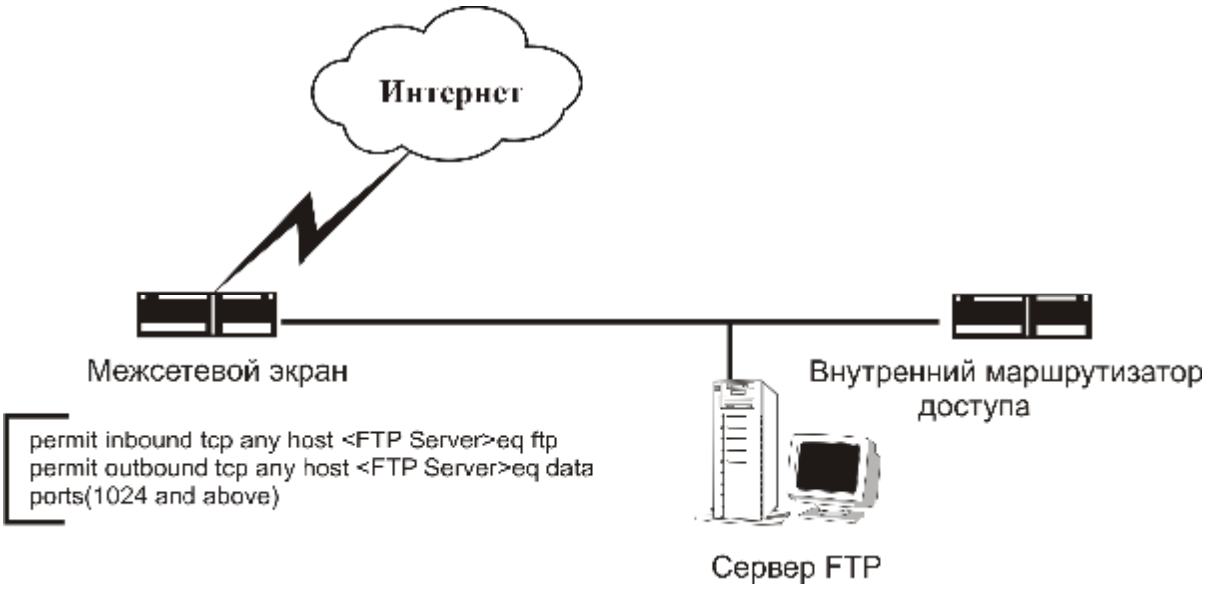


Рисунок 4 – Доступ к FTP серверу в пределах ДМЗ

Напротив, применение сервера FTP, использующего режим PASV, требует для простых межсетевых экранов, открытия широкого диапазона портов, начиная от 1024 для входящих соединений. Такие установки оставляли бы главные риски при межсетевой защите.

К сожалению, режим PORT не может быть использован в комбинации с трансляцией сетевого адреса через межсетевую защиту из-за раздельного установления канала данных. Режим PASV преодолевает это ограничение, потому что все каналы инициируются клиентской системой. Подразумеваемые риски при открытии широкого диапазона портов могут быть снижены путем осуществления более сложных методов межсетевой защиты: межсетевые экраны обеспечивают полную инспекцию текущего состояния, позволяя временно, по требованию, открытие входящих портов для

обеспечения режима PASV для FTP без необходимости открытия широкого диапазона портов для приема. Тот же самый результат может быть получен при использовании специального прокси-компонента в межсетевом экране.

При рассмотрении предоставляемых удаленным клиентам возможностей FTP важно знать, что протокол FTP сам по себе предоставляет только базовые меры безопасности. Конфиденциальность не поддерживается, а услуги аутентификации предоставляются только на самом базовом уровне. В качестве примера, пароли передаются простым текстом, что позволяет организовывать атаки.

Поэтому сервисы FTP должны при необходимости осуществляться в комбинации с нижележащим уровнем протоколов безопасного туннелирования (например TLS/SSL) или усовершенствованными приложениями для передачи файлов, такие как Secure FTP или SCP (безопасное копирование), оба основанные на протоколе SSH. Оба варианта позволяют осуществление строгой аутентификации и обеспечение конфиденциальности сервисов.

7.3 Доступ к ресурсам ЛВС

Такой доступ требует специальной инсталляции компьютеров и определенной конфигурации системы. Из-за того, что удалённый пользователь, пытающийся установить доступ к ресурсам внутри сети, представляет угрозу для этой сети, удалённый доступ должен удовлетворять следующим условиям:

Аутентификация: механизм строгой аутентификации или двухфакторная аутентификация должны удостоверить, что идентичность удалённого пользователя подтверждена.

Предоставление права доступа в систему (Авторизация): После успешной аутентификации удалённый пользователь получает предоставляемые ему права, которые позволяют выполнять свою работу. Таким образом, пользователь выполняет определенную роль удалённого пользователя.

Управление доступом: до предоставления доступа к ресурсам или данным удалённый пользователь проверяется на предоставляемые ему права.

Конфиденциальность, подлинность и целостность: в зависимости от используемых данных или ресурсов должна быть установлена безопасность связи с помощью предоставляемых услуг конфиденциальности, подлинности и целостности.

Эти требования будут выполняться при использовании протоколов безопасного туннелирования для виртуальных частных сетей, включая соответствующие механизмы аутентификации.

Соответствующими механизмами аутентификации для удалённых пользователей являются, например, токены (набор символов) однократного пароля, которые обеспечивают уникальный пароль каждый раз, когда производится попытка доступа пользователем, вводящим свой личный идентификационный номер (Personal Identification Number, PIN). Такие токены обеспечивают двухфакторную аутентификацию, когда пользователь должен иметь токен и знать соответствующий PIN.

Предоставление права доступа в систему (Авторизация) устанавливает специфические роли, которые могут быть назначены группам удалённых пользователей. Группа должна быть наделена только теми правами, которыми необходимы для выполнения заданий, которые она выполняет дистанционно. Такой способ ограничения доступа для удалённых пользователей может быть легко осуществлён.

Управление доступом может быть осуществлёно с помощью политики, поддерживаемой механизмами, предоставляемыми используемыми операционными

системами. Например, политика учётной записи пользователя может определять требуемые права и ограничения. Операционные системы могут также предоставлять групповую политику, специально разработанную для удалённых пользователей.

Наиболее общеупотребительным набором протоколов является протокол, предоставляемый службой удалённой аутентификации подключающегося пользователя (RADIUS). Эти протоколы, первоначально разработанные только для коммутируемого удалённого доступа, дают возможность централизовать аутентификацию, авторизацию и учётную запись для доступа в сеть, они поддерживаются VPN и строгими механизмами аутентификации. Протоколы работают следующим образом:

Клиент службы RADIUS (обычно сервер доступа типа сервера модемной связи, сервер VPN или точка беспроводного доступа) посылает мандат пользователя и информацию о параметрах соединения в форме сообщения RADIUS в сервер RADIUS. Сервер RADIUS подтверждает подлинность и разрешает запрос клиента RADIUS и посылает назад ответное сообщение RADIUS. Клиенты RADIUS также посылают сообщения RADIUS об учётных записях в сервер RADIUS. Дополнительно, стандарты RADIUS поддерживают использование прокси-сервиса RADIUS. Прокси-сервис RADIUS − это компьютер, который направляет сообщения RADIUS между клиентами RADIUS и серверами RADIUS, возможно через другие прокси-сервисы RADIUS. Сообщения RADIUS никогда не посылаются между клиентом, пытающимся осуществить доступ, и сервером доступа.

Сообщения RADIUS посылаются как сообщения протокола датаграмм пользователя (UDP); порт 1812 UDP используется для сообщений аутентификации RADIUS, а порт 1813 UDP используется для сообщений учётных записей RADIUS. Только одно сообщение RADIUS может быть включено в качестве полезной информации в пакет UDP.

Рекомендация [30] определяет следующие типы сообщений RADIUS:

– **Запрос Доступа.** Посылается клиентом RADIUS для запроса аутентификации и авторизации при доступе в сеть;

– **Принятие Доступа.** Посылается сервером RADIUS в ответ на сообщение Запрос Доступа. Такое сообщение информирует клиента RADIUS, что попытка соединения подтверждена и разрешена;

– **Отклонение Доступа.** Посылается сервером RADIUS в ответ на сообщение Запроса доступа. Это сообщение извещает клиента RADIUS, что попытка подключения отклонена. Сервер RADIUS посылает это сообщение, если или мандат не подлинный или попытка подключения не разрешается;

– **Вызов Доступа.** Посылается сервером RADIUS в ответ на сообщение Запрос Доступа. Это сообщение является вызовом клиента RADIUS, который ждёт ответ.

В приложении В даются рекомендации по реализации и размещению RADIUS внутри операционной системы Microsoft Windows 2000.

7.4 Доступ для технического обслуживания

Этот тип удалённого доступа предоставляется системным администраторам, которые соединяются, когда требуется управлять системой дистанционно. Из-за того, что эта группа пользователей имеет обычно высшие права доступа к системе, доступ должен быть установлен наиболее безопасным образом. Также, любая деятельность, проводимая дистанционно, должна быть позднее проверена, в особенности, когда ведётся системное администрирование системных служб.

Поэтому доступ нужно обеспечить только на определенный компьютер, которым нужно управлять удаленно.

В этом случае требуются следующие меры:

– Доступ должен обеспечиваться только к определенной учетной записи на определенной машине;

– Связь между удалённым пользователем и машиной, за которой необходим надзор администратора, должна быть защищена с использованием таких средств как SSH;

– Аутентификация пользователя должна быть проведена с использованием строгих механизмов аутентификации;

– Каждый пользователь, получающий доступ к удалённому администрированию системы, должен быть обучен необходимым процедурам и методикам;

– Каждое действие должно быть зарегистрировано;

– Регистрация должна быть проверена немедленно после выполнения удалённого администрирования или при первой возможности в случае превышения времени, выделенного для технического обслуживания.

Механизм обратного вызова (требует использования добавочных защитных мер, см. также 8.2) является дополнительным. Следование этим требованиям ограничивает риски, имеющиеся при данном типе удалённого доступа.

8 Рекомендации по выбору и конфигурации

8.1 Общие положения

В данном разделе обсуждаются меры, требуемые для противодействия известным угрозам. Каждая предлагаемая мера будет подробно объяснена, будут приведены аргументы за и против. Структура изложения такова, что области клиента RAS, сервера RAS и коммуникаций RAS будут рассмотрены отдельно. Совместные меры будут обсуждаться в конце.

Мы не рассматриваем угрозы клиенту и серверу полностью раздельно, поскольку если клиент RAS был бы атакован, то сервер RAS тоже был бы автоматически подвергнут опасности. Более того, необходимо помнить, что например, в операционной системе Windows каждый клиент RAS может также работать как сервер RAS, так что угрозы серверу RAS могут быть и угрозами клиенту RAS.

8.2 Защита клиента RAS

8.2.1 Стационарный клиент RAS

Стационарный клиент должен быть сначала защищён физически, т.е. должен находиться в комнате, куда имеют доступ только те лица, которым такой доступ разрешён. Это может быть приемлемым для тех лиц, которые удаленно работают в офисе из дома.

Стационарный клиент может соединяться с сервером RAS, используя телефонный модем, кабельный модем или DSL соединение. Второй и третий тип соединения требуют дополнительных мер для обеспечения высокоскоростного соединения, обеспечивающего постоянное соединение с Интернет. Простым защитным приёмом является инсталляция и правильная конфигурация так называемого «персонального межсетевого экрана», который ограничивает доступ к соединяемому компьютеру извне.

8.2.2 Все клиенты RAS

Для всех клиентов RAS существует несколько уровней безопасности, применяемых во избежание неправильного использования компьютера и обеспечения безопасного

удалённого соединения.

Первым устанавливаемым барьером является сами аппаратные средства компьютера. Простым приёмом защиты компьютера и исключения его неправильного использования является установка пароля при загрузке, который производит идентификацию пользователя до загрузки системы. Этот барьер является первым препятствием для потенциальных атакующих, но он не обеспечивает достаточной защиты.

Вторым препятствием является операционная система. Для портативных компьютеров и рабочих станций должна использоваться операционная система, которая обеспечивает идентификацию и аутентификацию пользователя. Такое свойство имеют большинство действующих систем. Используемая учётная запись должна быть обычной учётной записью пользователя, но не учётной записью администратора, потому что эти учётные записи дают больше привилегий и поэтому должны быть использованы только для администрирования компьютера. Также следует помнить, что должно быть обязательно обеспечено соответствующее качество пароля[1].

Если в компьютере сохраняется информация, представляющая интерес для всей компании, то должны быть предусмотрены дополнительные меры.

Для операционной системы должна быть обеспечена большая безопасность, чем при типовой конфигурации. Это означает, что все ненужные компоненты операционной системы должны быть удалены, а инсталлированы только необходимые приложения. Также, такие особенности как конфигурация сети ограничиваются тем, что разрешаются только требуемые для конкретной системы сервисы.

Должна быть достигнута строгая аутентификация путём использования смарт-карт, токен-карт или биометрических[2] механизмов. Строгая аутентификация, известная также как много - или двухфакторная аутентификация, требует от пользователя произвести по меньшей мере два этапа идентификации[3].

Шифрование жёсткого диска обеспечивает защиту от раскрытия сохраняемой информации. Этот сервис конфиденциальности должен обязательно использовать строгие алгоритмы (см. также[4][4]).

Другим важным вопросом конфигурации является конфигурация модема. Модем клиента должен быть установлен таким способом, чтобы он не принимал входящие звонки. Соединение должно быть инициировано только самим пользователем-клиентом.

Во многих случаях улучшить безопасность может персональный межсетевой экран при его правильной конфигурации.

Наконец, чтобы избежать и ограничить ущерб, вызванный вредоносным программным кодом, должна быть установлена и регулярно обновляема антивирусная программа.

8.3 Защита сервера RAS

8.3.1 Физическая и логическая установка

Для сервера RAS физическая безопасность является необходимостью. Обычно

[1] Больше информации по управлению паролем можно найти в ИСО/МЭК 17799.

[2] Биометрия означает аутентификацию людей по физическим или поведенческим характеристикам.

[3] Аутентификация обычно требует от пользователя предоставить что-то, что они знают (пароль), чем владеют (токен- или смарт-карта), или чем являются (биометрическая характеристика) или какую-либо комбинацию из перечисленных действий для того, чтобы подтвердить идентичность.

[4] Находится в процессе опубликования.

сервер RAS является частью инфраструктуры серверов предприятия и должен иметь такую же степень физической безопасности, как и другие серверы. Как и любые другие сервисы используемые для удалённого обслуживания сервер RAS должен быть расположен в ДМЗ. Защита против неавторизованного физического доступа достигается путём размещения его в запертой серверной комнате, против сбоев питания - применением источника бесперебойного питания. Другими требуемыми мерами является безопасная установка и конфигурация сервера RAS, безопасное администрирование и процедуры резервного копирования и восстановления информации.

Хотя наиболее распространённым типом сервера RAS все ещё остаётся сервер, обеспечивающий доступ через модем или использующий телефонную линию ISDN, тем не менее, имеются такие решения, когда доступ осуществляется через местного сервис провайдера RAS без контроля со стороны организации. Дальнейший доступ затем предоставляется через Интернет и управляется и ограничивается в организации системой межсетевых экранов.

Преимуществом такого подхода является низкая стоимость (доступ является обычно местным звонком), а недостатком - двойная идентификация клиента: сначала у сервис провайдера Интернет, а затем снова в месте удаленного расположения.

8.3.2 Сервер RAS и модем

Для сервера RAS, предоставляющего доступ через модем, должны быть предусмотрены некоторые меры, гарантирующие, что работа модема не вносит дополнительных рисков в инфраструктуру.

Компьютер должен быть сконфигурирован так, чтобы выполнять только задачу предоставления RAS, а другие услуги должны быть игнорированы. Операционная система должна быть усилена и в ней сделаны все появившиеся исправления и обновления. Только административному и обслуживающему персоналу разрешен физический доступ к серверу. На сервере не должно быть учётных записей обычных пользователей.

Если сервер RAS предоставляет также и другие сервисы, то должно быть проверено и подтверждено, что комбинация сервисов не вносит новых рисков. Поддержка конфигурации сервера RAS должна быть предоставлена разработчиком программного обеспечения.

Другими важными вопросами, которые должны быть приняты во внимание, являются: резервное копирование данных; регистрационная информация, которую нужно собирать; передача файлов регистрации на управляющую станцию (для ежедневного анализа) и разработка планов действий в критических ситуациях.

До начала активного предоставления услуг удалённого доступа сервер должен быть проверен на известные уязвимости. Тесты должны включать проверку местной конфигурации и защиты сети.

Модем должен быть сконфигурирован для пассивной работы в одном направлении, позволяя только входящие звонки. Если возможно, конфигурация должна позволять производить аутентификацию в модеме, а затем инициировать обратный звонок (известный также как обратный вызов) по предыдущему сохраненному в памяти номеру. Такой обратный вызов работает только со стационарными клиентами или портативными компьютерами, соединёнными через мобильные телефоны. При этом подтверждаются соединения только с известных адресов (телефонных номеров) и такой способ позволяет звонящему субъекту уменьшить стоимость звонка.

Современное телефонное оборудование (например, PBX) предоставляет возможности переадресации входящих (звонков), когда можно перенаправить вызов на

другой номер, чем предназначалось первоначально. Поэтому, механизмы обратного вызова нужно использовать с дополнительными предосторожностями

У клиентов должна быть инсталлирована и регулярно обновляема антивирусная программа.

8.3.3 Сервер доступа к сети

Если удалённый доступ устанавливается через местного сервис провайдера Интернет (ISP), то доступ в сеть должен быть контролируем сервером доступа в сеть (NAS), так как доступ к ISP будет находиться вне прямого контроля со стороны организации и результат аутентификации не будет ей известен.

NAS должен быть защищён как и любое другое сетевое устройство, т.е. он должен храниться в закрытом помещении так, чтобы только авторизованные администраторы могли получить к нему физический доступ. Управление устройством должно соответствовать местной политике безопасности: если система управления сетью контролирует её действия, тогда трафик между системой управления и NAS должен осуществляться или внутри локальной сети, или быть туннелирован, чтобы скрыть тип информации.

8.3.4 Точки беспроводного доступа

Хотя точки доступа для беспроводной ЛВС не являются типичным способом удалённого доступа, они могут быть использованы для предоставления доступа в сеть. Поэтому, точки доступа для других беспроводных технологий должны быть расположены в ДМЗ и защищены. Дополнительную информацию о безопасности беспроводного доступа см. 8.5.

8.4 Защита соединения

8.4.1 Общие замечания

Соединение между клиентом RAS и сервером RAS проходит некоторое число стадий. Вначале соединение устанавливается, затем оно будет работать, а после использования оно будет прекращено. Все эти стадии связи требуют защиты.

Следующий раздел рассматривает различные стадии защиты соединения между клиентом RAS и сервером RAS.

8.4.2 Установление соединения

Установление безопасного соединения требует аутентификации удалённого пользователя. Это происходит, когда установлен специальный протокол[1], используемый для удалённого доступа.

Существуют различные способы аутентификации пользователя, которые различаются также по уровням безопасности. Первые два протокола используются между клиентом (которого называют абонентом) и сервером (аутентификатором), третий протокол использует сервер аутентификации, который позволяет включить дополнительные схемы аутентификации.

Наиболее общей схемой аутентификации является использование протокола парольной аутентификации (PAP), который является двухсторонним протоколом

[1] Для модемного доступа раньше использовался протокол SLIP, который позволял осуществлять только простую аутентификацию, используемый сейчас протокол точка - точка (PPP) является более надёжным и обеспечивает лучшую аутентификацию.

установления связи, в котором сервер аутентификатор получает мандаты абонентов и позволяет им доступ или отказывает в нем, основываясь на этих мандатах. Мандаты посылаются открытым текстом и, обычно, состоит из идентификатора пользователя (ID) и пароля. Поэтому этот протокол не обеспечивает защиты от повторения однотипных атак.

Более совершенная схема аутентификации предлагается протоколом аутентификации «запрос соединения» (CHAP). Он является протоколом установления связи, состоящим из трех признаков, в котором аутентификатор посылает «запрос» клиенту. Этот запрос уникальный и изменяется всякий раз при новой посылке. Клиент отвечает секретным значением, вычисляемым из параметров своего идентификатора ID (так называемого «секрета») и «запроса». Аутентификатор сравнивает результат со своими вычислениями и позволяет или отклоняет доступ. Передаваемый мандат шифруется с использованием хэш-алгоритма (наиболее часто используемым является алгоритм MD5). CHAP защищает против повторных однотипных атак, поскольку запрос непредсказуем.

Наиболее общий подход реализуется в RADIUS, как было описано в 7.3.

Сервер RADIUS обычно хранит ID централизованно, т.е. он хранит общедоступные секреты удалённых пользователей. Если пользователь хочет получить доступ в сеть, он посылает «запрос доступа» в сервер RADIUS, содержащий ID, пароль, идентификационные данные системы и порт системы, используемый для доступа. Когда имеется пароль, он маскируется с использованием криптографических средств. Сервер RADIUS может или сам ответить на запрос или отослать запрос другому серверу RADIUS. Если сервер отвечает на запрос, то он сначала должен подтвердить, что переданные данные истинны. Истинная идентификация должна, по меньшей мере, состоять из ID и пароля, но может также включать системный адрес и назначенный порт. Если запрос отсылается другому серверу RADIUS, тогда первоначально адресованный сервер ведёт себя как клиент. Таким способом может быть проведена дополнительная аутентификация. Примерами могут быть аутентификации в UNIX, WINDOWS или NOVELL. Сервер RADIUS может также использовать схемы аутентификации PAP или CHAP.

Строгая аутентификация может быть проведена с использованием цифровых сертификатов или токенов. Этот способ аутентификации основывается не только на знании пользователя, но и на владение токеном или сертификатом, поэтому он называется двухфакторной аутентификацией. Также может быть использована и биометрическая идентификация.

Примечание - Устаревший сетевой сервис TACACS и его модификации XTACACS и TACACS+ по-прежнему используется, но не играют столь важной роли как RADIUS.

8.4.3 Шифрование связи

Угроза перехвата информации может быть ликвидирована при использовании криптографии. Шифрование в канале связи ограничивает возможность связи только с теми аппаратными средствами, где имеется аналогичное шифровальное оборудование. Шифрование содержания даёт больше гибкости и позволяет подсоединяться к серверам, которые не предоставляют собственного сервиса шифрования. При этом обеспечивается конфиденциальность связи между соответствующими конечными точками шифрования.

Примером шифрования содержания является использование программного обеспечения PGP, пакета программ, который предоставляет шифрование, основанное на использовании открытого ключа, при этом оказывая такие услуги, как невозможность отказа от авторства и аутентичность.

Важно: При использовании программы шифрования удостоверьтесь, что длина используемого ключа достаточна. Также определите процедуры для верификации аутентичности и подлинности сертификатов открытого ключа, получаемых через электронную почту, прежде чем использовать их.

Дополнительные способы защиты содержания связи при удалённом доступе обеспечивается использованием виртуальных закрытых сетей (VPN). Существует некоторое количество доступных продуктов, которые предлагают такой вид защиты. Применяя их, удостоверьтесь, что для организации VPN будут использоваться только стандартизированные протоколы.

8.5 Защита беспроводного соединения

Протоколы беспроводной связи могут быть использованы при различных вариантах удалённого доступа:

– Такие протоколы, как Bluetooth используются для ближней связи мобильных телефонов, модемов или иных компонентов широкополосного доступа в клиентскую систему удалённого доступа;

– Беспроводные ЛВС протоколы, такие как протоколы, определённые в серии стандартов IEEE 802.11 могут быть использованы для подключения клиентских систем удалённого доступа к общедоступным и частным сетям.

В большинстве подобных ситуаций организация, предоставляющая возможности удалённого доступа, не имеет или имеет очень ограниченное влияние на конфигурацию или настройки используемых протоколов беспроводной связи:

В качестве примера, мобильный пользователь может соединиться с клиентской системой удалённого доступа, используя средства доступа к общедоступным беспроводным ЛВС (так называемые «hot spot»), имеющихся в аэропортах. Инфраструктура такого беспроводного доступа, обычно, принадлежит ISP и пользователи или их организациями не могут влиять на её конфигурацию.

Хотя беспроводные протоколы предоставляют некоторые услуги безопасности, на них нельзя полагаться целиком в области удаленного доступа. Поэтому, если беспроводные протоколы позволяют осуществлять связь с возможностями удалённого доступа все требуемые услуги безопасности, такие как аутентификация или конфиденциальность должны быть реализованы с использованием возможностей протоколов более высокого уровня, как описано в 8.3. Общим подходом является использование протоколов туннелирования, такие как IPsec или SSL/TLS, чтобы обеспечить строгую аутентификацию и конфиденциальность.

Для ситуаций, когда организация может конфигурировать беспроводную инфраструктуру для удаленного доступа, требуются дополнительные технические меры, чтобы обезопасить точку доступа. Существуют три современных метода, используемых чтобы обезопасить доступ к AP, которые встроены в протоколы IEEE 802.11:

– Идентификатор установки сервиса (SSID);

– Фильтрация адресов управления общим доступом (MAC);

– Конфиденциальность, равноценная проводной (WEP) или защищенный доступ WiFi (WPA).

Но даже использование всех трёх методов совместно не всегда может обеспечить соответствующую безопасность организации.

SSID предоставляет собой механизм сегментации сети на несколько более мелких подсетей, обслуживаемых одной или несколькими точками доступа (AP). Каждая точка доступа поступает от производителей с установленным по умолчанию идентификатором

SSID, указывающим на производителя этой AP и, возможно, другую информацию, относящуюся к соответствующей AP. Такой SSID должен быть изменён на другой SSID, который не содержит информации об организации, работающей с AP, и о самом оборудовании. Минимальным требованием для AP является запрет широковещательной передачи своего SSID по радиоканалу. С другой стороны, любое слушающее устройство может записать SSID и попытаться соединиться с AP, вызывая правильный SSID. Поэтому строго рекомендуется запрещать конфигурирование AP на режим широковещательной передачи, хотя все равно остаются способы записать SSID, который не передаётся широковещательно.

В то время как SSID идентифицирует AP, MAC-адрес идентифицирует сетевой интерфейс компьютера. Каждая плата сетевого интерфейса имеет уникальный MAC-адрес. Чтобы увеличить безопасность беспроводной ЛВС, AP должна идентифицировать подлинность клиентских компьютеров посредством анализа их MAC-адресов, если такое возможно[1]. Хотя и возможно совпадение MAC-адресов, но это добавляет некоторую защиту доступа к беспроводной ЛВС.

WEP известен как имеющий фундаментальную уязвимость, которая влияет на конфиденциальность, целостность и аутентичность. Однако он предоставляет шифрование при связи, используя секретный ключ длиной 40 или 104 бита. Этот ключ подсоединяется к 24–битному вектору инициализации, в результате длина ключа становится 64- или 128-битной. Из-за известной уязвимости протокола WEP, ключи должны часто изменяться, чтобы увеличить безопасность. WPA (усовершенствованный WEP) преодолевает эти недостатки, если сконфигурирован правильно с предоставлением временных секретных ключей.

В дополнение к этому рекомендуется использование протокола динамической конфигурации настроек хоста (DHCP), предоставляемое AP с возможностью «резервирования клиента» (т.е. компьютерные MAC-адреса привязаны, к определенным IP-адресам) или рекомендуются использовать статические адреса.

В случае использования не маршрутизируемых IP-адресов, измените внутренние IP-адреса подсети (обычно используют 192.168.0.0) на другие адреса подсети. Также запретите беспроводной доступ для администрирования WAP и беспроводного маршрутизатора, чтобы избежать их модификаций атакующими.

Наконец, регулярно оценивайте состояние вашей беспроводной ЛВС.

Подробный перечень рекомендаций по безопасности беспроводной ЛВС приведен в приложении F.

8.6 Организационные меры

Организационные меры должны включать политику удалённого доступа, которая определяет роли пользователей, администраторов и персонала службы безопасности. Также должна быть определена ответственность вовлечённых в эти процессы людей. Пример политики удалённого доступа приводится в Приложении А.

Для некоторых мобильных устройств (например, PDA, смарт-телефон) может быть невыполнимым осуществить достаточную техническую защиту, поэтому может возникнуть потребность в дополнительных организационных мерах по противостоянию рискам.

Другими аспектами организационных мер являются план обеспечения

[1] Ограничение доступа, основанное на MAC-адресе, может быть не целесообразно в большой беспроводной сети или в некоторых рабочих ситуациях.

конфиденциальности, резервное копирование, восстановление информации, обучение персонала, тренинги пользователей и осознание пользователями важности вопроса.

Больше информации по этим вопросам можно найти в [1], [2] и [3].

8.7 Юридические аспекты

Осуществление технологии удалённого доступа должно предприниматься, учитывая все применяемые национальные законы и (или) нормативные ограничения или требования.

Проектировщики должны удостовериться, что учтены должные договорные и другие юридические аспекты удалённого доступа, чтобы быть уверенным в технике в случае непредвиденных обстоятельств.

9 Заключение

Предоставление услуг удалённого доступа требует использования хорошо спланированного подхода, начинающегося с принятия соответствующей политики безопасности, использования необходимых технических средств, а также организационных и юридических мер.

Приложение А
(справочное)

Пример организации политики защиты удалённого доступа

А.1 Цель

Цель данной политики состоит в определении стандартов для соединения с сетью «Компании» с любого хоста. Эти стандарты разработаны, чтобы минимизировать потенциальный ущерб «Компании», который может произойти от неавторизованного использования ресурсов «Компании». Ущерб включает потерю конфиденциальных сведений компании, интеллектуальной собственности, угрозу общественному имиджу компании, угрозу внутренним системам «Компании» и т.д.

А.2 Область применения

Эта политика применяется ко всем служащим, партнёрам, поставщикам, агентам и владельцам «Компании», владельцам персональных компьютеров и рабочих станций, соединяющихся с сетью «Компании». Эта политика применяется к соединениям удаленного доступа, используемым для выполнения работы от имени «Компании», включая чтение или отправку электронной почты и просмотр интернетовских Web-ресурсов.

Данная политика распространяется на выполнение удаленного доступа с использованием модемов, Frame Relay, ISDN, DSL, VPN, SSH, кабельных модемов, и т.д.

А.3 Политика

А.3.1 Общие положения

1) Служащие, партнёры, поставщики, агенты «Компании», имеющие преимущественные права удалённого доступа к корпоративной сети «Компании» несут ответственность за то, что при удалённом соединении они исходят из тех же самых соображений, что и локальные пользователи подключённые к сети «Компании»;

2) Общий доступ в Интернет с персональных компьютеров домашних пользователей через сеть «Компании» разрешается только служащим, которые непосредственно являются работниками «Компании». Служащий «Компании» ответственен за то, что никто из членов семьи не будет нарушать политику «Компании», не будет выполнять незаконной деятельности, и не будет использовать доступ для посторонних деловых интересов. Служащий «Компании» несёт полную ответственность, если доступ будет использоваться неправильно;

3) Пожалуйста, внимательно посмотрите следующие правила защиты информации, при доступе в корпоративную сеть с помощью методов RAS и используемого в сети «Компании»:

a) Принятая политика шифрования;

b) Виртуальная закрытая сеть(VPN);

c) Правила беспроводной связи;

d) Принятые правила эксплуатации.

4) Дополнительную информацию относительно аспектов соединений RAS «Компании», включая порядок заказа или отключения услуги, сравнительные цены, решение возможных проблем и т.д. можно найти на Web-сайте RAS.

А.3.2 Требования

1) Безопасный удалённый доступ должен быть строго контролируемым. Контроль будет выполняться через аутентификацию с однократным паролем или открытые/закрытые ключи со строгой парольной фразой. Информацию о создании строгой парольной фразы см. в разделе Парольная политика;

2) Служащий «Компании» никогда никому, даже членам своей семьи, не должен передавать свой логин или пароль электронной почты;

3) Служащие «Компании» и её партнёры с преимущественными правами удалённого доступа должны быть уверены, что их принадлежащие «Компании» персональные компьютеры или рабочие станции, которые удалённо связываются с корпоративной сетью «Компании», не связываются в одно и то же время с какой-либо другой сетью, за исключением персональной сети, которая находится под полным контролем пользователя;

4) Служащие «Компании» и её партнёры с преимущественными правами удалённого доступа в корпоративную сеть «Компании» не должны использовать учётные записи электронной почты не принадлежащие «Компании» (например, Hotmail, Yahoo, AOL), ни иные внешние ресурсы для выполнения дел «Компании», чтобы иметь уверенность, что официальный бизнес никогда не будет смешан с личным;

5) Маршруты для линий ISDN, сконфигурированных для доступа к сети «Компании» должны соответствовать минимуму требований по аутентификации предъявляемых CHAP;

6) Изменение конфигурации домашнего оборудования пользователя для целей раздельного туннелирования или для его двойного подключения запрещено;

7) Frame Relay должна соответствовать минимуму требований по аутентификации предписанных стандартами DLCI;

8) Нестандартные конфигурации аппаратных средств должны быть одобрены службой RAS, а служба информационной безопасности должна подтвердить безопасность конфигураций для доступа к оборудованию;

9) Все хосты, включая персональные компьютеры, которые соединяются с внутренними сетями «Компании» посредством технологий удалённого доступа, должны использовать современные антивирусные программы (поместите сюда URL корпоративного сайта где размещаются эти программы). Соединение с третьей стороной должно соответствовать требованиям, установленным в соглашении с третьей стороной;

10) Личное оборудование, которое используется для подсоединения к сетям «Компании», должно соответствовать требованиям к оборудованию, принадлежащему «Компании»;

11) Организации или лица, желающие осуществить нестандартные решения по удалённому доступу к сети «Компании» должны предварительно получить согласование от службы удаленного доступа и службы информационной безопасности.

А.4 Принудительное проведение политики

Любое лицо, нарушившее данную политику, может быть подвергнуто дисциплинарным мерам, включая увольнение с работы.

А.5 Термины и определения

Кабельный модем: Некоторые кабельные компании предоставляют доступ к Интернет по телевизионному кабелю.

Телевизионный коаксиальный кабель: Этот коаксиальный кабель, который соединяется с кабельным модемом, по нему данные из Интернета передаются со скоростью более 1,5 Мб/с. В настоящее время кабель применяется только в некоторых случаях.

CHAP: Протокол аутентификации «запрос соединения» − способ аутентификации, который использует одностороннюю функцию хэширования.

DLCI: Идентификатор соединения при передаче данных. Уникальный номер для непрерывной виртуальной сети (VPC), присваиваемый конечной точке в сети Frame Relay. DLCI идентифицирует конечную точку в обычных VPC внутри пользовательского каналом доступа в сети Frame Relay и имеет локальную значимость только для этого канала.

Телефонный модем: Периферийное устройство, которое соединяет компьютеры один с другим для передачи данных через телефонные линии. Модем преобразует цифровые данные компьютеров в аналоговые сигналы (модуляция) для посылки через телефонные линии, и преобразует принятые аналоговые сигналы в цифровые (демодуляция), читаемые компьютером на другом конце линии, таким образом, название модем означает модулятор/демодулятор.

Двойное подключение: Возможность подключения более чем к одной сети компьютера или сетевого устройства. Например, в момент соединения с корпоративной сетью через локальную Ethernet связь, осуществить подключение к провайдеру Интернет (ISP). Или, находясь в сети «Компании», предоставляющей удалённый доступ из дома, соединяется с другой сетью, например с сетью компании супруга. Или, сконфигурировать маршрутизатор ISDN для соединения с «Компанией» и с ISP в зависимости от назначения пакетов.

DSL: Цифровой абонентский канал является формой высокоскоростного доступа в Интернет, конкурирующей с кабельными модемами. DSL работает через стандартные телефонные линии и поддерживает скорости входящего потока данных до 2 Мб/сек, и меньшие величины скоростей для исходящего потока.

Frame Relay: Способ связи, при котором можно менять пошагово от скорости соединения от скорости ISDN до скорости линии T1. Frame Relay использует фиксированную тарифную ставку в зависимости от скорости вместо использования повременной оплаты. При Frame Relay соединяются через сеть телефонной компании.

ISDN: Существует два вида услуг цифровой сети с интегрированным севисом или ISDN: BRI и PRI. BRI используется для домашних офисов/удалённого доступа. BRI имеет два скоростных канала по 64 килобита (вместе 128 килобит) и 1D канал для передачи сигнальной информации.

Удалённый Доступ: Любой доступ к корпоративной сети «Компании» через сеть, устройство или среду, не контролируемые «Компанией».

Раздельное туннелирование: Одновременный прямой доступ к сети, не принадлежащей компании (Интернет или домашняя сеть), с удаленного устройства (ПК, PDA, WAP телефон и т.д.) во время соединения с корпоративной сетью «Компании» через VPN-туннель. Виртуальная закрытая сеть (VPN) − метод доступа к удалённой сети посредством туннелирования через Интернет.

Приложение В
(справочное)

Рекомендации по внедрению и установке RADIUS

В.1 Общие положения

В этом приложении даются рекомендации по использованию RADIUS в среде Microsoft Windows 2000 и в других операционных системах.

Чтобы работать с RADIUS безопасно, вы должны следовать следующим указаниям.

В.2 Рекомедации по внедрению

Когда вы используете клиентов сервера или прокси-сервера RADIUS, следуйте следующим рекомендациям:

Чтобы обеспечить конфиденциальность данных RADIUS, применяйте IPsec, с использованием ESP и алгоритм шифрования, такой как, например, 3DES.

Это описано в [31]. При шифровании всех сообщений RADIUS с помощью IPsec, критичные поля сообщений RADIUS (такие, например, как поле запроса аутентификатора в сообщении Запрос-Доступа) и атрибуты (такие, например, как пароль пользователя, пароль туннеля и атрибуты ключа MPPE) защищаются от просмотра. Атакующий должен сначала расшифровать сообщения RADIUS, защищённое ESP, до того как станет возможным анализировать содержание сообщений RADIUS. Чтобы препятствовать атакующему организовывать атаки против сервера RADIUS при подключении к нему, рекомендуется поддерживать аутентификацию, основанную на сертификате IPsec.

Альтернативно, или совместно с использованием IPsec, вам необходимо:

1) Сконфигурировать и использовать секретные ключи, длиной не менее 32 шестнадцатеричных символов или, не менее 22 клавиатурных символов;

2) Использовать атрибут аутентификатора сообщения для всех сообщений запроса доступа;

Для клиента RADIUS использовать атрибут аутентификатора сообщения для всех сообщений запроса доступа и включить его в конфигурации. Для сервера или прокси-сервера RADIUS требуется использовать атрибут аутентификатора сообщения для сообщений вида Запрос-Доступа и включить его в конфигурации.

3) Используйте криптографически стойкий генератор случайных чисел для аутентификатора запроса.

Чтобы обеспечить дополнительную защиту для аутентификации клиента при внедрении RADIUS используйте следующие рекомендации:

1) Применяйте протоколы EAP и подобные EAP, которые используют строгие методы аутентификации;

Примером строгого метода EAP является EAP-TLS, который требует изменения сертификатов клиента доступа и сервера RADIUS. Все сообщения EAP требуют использования атрибута аутентификатора сообщения, что обеспечивает защиту сообщений запроса доступа, которые не защищены IPsec.

2) Используйте методы аутентификации, которые требуют использования взаимной аутентификации;

При взаимной аутентификации обе стороны соединения аутентифицируют своего партнёра. Если одна из аутентификаций не удалась, попытка соединения отклоняется. Например, EAP-TLS и MS-CHAP версии 2 являются методами взаимной аутентификации.

При использовании EAP-TLS сервер RADIUS подтверждает подлинность сертификата пользователя клиента доступа, а клиент доступа подтверждает подлинность компьютерного сертификата сервера RADIUS. При использовании MS-CHAP версии 2 и клиент доступа, и сервер доступа подтверждают знание пароля учётной записи пользователя.

3) Если вы применяете аутентификацию PAP, сделайте её использование недоступным по умолчанию;

Например, OTP/токен-карта использует PAP, чтобы послать аутентификационную информацию. Если вам необходимо использовать протокол PAP, сделайте его использование недоступным по умолчанию и применяйте длинные секретные ключи и криптографически качественные аутентификаторы запроса. Из-за того, что IEEE 802.1X не поддерживает PAP, это положение применимо только к соединениям PAP.

4) Если вы применяете аутентификацию CHAP, используйте строгий запрос CHAP;

Подобно аутентификатору запроса RADIUS, запрос CHAP должен быть случайным и криптографически качественным.

5) Если вы применяете аутентификацию MS-CHAP, не пользуйтесь поддерживающимся менеджерами ЛВС шифрованием для ответов на запрос MS-CHAP или изменения паролей.

В.3 Рекомендации по установке

Чтобы работать с RADIUS безопасно, при установке RADIUS, выполняйте следующие рекомендации:

Чтобы обеспечить конфиденциальность данных для всего сообщения RADIUS конфигурируйте ваших клиентов и сервер RADIUS так, чтобы использовать IPsec совместно с ESP и с, например, 3DES для всех трафиков RADIUS.

Конфигурация IPsec для использования с ESP и 3DES зависит от применяемого IPsec. Например, если вы используете Windows 2000 для маршрутизации и услуг удалённого доступа как сервер доступа и Windows 2000 IAS как сервер RADIUS в окружении Active Directory™, вы имеете возможность сконфигурировать активную политику IPsec для соответствующего контейнера системы с правилом, чтобы использовался ESP с 3DES шифрованием для всех входящих и исходящих трафиков портов 1812 и 1813 UDP. Для получения большей информации смотри меню «Помощь» в сервере Windows 2000.

Альтернативно или совместно с использованием IPsec, вам необходимо:

1) Использовать стойкие секретные ключи, состоящие из случайной последовательности длиной не менее 32 шестнадцатеричных знаков или из случайной последовательности символов клавиатуры верхнего и нижнего регистров, чисел и знаков пунктуации длиной не менее 22 символа. В идеальном случае, секретные ключи должны быть сгенерированы компьютером;

2) Используйте различные совместные секретные ключи для каждой пары клиент-сервер RADIUS;

3) Используйте атрибут аутентификатора сообщения для сообщений запроса доступа. Конфигурируйте каждого клиента RADIUS так, чтобы он посылал атрибут аутентификатора сообщения со всеми сообщениями запроса доступа. Конфигурируйте каждый сервер RADIUS так, чтобы требовать от каждого клиента RADIUS атрибут аутентификатора сообщения в сообщениях запроса доступа.

4) Используйте клиентов сервера и прокси-сервера RADIUS, которые используют криптографически стойкие аутентификаторы запроса.

Чтобы обеспечить дополнительную защиту для аутентификации доступа клиента при установке RADIUS, используйте следующие рекомендации:

1) Если протокол PAP не требуется, запретите его использование на сервере доступа и на сервере RADIUS. Единственным приемлемым вариантом использования PAP для безопасных соединений является применение аутентификации с разовым паролем и токен-картой, когда пароль имеет высокую энтропию и изменяется при каждом использовании. Однако, доступность PAP позволяет незарегистрированным клиентам использовать PAP с их серверов доступа и посылать незащищенные пароли учётных записей пользователя. Более правильным решением является использование протокола EAP или подобного EAP для аутентификации с однократным паролем и токен-картой.

2) Если требуется использовать MS-CHAP запретите использование шифрование менеджером ЛВС;

Если вы используете Windows 2000 IAS, установите значение ключа регистра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteAccess\Policy\Allow LM Authentication в 0 на сервере IAS.

3) Используйте протокол EAP или подобный EAP с методом строгой аутентификации;

Аутентификация протокола IEEE 802.1x для беспроводного доступа требует использования EAP, используйте также атрибут аутентификации сообщения, для защиты каждого сообщения запроса доступа и не используйте аутентификацию PAP.

4) Используйте метод взаимной аутентификации такой как EAP- TLS или MS-CHAP версии 2.

Приложение С
(справочное)

Два режима FTP

Существуют два режима FTP:
- режим PORT FTP;
- режим PASV FTP.

С.1 Режим PORT FTP

Режим PORT FTP является традиционным режимом FTP. Последовательность действий при установлении соединений в PORT FTP должна быть следующей:

1) **Клиент FTP:** Открывает случайно откликнувшийся порт в диапазоне больших номеров. (Для примера, мы будем считать ими порты 6000 и 6001 TCP);

2) **Клиент FTP:** Посылает запрос для открытия канала команд из порта 6000 TCP в порт 21 TCP сервера FTP;

3) **Сервер FTP:** Посылает «ОК» из порта 21 TCP в порт 6000 TCP клиента FTP (организуется командный канал). В этот момент устанавливается командный канал;

4) **Клиент FTP**: Посылает запрос данных (команда PORT) в сервер FTP. Клиент FTP включает в команду PORT номер порта данных, который он открыл для получения данных. В данном примере клиент FTP открыл порт 6001 TCP для получения данных;

5) **Сервер FTP:** Сервер FTP открывает *новое* входящее соединение к клиенту FTP через порт, указанный клиентом FTP в команде PORT. Исходящим портом сервера FTP является порт 20 TCP. В данном примере сервер FTP посылает данные из своего собственного порта 20 TCP в порт 6001 TCP клиента FTP.

В этом примере были установлены два соединения: исходящее соединение, инициированное клиентом FTP, и входящее соединение, установленное сервером FTP. Заметьте, что информация, содержащаяся в команде PORT (посланная через командный канал), сохраняется внутри пакета данных.

С.2 Режим PASV FTP

Наиболее популярной реализацией FTP является режим PASV или пассивный режим. Режим PASV соединений FTP является наиболее популярным в большинстве браузеров. Одним из основных преимуществ режима PASV является то, что серверу не нужно создавать новое входящее соединение к клиенту FTP. Как мы увидим дальше, это делает режим PASV FTP более дружественным к межсетевым экранам.

Последовательность действий для режима PASV соединений FTP должна быть следующей:

1) **Клиент FTP:** Открывает случайно откликнувшийся порт в диапазоне больших номеров. (Для примера, мы будем считать ими порты 6000 и 6001 TCP);

2) **Клиент FTP**: Посылает запрос для открытия канала команд из порта 6000 TCP в порт 21 TCP сервера FTP;

3) **Сервер FTP**: Посылает «ОК» из порта 21 TCP в порт 6000 TCP клиента FTP (организуется командный канал). В этот момент устанавливается командный канал;

4) **Клиент FTP**: Посылает команду PASV, запрашивающую чтобы сервер FTP открыл номер порта, с которым клиент FTP может соединиться, чтобы организовать канал данных;

5) **Сервер FTP**: Посылает через командный канал номер порта TCP, через который клиент FTP может инициировать соединение, чтобы установить канал данных. В данном примере сервер FTP открывает порт 7000;

6) **Клиент FTP:** Открывает *новое* соединение из своего собственного отвечающего порта 6001 TCP к каналу данных 7000 сервера FTP. Передача данных идет через этот канал.

Заметьте, что в режиме PASV все соединения инициирует клиент FTP. Серверу FTP нет необходимости для создания нового возвратного соединения с клиентом FTP.

Приложение D
(справочное)

Перечень проверок безопасной работы почты

Следующие перечни помогут конфигурировать, планировать и поддерживать работу почтового сервера. Проверки приведены для операционной системы, почтовой программы, фильтров и т.д. [6].

D.1 Перечень проверок операционной системы почтового сервера

Выполнение	Действие
	План конфигурации и развёртывания почтового сервера
○	Определение функций почтового сервера
○	Определение категорий информации, которая будет сохраняться, обрабатываться и передаваться через почтовый сервер
○	Определение требований к безопасности информации
○	Определение выделенного хоста для этого сервера
○	Определение сетевых услуг, которые будут предоставляться или поддерживаться данным сервером
○	Определение пользователей и категорий пользователей, и определение прав каждой категории пользователей
○	Определение методов аутентификации для почтового сервера
	Выбор операционной системы для почтового сервера
○	Минимальная подверженность уязвимости
○	Способность административно ограничить деятельность с правами администратора только для назначенных пользователей, прошедших авторизацию
○	Способность отклонять доступ к информации на сервере для неавторизованных лиц
○	Способность сделать недоступными услуги сервера, встроенные в операционную систему и программное обеспечение в которых нет необходимости
○	Приемлемая стоимость гарантий и уверенности (некоторая уверенность обеспечивается использованием определенных операционных систем)
○	Наличие опытного персонала для установки, конфигурирования, технического обслуживания и соблюдения требований безопасности системы
	Установка сервис-паков (исправлений) и обновлений операционной системы
○	Определение и установка всех необходимых сервис-паков и обновлений операционной системы
○	Определение и установка всех необходимых сервис-паков и обновлений для всех приложений и сервисов, включая встроенные в операционную систему
	Удаление или запрет ненужных сервисов и приложений
○	Удаление или запрет сервисов и приложений, в которых нет необходимости

Выполнение	Действие
	Конфигурирование аутентификации пользователя в операционной системе
○	Удалить или сделать недоступными все неиспользуемые учётные записи и группы
○	Заблокировать неактивные учётные записи
○	Создать группы пользователей для конкретного компьютера
○	Создать учётные записи пользователей для конкретного компьютера
○	Проверить политику паролей организации (т.е. длина, сложность) и установить соответствующие пароли
○	Сконфигурировать компьютер, чтобы отклонять регистрацию пользователя после ограниченного числа неудачных попыток
○	Установить и сконфигурировать другие механизмы для усиления аутентификации
	Проверка безопасности операционной системы
○	Провести тестирование операционной системы после её установки для определения уязвимостей.
○	Осуществлять периодическую проверку операционной системы (например, поквартально), для выявления новых уязвимостей.

D.2 Перечень проверок почтового сервера и безопасности содержимого

Выполнение	Действие
	Инсталляция почтового сервера
○	Установка программного обеспечения на выделенный хост
○	Установка минимально требуемых сервисов Интернет
○	Установка сервис паков и обновлений для исправления уже известных уязвимостей
○	Удаление или блокировка всех сервисов, установленных, но не используемых на почтовом сервере, (например, использующей Web почты, FTP, удалённого администрирования)
○	Удалить с сервера всю документацию от поставщиков.
○	Применить к серверу соответствующий шаблон безопасности или инсталлировать скрипт на сервере
○	Реконфигурировать отклики сервисов SMPT, POP и IMAP (и других при необходимости), чтобы не было видно, что это почтовый сервер, тип операционной системы и версию
○	Заблокировать опасные или ненужные почтовые команды (например, VRFY EXPN)
	Конфигурирование операционной системы и управление доступом к почтовому серверу
○	Ограничить доступ приложений сервера к вычислительным ресурсам
○	Ограничить доступ пользователей через дополнительные средства управления доступом, выполняемые почтовым сервером, если требуется более детальные уровни контроля доступа
○	Сконфигурировать приложения почтового сервера, чтобы действия могли выполняться только при идентификации группы, идентификации пользователя с контролем ограничения доступа

Выполнение	Действие
○	Удостовериться, что почтовый сервер не запущен с правами root или системного администратора
○	Сконфигурировать операционную систему хоста так, чтобы этот почтовый сервер мог писать файлы регистрации, но не читать их
○	Сконфигурировать операционную систему хоста так, чтобы временные файлы, созданные приложениями почтового сервера были ограничены для доступа и находились в соответствующим образом защищённой поддиректории
○	Сконфигурировать операционную систему хоста так, чтобы доступ к любым временным файлам, созданным приложениями почтового сервера, ограничивались процессами почтового сервера, которыми создаются этими файлы
○	Убедиться, что почтовый сервер не может сохранять файлы вне файловой структуры, выделенной этому серверу
○	Сконфигурировать почтовый сервер, чтобы запретить команду chroot при использовании операционных систем Linux или Unix
○	Установить почтовые ящики пользователей на других жестких дисках или логических разделах, чем операционная система и приложения почтового сервера
○	Удостоверьтесь, что регистрационные файлы сохраняются в месте, которое имеет достаточный размер
	Борьба с вредоносными вложениями и содержимым
○	Установить централизованный сканер вирусов (на шлюзе электронной почты, на межсетевом экране и (или) на почтовом сервере)
○	Установить сканеры вирусов на всех клиентских хостах
○	Обновлять все вирусные базы данных на всех сканерах или еженедельно или когда обнаружено заражение вирусом
○	Обучить пользователей опасностям, возникаемым при поражении вирусом, и способам уменьшения этой опасности
○	Уведомлять пользователей о случае заражения
○	Сконфигурировать фильтрацию содержимого, чтобы заблокировать подозрительные сообщения
○	Сконфигурировать фильтрацию содержимого, чтобы заблокировать сообщения UCE (Unsolicited Commercial E-mail), т.е. спам.
○	Сконфигурировать лексический анализ, если требуется
○	Создать дополнительную политику фильтрации
○	Добавить юридическое уведомление к электронной почте, если требуется
○	Сконфигурировать почтовый сервер, чтобы заблокировать почту с адресов из черного списка, полученного из открытых источников
○	Сконфигурировать почтовый сервер, чтобы заблокировать почту с конкретных доменов, если потребуется
○	Сконфигурировать аутентификацию почты, предназначенной для сквозной трансляции через сервер
○	Сконфигурировать почтовый сервер, чтобы использовать шифрованную аутентификацию
○	Сконфигурировать почтовый сервер, чтобы поддерживать доступ к Web только через SSL/TLS и только, если такой доступ необходим

D.3 Перечень проверок инфраструктуры сети

Выполнение	Действие
	Расположение сети
○	Почтовый сервер должен располагаться во внутренней сети и защищаться почтовым шлюзом и (или) межсетевым экраном, или почтовый сервер должен располагаться в демилитаризованной зоне
	Конфигурация межсетевого экрана
○	Почтовый сервер должен защищаться межсетевым экраном
○	Почтовый сервер, если он находится под угрозой или более уязвим, необходимо защищать межсетевым экраном уровня приложений
○	Межсетевой экран должен контролировать весь трафик между Интернетом и почтовым сервером
○	Межсетевой экран должен блокировать весь входящий трафик к почтовому серверу, за исключением порта 25 TCP (SMPT), порта 110 TCP (POP3), порта 143 TCP (MAP), порта TCP 398 (LDAP) и порта 636 TCP (безопасный LDAP), если требуется
○	Межсетевой экран должен блокировать (вместе с системой обнаружения вторжения (Intrusion-Detection System, IDS)) IP адреса или подсети с которых, по сообщению системы обнаружения вторжений, контролируемая сеть подвергается атаке
○	Межсетевой экран должен оповещать сетевого администратора или администратора почтового сервера о подозрительной активности через соответствующие средства
○	Межсетевой экран должен обеспечивать фильтрацию содержимого (межсетевой экран уровня приложений)
○	Межсетевой экран должен быть сконфигурирован, чтобы защищать против атак типа отказ в обслуживании (Denial of Service, DoS)
○	Межсетевой экран должен регистрировать критические события
○	На межсетевой экран и операционную систему должна производиться установка сервис-паков и обновлений последнего и наиболее безопасного уровня.
	Системы обнаружения вторжения
○	Сконфигурировать IDS, чтобы контролировать сетевой трафик перед любым межсетевым экраном или маршрутизатором (основной сети)
○	Сконфигурировать IDS, чтобы контролировать входящий и исходящий сетевой трафик почтового сервера после межсетевого экрана.
○	Сконфигурировать IDS, чтобы контролировать изменения в критических файлах на почтовом сервере (встроенными средствами или программой проверки целостности файлов)
○	IDS должен блокировать (вместе с межсетевым экраном) IP адреса или подсети, из которых атакуют сеть организации
○	IDS должен уведомлять сетевого или почтового администратора об атаках через соответствующие средства
○	Сконфигурировать IDS, чтобы определять сканируемый порт
○	Сконфигурировать IDS, чтобы обнаруживать DoS-атаки
○	Сконфигурировать IDS, чтобы регистрировать события

Выполнение	Действие
○	По возможности часто обновлять IDS новыми сигнатурами атак (в основном еженедельно)
○	Сконфигурировать IDS, чтобы контролировать системные ресурсы доступные почтовому серверу (расположенном на хосте)
	Сетевые коммутаторы
○	Сетевые коммутаторы необходимо использовать на сегменте почтового сервера, для защиты от сетевого подслушивания
○	Сетевые коммутаторы должны быть сконфигурированы в режиме с повышенной защитой, чтобы защитить от атак с имитацией протокола ARP и с подменой результата запроса ARP
○	Сетевые коммутаторы должны быть сконфигурированы, чтобы направлять весь трафик сегмента сети через хост IDS (базовой сети)

D.4 Перечень проверок безопасности почтового клиента

Выполнение	Действие
	Установка сервис-паков и обновлений для почтовых клиентов
○	Обновите почтового клиента до наиболее безопасной версии
○	Примените все необходимые сервис-паки для почтового клиента
○	Примените все необходимые сервис-паки к браузеру (для почтовых клиентов, которые интегрированы с браузером (например, Outlook и Netscape)
	Безопасность почтового клиента
○	Удостоверьтесь, что в операционной системе установлены сервис-паки и обновления до наиболее безопасного уровня
○	Сконфигурируйте операционную систему так, чтобы позволить доступ к локально сохраненным сообщениям и файлам конфигурации почтового клиента только соответствующим пользователям
○	Обезопасьте или удалите скрипты Windows (для хостов с Windows)
○	Измените действия по умолчанию над файлами, связанными со скриптами Windows от выполнения до редактирования (только для хостов с Windows)
○	Удостоверьтесь, что операционная система сконфигурирована, чтобы показывать полное расширение имён файлов (только хосты с Windows)
○	Удостоверьтесь, что критические компоненты операционной системы защищены от злонамеренного кода
○	Используйте систему шифрования файлов для защиты почты, сохраняемой локально на жестком диске пользователя (в особенности это важно для переносных компьютеров)
○	Сконфигурируйте клиентскую операционную систему, чтобы она после фиксированного периода бездействия для автоматически блокировалась

D.5 Перечень проверок безопасного администрирования почтового сервера

Выполнение	Действие
	Регистрация
○	Регистрируйте ошибки установки IP стека
○	Регистрируйте проблемы разрешения имен и адресов (например, DNS, NIS,WINS)
○	Регистрируйте ошибки конфигурации почтового сервера (например, несоответствием с DNS, ошибки локальной конфигурации, отсутствием в базе данных псевдонимов)
○	Регистрируйте неприемлемые изменения разрешений доступа к файлам и каталогам, небезопасные символьные и аппаратные связи
○	Регистрируйте использование псевдонимов из устаревшей базы данных
○	Регистрируйте недостаток системных ресурсов (например, дисковое пространство, память, CPU)
○	Регистрируйте реконструкции базы данных псевдонимов
○	Регистрируйте регистрации в системе (успешные и нет)
○	Регистрируйте проблемы безопасности (например, спам)
○	Регистрируйте потери связи (сетевые проблемы)
○	Регистрируйте протоколы ошибок
○	Регистрируйте тайм-ауты связи
○	Регистрируйте отказы от связи
○	Регистрируйте использование команд VRFY и EXPN
○	Регистрируйте имена отправителей
○	Регистрируйте формат отправки
○	Регистрируйте загрузки файлов
○	Регистрируйте некорректные адреса
○	Регистрируйте статистику сообщений
○	Регистрируйте создание сообщений об ошибках
○	Регистрируйте неудачные доставки (долговременные ошибки)
○	Регистрируйте отложенные сообщения (кратковременные ошибки)
○	Сохраняйте протоколы регистраций на отдельном (syslog) хосте
○	Архивируйте протоколы регистраций согласно организационным требованиям
○	Ежедневно анализируйте файлы регистрации
○	Еженедельно анализируйте файлы регистрации (для выявления более долгосрочных тенденций)
○	Используйте инструментарий для автоматизированного анализа файлов регистрации
	Резервное копирование почтового сервера
○	Разработайте политику резервного копирования почтового сервера
○	Осуществляйте инкрементальное резервное копирование почтового сервера в основном ежедневно в течение недели
○	Осуществляйте полное резервное копирование почтового сервера в основном еженедельно в течении месяца
○	Периодически архивируйте резервные копии

Выполнение	Действие
	Восстановление после компрометации
○	Поступайте в соответствии с политикой безопасности организации (это должно быть более приоритетно перед данными рекомендациями)
○	Отсоедините скомпрометированную систему от сети и примите меры по сохранению следов атаки, для сбора дополнительных свидетельств
○	Изучите сведения об «аналогичных» хостах, чтобы установить, подверглись ли нападению другие системы
○	Проконсультируйтесь с руководством фирмы, юристами и правоохранительными органами (немедленно уведомите правоохранительные органы, если предполагается судебное обвинение)
○	Проанализируйте вторжение
○	Восстановите систему
○	Вновь подключите систему в сеть
○	Протестируйте систему, чтобы удостовериться в её безопасности
○	Проведите мониторинг системы и сети для определения признаков того, что нападающий вновь пытается получить доступ к системе или сети
○	Изучите документы по прошедшим событиям

Приложение Е
(справочное)

Перечень проверок Web-служб

Следующий перечень проверок предназначен для планирования, инсталляции и безопасной эксплуатации Web-сервера [5].

Е.1 Перечень проверок операционной системы Web-сервера

Выполнение	Действие
	Планирование конфигурации и развертывания Web-сервера
○	Определите функции Web-сервера
○	Определите категории информации, которые будут загружаться, обрабатываться, и передаваться через Web-сервер
○	Определите требования по безопасности информации
○	Определите методы опубликования информации на Web-сервере
○	Определите выделенный хост для инсталляции Web-сервера
○	Определите сетевые услуги, которые будут предусмотрены или поддерживаемы Web-сервером
○	Определите категории пользователей Web-сервера и определите привилегии для каждой категории пользователей
○	Определите методы аутентификации пользователя на Web-сервере
	Критерии выбора операционной системы для Web-сервера
○	Минимальное время раскрытия уязвимых мест
○	Способность ограничивать деятельность на административном или корневом уровне только уполномоченным пользователям
○	Способность запрещать доступ к информации на сервере всем, кроме тех, кому она предназначается
○	Способность блокировать необязательные сетевые услуги, которые могут быть встроены в операционную систему или программное обеспечение сервера
○	Приемлемые издержки страхования и ответственности (для некоторых операционных систем необходимо увеличение страховых расходов)
○	Наличие опытного персонала, чтобы устанавливать, конфигурировать, обезопасить, и сопровождать операционную систему.
	Установка патчей и обновлений для операционной системы
○	Определите и установите все необходимые патчи и обновления для операционной системы
○	Определите и установите все необходимые патчи и обновления для приложений и сервисов, включенных в операционную систему
○	Удалите или заблокируйте необязательные услуги и приложения
○	Сконфигурируйте аутентификацию пользователя операционной системы
○	Удалите или заблокируйте ненужные учетные записи и группы, заведенные по умолчанию
○	Заблокируйте неактивные учетные записи
○	Создайте группы пользователей для конкретного компьютера
○	Создайте учетные записи пользователей для конкретного компьютера

Выполнение	Действие
○	Проверьте политику организации паролей (например: длина, сложность) и установите соответствующие пароли
○	Сконфигурируйте компьютер, чтобы запрещать вход после ограниченного количества неудачных попыток
○	Установите и конфигурируйте другие механизмы безопасности, чтобы усилить аутентификацию
	Проверки безопасности операционной системы
○	Протестируйте операционную систему после инсталляции, чтобы определить уязвимые места
○	Проводите периодическое тестирование операционной системы (например: поквартально), чтобы определять новые уязвимые места

Е.2 Перечень действий по безопасной установке и конфигурации Web-сервера

Выполнение	Действие
	Безопасная установка Web-сервера
○	Установите программное обеспечение сервера на выделенном хосте
○	Установите минимально требуемые услуги Интернет
○	Установите патчи или обновления, чтобы исправить известные уязвимые места
○	Для содержимого Web специально выделите физический диск или логический раздел (отделите от операционной системы и приложений сервера)
○	Удалите или заблокируйте все услуги, установленные Web-сервером но не требуемые (например, gopher, FTP, и дистанционное администрирование)
○	Удалите все образцы документов, скрипты (макросы) и выполняемый код
○	Удалите с сервера всю документацию поставщиков
○	Примените подходящий шаблон безопасности или инсталлируйте необходимые скрипты (макросы) на сервере
○	Переконфигурируйте заголовок сервиса HTTP (и других, если потребуется), чтобы НЕ сообщать, что это Web-сервер, тип и версию операционной системы
	Конфигурирование управления доступом операционной системы хоста Web-сервера
○	Сконфигурируйте так, чтобы содержимое файлов на Web можно было прочитать, но не записать с помощью услуг процессов Web-сервера
○	Сконфигурируйте так, чтобы сервисные процессы Web-сервера не могли записывать в каталоги, где хранится открытое содержимое Web
○	Сконфигурируйте так, чтобы только процессы, уполномоченные для администрирования Web-сервера, могли записывать файлы содержимого Web
○	Сконфигурируйте так, чтобы приложение Web могло писать регистрационные файлы Web-сервера, но файлы регистрации не могли быть прочитаны приложением Web-сервера
○	Сконфигурируйте так, чтобы временные файлы, созданные приложением Web-сервера, были сосредоточены в определенных и, соответственно, защищенных подкаталогах

Выполнение	Действие
○	Сконфигурируйте так, чтобы доступ к любым временным файлам созданным приложением Web-сервера, ограничивался процессами сервиса Web, который создавал эти файлы
○	Установите содержимое Web на другой накопитель (на жесткий диск или в логический раздел), чем операционная система и приложения Web
○	Сконфигурируйте так, чтобы если загрузка в сервер Web разрешена, было соответствующее ограниченное пространство на жестком диске, который выделен для этой цели
○	Удостоверьтесь, что регистрационные файлы сохраняются в месте, которое имеет достаточный размер
	Конфигурирование безопасного каталога для содержимого Web
○	Выделите отдельный накопитель на жестком диске или логический раздел для Web, и устанавливайте в связанные подкаталоги исключительно файлы для Web сервера, включая графику, но исключая скрипты и другие программы
○	Выделите единственный каталог исключительно для всех внешних скриптов или программ, выполняемых как часть содержимого Web-сервера (например, CGI, ASP)
○	Блокируйте выполнение скриптов, которые не находятся исключительно под управлением административной учетной записи. Это действие выполняется для создания и управления доступом к отдельному каталогу, содержащему скрипты авторизации
○	Создайте группы пользователей для компьютера
○	Заблокируйте использование коротких связей к аппаратуре или символам (таких как, ярлыки в Windows).
○	Определите полную форму доступа к Web. Определите все папки, и установите - какие документы в пределах Web сервера должны быть ограничены по доступу, а какие доступны (и кому)
○	Проверьте политику паролей организации (например: длина, сложность) и установите соответственно пароли
○	Используйте файл robots.txt, если возможно
	Использование проверок файловой целостности
○	Установите проверку файловую целостности, чтобы защищать файлы конфигурации Web-сервера, файлы паролей и содержимого Web
○	Обновляйте контрольные суммы файловой целостности всякий раз, когда производите улучшение или изменение содержимого
○	Храните контрольную сумму на защищенном от записи носителе
○	Регулярно сравнивайте контрольные суммы

Е.3 Перечень проверок содержимого Web

Выполнение	Действие
	Убедитесь, что ни один из следующих типов информации не доступен на или через открытый Web-сервер
○	Секретные или критичные записи
○	Внутренние правила и процедуры для персонала
○	Конфиденциальная или частная информация
○	Записи ведения расследования

Выполнение	Действие
○	Финансовые записи (кроме тех, что уже опубликованы)
○	Процедуры организации физической и информационной безопасности
○	Информация об организации сети и инфраструктуре информационной системы
○	Охраняемый авторским правом материал без письменного разрешения владельца
○	Секретности или политика безопасности, которые указывают типы мер безопасности на месте
	Установите общеорганизационную зарегистрированную формальную политику для одобрения общедоступного содержимого Web
○	Определите информацию, которая должна быть опубликована на Web
○	Определите целевую аудиторию
○	Определите возможные отрицательные последствия опубликования информации
○	Определите, кто должен быть ответственным за создание и публикацию этой конкретной информации
○	Определите руководящие принципы для стилей и форматов, используемых для публикации на Web
○	Обеспечьте приемлемый просмотр информации по управлению критичными данными и их распространением/публикацией (включая критичную информацию в целом)
○	Определите правила доступа и управления безопасностью
○	Создайте руководство по информации, содержащейся внутри исходного кода содержимого Web
	Соображения по конфиденциальности для пользователя Web
○	Опубликованная политика конфиденциальности
○	Запрещение сбора личных данных без явного разрешения пользователя
○	Запрещение на использование "постоянных" Куки-файлов (англ. cookies)
○	Если используются сеансовые куки-файлы, они должны быть ясно определены в опубликованной политике конфиденциальности
	Соображения по обеспечению безопасности активного содержимого на стороне клиента
○	Используйте его только тогда, когда это абсолютно необходимо
○	Не используйте действий по умолчанию без специального разрешения пользователя
○	Не используйте активное содержимое с высоким риском на стороне клиента
○	Когда возможны альтернативы, используйте их (например: простой текст наряду с форматом PDF)
	Соображения по обеспечению безопасности активного содержимого на стороне сервера
○	Стремитесь к простоте и легкости понимания кода
○	Введите ограничения по чтению и записи файлов
○	Ограничьте или исключите взаимодействия с другими программами (например, sendmail)
○	Не используйте работу с привилегиями пользователя «suid»

Выполнение	Действие
○	Используйте явно заданные имена путей (то есть, не полагайтесь на переменную имени пути)
○	Исключайте каталоги с привилегиями записи и исполнения
○	Все исполняемые файлы располагайте в выделенных папках
○	Заблокируйте SSI
○	Проверяйте всё, что вводит пользователь
○	Динамически созданные страницы не должны создавать опасных метасимволов
○	Набор символов кодирования должен быть явно установлен для каждой страницы
○	Данные пользователя должны сканироваться на наличие байтовых последовательностей, соответствующим специальным символам для данной схемы кодирования
○	Куки должны быть изучены на наличие любых специальных символов
○	Используйте механизм шифрования, чтобы шифровать пароли, введенные через формы скриптов
○	Для приложений Web, которые ограничены именем пользователя и паролем, ни одна из страниц Web в приложении не должна быть доступна без прохода через соответствующий процесс регистрации входа
○	Удалите все образцы скриптов
○	Никакие скрипты третьей стороны или выполняемый код не должны применяться без проверки исходного кода

Е.4 Перечень проверок Web-аутентификации и шифрования

Выполнение	Действие
	Технологии Web-аутентификации и шифрования
○	Для ресурсов Web, которые требуют минимальной защиты и для которых есть небольшая, ясно определенная аудитория, конфигурируйте аутентификацию, основанную на адресе
○	Для ресурсов Web, которым требуется дополнительная защита, но для которых есть небольшая, ясно определённая аудитория, конфигурируйте аутентификацию, основанную на адресе, как вторую линию защиты
○	Для ресурсов Web, которым требуется минимальная защита, но для которой нет ясно определенной аудитории, конфигурируйте основную или частичную (лучше) аутентификацию
○	Для ресурсов Web, которым требуется защита от злонамеренных роботов поисковых систем, конфигурируйте основную или частичную (лучше) аутентификацию
○	Для ресурсов Web, которым требуется максимальная защита, конфигурируйте SSL/TLS
	Конфигурирование SSL/TLS
○	Для конфигураций, которые требуют минимальную аутентификацию но требуют шифрование, используется собственный сертификат
○	Для конфигураций, которые требуют аутентификацию на сервере и шифрования, используется сертификат, выпущенный третьей стороной

Выполнение	Действие
○	Для конфигураций, которые требуют среднего уровня аутентификации клиента, конфигурируйте сервер так, чтобы запрашивать имя пользователя и пароль через SSL/TLS
○	Для конфигураций, которые требуют высокого уровня аутентификации клиента, конфигурируйте сервер так, чтобы запрашивать сертификаты клиента через SSL/TLS
○	Для организаций, которые требуют средний уровень шифрования, можно использовать DES
○	Для организаций, где требуется высокий уровень шифрования, необходимо использовать RC4 (высокий) или 3DES (самый высокий)
○	Сконфигурируйте проверку целостности файлов, для контроля сертификата Web-сервера
○	Если на Web-сервере должен быть использован только SSL/TLS, убедитесь, что заблокирован доступ через порт 80 TCP
○	Если наибольшая часть трафика на Web-сервер проходит через закодированный SSL/TLS, убедитесь, что на Web-сервере применяется соответствующий механизм регистрации (поскольку сетевой перехват безрезультатен против закодированных сеансов SSL/TLS)

Е.5 Перечень проверок инфраструктуры сети

Выполнение	Действие
	Размещение Сети
○	Web-сервер должен быть расположен в ДМЗ или вне её, в этом случае он должен быть защищен межсетевым экраном
○	ДМЗ не должна подключаться к третьему (или более) интерфейсу межсетевого экрана
	Конфигурация межсетевого экрана
○	Web-сервер защищен межсетевым экраном
○	Web-сервер, если он сталкивается с более высокой угрозой или если он более уязвим, защищен межсетевым экраном прикладного уровня
○	Межсетевой экран контролирует весь трафик между Интернет и Web-сервером
○	Межсетевой экран блокирует весь входящий трафик на Web-сервер, кроме порта 80 TCP (http) и (или) 443 (HTTPS)
○	Межсетевой экран блокирует (вместе с IDS) отдельные адреса IP или подсети, по которым IDS сообщает, что из них атакуют сеть организации
○	Межсетевой экран уведомляет администратора сети или Web о подозрительной активности
○	Межсетевой экран обеспечивает фильтрацию содержимого
○	Межсетевой экран сконфигурирован, чтобы защищаться от атак на сервисы
○	Межсетевой экран обнаруживает деструктивные или известные атаки в запросах URL
○	Межсетевой экран регистрирует критические события
○	Межсетевой экран и его операционная система обновлены до самой новой версии или до наиболее безопасного уровня

Выполнение	Действие
	Системы обнаружения вторжения (IDS)
○	IDS помещённые на хосте, используются для Web-серверов, которые работают преимущественно с SSL/TLS
○	Сконфигурируйте IDS, чтобы контролировать сетевой трафик перед любым межсетевым экраном или фильтром маршрутизатора (основе сети)
○	Сконфигурируйте IDS, чтобы контролировать сетевой трафик к и от Web-серверу после межсетевого экрана
○	Сконфигурируйте IDS, чтобы проверять изменения в критических файлах на Web-сервере (встроенными средствами или программой проверки целостности файлов)
○	IDS блокирует вместе с межсетевым экраном отдельные IP адреса или подсети, через которые атакуют сеть организации
○	IDS уведомляет сетевого или Web-администратора об атаке
○	Сконфигурируйте IDS, чтобы обнаруживать попытки сканирования портов
○	Сконфигурируйте IDS, чтобы обнаруживать DoS атаки
○	Сконфигурируйте IDS, чтобы обнаруживать деструктивные запросы в URL
○	Сконфигурируйте IDS, чтобы регистрировать события
○	Обновляйте IDS новыми сигнатурами атак почаще (рекомендуется еженедельно)
○	Конфигурируйте IDS, чтобы контролировать системные ресурсы доступные на хосте Web-сервера (на хосте)
	Сетевые маршрутизаторы
○	Сетевые маршрутизаторы используются в сегменте сети Web-сервера, для защиты от сетевого подслушивания
○	Сконфигурируйте сетевые маршрутизаторы в режим высокой безопасности, чтобы нейтрализовать атаки, имитирующие подмену ARP и с недействительным ARP
○	Сконфигурируйте сетевые маршрутизаторы, чтобы направлять весь сетевой трафик через хост IDS (основу сети)

Е.6 Перечень проверок безопасного администрирования Web-сервера

Выполнение	Действие
	Регистрация
○	Используйте комбинированный формат регистрации для сохранения регистрации передач или сконфигурируйте вручную так, чтобы информация описывалась комбинированным форматом регистрации, являющимся стандартным форматом для регистрации передач
○	Разрешите работу обработчика регистрации или агента регистрации, если невозможно использовать комбинированный регистрационный формат
○	Установите, разные имена для файлов регистрации различных виртуальных Web-сайтов, которые могут быть частью единого физического Web-сервера
○	Используйте удаленную идентификацию пользователя как определено в [14]

Выполнение	Действие
○	Храните регистрацию на отдельном хосте
○	Архивируйте файлы регистрации согласно правилам организации
○	Анализируйте файлы регистрации ежедневно
○	Анализируйте файлы регистрации еженедельно (для выявления более долгосрочных тенденций)
○	Используйте специальный инструментарий для автоматизации анализа файлов регистрации
	Резервное копирование Web-сервера
○	Разработайте политику резервного копирования Web-сервера
○	Делайте инкрементальное резервное копирование Web-сервера ежедневно на протяжении недели
○	Делайте полное резервное копирование Web-сервера еженедельно на протяжении месяца
○	Периодически архивируйте копии
○	Имейте главную копию Web-сайта(ов)
	Восстанавливаясь после компрометации
○	Обратитесь к политике безопасности организации (она должна быть приоритетнее рекомендаций, приводимых здесь)
○	Отключите скомпрометированные системы от сети или примите меры по сохранению следов атаки, так это может помочь собрать дополнительные свидетельства
○	Изучите сведения об «аналогичных» хостах, чтобы установить, подверглись ли нападению другие системы
○	Проконсультируйтесь с руководством организации, юристами и правоохранительными органами (немедленно свяжитесь с правоохранительными органами, если предполагается судебное обвинение)
○	Проанализируйте вторжение
○	Восстановите систему
○	Подключите систему в сеть
○	Протестируйте систему, чтобы удостовериться в её безопасности
○	Проведите мониторинг системы и сети для определения признаков того, не пытается ли нападающий вновь получить доступ к системе или сети
○	Изучите документы по прошедшим событиям
	Проверка безопасности
○	Периодически сканируйте уязвимые места на Web-сервере и в поддерживающей сети
○	Обновляйте сканер поиска уязвимостей до начала тестирования
○	Устраняйте любые недостатки, найденные сканером поиска уязвимостей
	Удаленное администрирование и обновление содержимого
○	Используйте сильный механизм аутентификации (например, пару ключей - открытый/личный, двухфакторную аутентификацию)
○	Ограничьте хосты, которые могут быть использованы, чтобы дистанционно управлять или модифицировать содержимое Web-сервера конкретными IP адресами и внутренней сетью
○	Используйте безопасные протоколы (например, безопасную оболочку, HTTPS)

Выполнение	Действие
○	Настаивайте принятии на концепции наименьших привилегий в дистанционном администрировании и обновлении содержимого (то есть, попытайтесь минимизировать права доступа для дистанционного администрирования/обновления учетных записей)
○	Измените все встроенные по умолчанию учетные записи или пароли при использовании утилит или приложений для дистанционного администрирования
○	Не допускайте дистанционного администрирования из Интернет или через межсетевой экран
○	Не делайте общедоступными файлы из внутренней сети для Web-сервера или наоборот

Приложение F
(справочное)

Перечень проверок безопасности беспроводной ЛВС

Выполнение	Действия
○	Разработайте политику безопасности организации, которая направлена на использование беспроводной технологии
○	Удостоверьтесь, что пользователи в сети полностью осведомлены о правилах компьютерной безопасности
○	Выполните оценку риска, понимая величину рисков организации, нуждающихся в защите
○	Удостоверьтесь (до покупки), что встроенное программное обеспечение клиента NIC и IP, обновлено до последнего доступного уровня
○	Регулярно выполняйте всестороннюю оценку безопасности (включая подтверждение об отсутствии не зарегистрированных точек доступа в беспроводной ЛВС протокола 802.11), чтобы полностью понимать текущее состояние безопасности беспроводной сети
○	Удостоверьтесь, что действует защита внешней границы, по периметру здания или строения организации
○	Проведите централизованное обследование, для измерения и установления зоны покрытия беспроводной сети организации
○	Проведите полную инвентаризацию всего оборудования сети 802.11 и точек доступа
○	Опытным путем проверьте границы удаления точек доступа, чтобы точно определить границы беспроводного охвата
○	Проверьте, что каналы точек доступа (по крайней мере пять каналов) отличны по частоте от любых других соседних беспроводных сетей, чтобы предотвратить возможные помехи
○	Расположите точки доступа внутри строений подальше от внешних стен и окон
○	Место расположения точек доступа должно быть в защищенных областях, чтобы предотвратить неавторизованный физический доступ и манипуляции пользователей
○	Убедитесь, что точки доступа выключены в течение того времени, когда они не используются
○	Убедитесь, что функция сброса на точках доступа используется только когда необходимо, и только уполномоченной группой сотрудников
○	Восстановите настройки точек доступа к последним параметрам безопасности если использовалась функция сброса
○	Измените встроенный SSID в точке доступа на значение, которое нелегко угадать
○	Запретите "широковещательную передачу SSID", чтобы клиент SSID точно соответствовал адресуемой точке доступа
○	Проверьте, что символьная строка SSID не содержит имя организации (подразделение, отдел, улица, и т.п.) или наименование продукта
○	Запретите широковещательный маяк точек доступа

Выполнение	Действия
○	Проверьте и убедитесь, что все встроенные по умолчанию параметры изменены
○	Блокируйте все опасные и несущественные протоколы управления на точках доступа
○	Включите все функции безопасности продукта беспроводной ЛВС, включая шифрованную аутентификацию и возможности WEP/WPA
○	Удостоверьтесь, что ключ шифрования длинной не менее 128 бит
○	Убедитесь, что секретные ключи периодически заменяются на более безопасные уникальные ключи
○	Установите правильно сконфигурированный межсетевой экран между проводной инфраструктурой и беспроводной сетью (точках доступа или HUB точек доступа)
○	Установите антивирусное программное обеспечение и персональный межсетевой экран на всех беспроводных клиентах
○	Используйте списки управления доступом по MAC-адресам
○	Используйте для беспроводных коммуникаций технологию виртуальной закрытой сети (VPN), базирующуюся на IPsec
○	Удостоверьтесь, что используемое шифрование настолько сильно, насколько позволяет производительность сети и скорости процессоров компьютеров
○	Удостоверьтесь, что все точки доступа имеют сильные административные пароли, и все пароли регулярно изменяются
○	Удостоверьтесь, чтобы режим «ad hoc (как есть)» для 802.11 заблокирован
○	По возможности используйте статические IP адреса в сети
○	Используйте DHCP с функцией "резервирование клиента"
○	Включите механизмы аутентификации пользователя для интерфейсов управления точками доступа
○	Удостоверьтесь, что трафик управления, предназначенный для точек доступа, находится в выделенной защищенной проводной подсети

Приложение
(справочное)

Библиография

[1] ISO/IEC TR 13335-4:2000*, Information technology — Guidelines for the management of IT Security —Part 4: Selection of safeguards

[2] ISO/IEC TR 13335-5:2001*, Information technology — Guidelines for the management of IT Security —Part 5: Management guidance on network security

[3] ISO/IEC 17799:2000*, Information technology — Code of practice for information security management

[4] ISO/IEC 18033-3*, IT security techniques — Encryption algorithms — Part 3: Block ciphers7)

[5] NIST Special Publication 800-44: 2002 Guidelines on Securing Public Web Servers

[6] NIST Special Publication 800-45: 2002 Guidelines on Electronic Mail Security

[7] NIST Special Publication 800-46: 2002 Security for Telecommuting and Broadband Communications

[8] NIST Special Publication 800-48: 2002 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices

[9] IETF RFC 768 User Datagram Protocol (1980)

[10] IETF RFC 821 Simple Mail Transfer Protocol (1982)

[11] IETF RFC 959 File Transfer Protocol (1985)

[12] IETF RFC 1055 Nonstandard for transmission of IP datagrams over serial lines: SLIP (1988)

[13] IETF RFC 1334 PPP Authentication Protocol (1992)

[14] IETF RFC 1413 Identification Protocol (1993)

[15] IETF RFC 1939 Post Office Protocol – Version 3 (1996)

[16] IETF RFC 1991 PGP Message Exchange Formats (1996)

[17] IETF RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP) (1996)

[18] IETF RFC 2045 to IETF RFC 2049 Multipurpose Internet Mail Extensions (MIME) (1996)

[19] IETF RFC 2060 Internet Message Access Protocol - Version 4rev1 (1996)

[20] IETF RFC 2131 Dynamic Host Configuration Protocol (1997)

[21] IETF RFC 2139 RADIUS Accounting (1997)

[22] IETF RFC 2246 The TLS Protocol Version 1.0 (1999)

[23] IETF RFC 2284 PPP Extensible Authentication Protocol (EAP) (1998)

[24] IETF RFC 2401 Security Architecture for the Internet Protocol (1998)

[25] IETF RFC 2406 IP Encapsulating Security Payload (ESP) (1998)

[26] IETF RFC 2440 Open PGP Message Format (1998)

[27] IETF RFC 2631 Diffie-Hellman Key Agreement Method (1999)

[28] IETF RFC 2632 S/MIME Version 3 Certificate Handling (1999)

[29] IETF RFC 2633 S/MIME Version 3 Message Specification (1999)

[30] IETF RFC 2865 Remote Authentication Dial In User Service (RADIUS) (2000)

[31] IETF RFC 3162 RADIUS and IPv6 (2001)

[32] IETF RFC 3369 Cryptographic Message Syntax (CMS) (2002)

[33] IETF RFC 3370 Cryptographic Message Syntax (CMS) Algorithms (2002)

* Применяется в соответствии с СТ РК 1.9 Порядок применения международных, региональных и национальных стандартов и нормативных документов по стандартизации, метрологии, сертификации и аккредитации.

УДК 681.3 **МКС 35.040**

Ключевые слова: информационные технологии, удаленный доступ, защищаемая информация, аутентификация, управление доступом, точка доступа, локальная сеть

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы, Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074