ҚАЗАҚСТАН РЕСПУБЛИКАСЫ АУЫЛ ШАРУАШЫЛЫҒЫ МИНИСТРЛІГІ
Жәңгір хан атындағы Батыс Қазақстан
аграрлық-техникалық университеті

Камалова Г. А.,
Диярова. Л. Б.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ АҚПАРАТТЫ ҚОРҒАУ

оқу құралы

«Альманахъ» баспа үйі
Алматы
2020

ӘОЖ: 004.4(075)
КБЖ 32.81я73
К 18

Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университетінің оқу жоспарлары және бағдарламалары комитетінің отырысында басылымға мақұлданды. (26.04.2018 ж. № 3 хаттама)

Сын-пікір беруші: Кушеккалиев А.Н., физ.-мат. ғыл. канд., доцент

Камалова Г. А.
К 18 Ақпараттық қауіпсіздік және ақпаратты қорғау: оқу құралы / **Г. А. Камалова, Л. Б. Диярова,** – Алматы, Альманахъ, 2020, – 116 б.

ISBN 978-601-7590-04-08

Оқу құралында ақпаратты қорғау әдістері, ақпараттық қауіпсіздік механизмдері, қауіпсіздік саясаты, ақпаратты криптографиялық қорғау, цифрлық қолтаңба технологиясы қарастырылған. Әрбір тарау дәрістерден және білім деңгейін бағалауға арналған бақылау сұрақтардан тұрады.

Оқу құралы жоғары оқу орындарының 5В070300 - «Ақпараттық жүйелер» мамандығының білім алушыларына, оқытушыларына арналған.

К33.2;140.М.С.lic

ӘОЖ: 004.4(075)
КБЖ 32.81я73

Бұл басылым «Альманахъ» баспа үйінде 2019 жылдың 15 қаңтарындағы №1 лицензиялық келісімге сәйкес жарияланған

ISBN 978-601-7590-04-08

МАЗМҰНЫ

Кіріспе 5
1 АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ АҚПАРАТТЫ ҚОРҒАУ НЕГІЗДЕРІ 6
1.1 Ақпарат және ақпараттық қауіпсіздік 6
1.2 Ақпараттық қауіпсіздіктің негізгі құрауыштары 8
1.3 Қорғау объектілері 9
1.4 Ақпаратты тасымалдауыштары мен категориялары 10
Өзін-өзі бақылау сұрақтары 12
2 АҚПАРАТТЫ ҚОРҒАУДЫҢ ӘДІСТЕМЕСІ 15
2.1 Ақпараттық қауіпсіздік жүйесін құру принциптері мен құру бағыттары 15
2.2 Ақпараттық қауіпсіздікті қамтамасыз етудің әдістері мен құралдары 17
Өзін-өзі бақылау сұрақтары 19
3 АҚПАРАТТЫҚ ҚАУІПСІЗДІК МЕХАНИЗМДЕРІ 22
3.1 Идентификация және аутентификация 22
3.2 Ақпараттық жүйедегі енуді басқару 26
3.3 Протоколдау және аудит 31
3.4 Шифрлау 32
3.5 Тұтастылықты бақылау 34
3.6 Экрандау 36
Өзін-өзі бақылау сұрақтары 37
4 АҚПАРАТТЫ ҚОРҒАУ ҚҰРАЛДАРЫ 40
4.1 Ақпаратты қорғаудың инженерлік-техникалық принциптері 41
4.2 Техникалық құралдармен ақпаратты қорғаудың негізгі әдістері.. 42
4.3 Ақпараттың ағып кету арналары 43
Өзін-өзі бақылау сұрақтары 44
5 КОМПЬЮТЕРЛІК ВИРУСТАР ЖӘНЕ ОЛАРДЫ ҚОРҒАУ 48
5.1 Компьютерлік вирустар және олардың түрлері 48
5.2 Вирустардың өмір сүру циклі және олардың әсер ету белгілері... 52
5.3 Вирустарды анықтау әдістері және вирусқа қарсы бағдарламалар және кешендер 54
Өзін-өзі бақылау сұрақтары 56
6 АҚПАРАТТЫҚ КРИПТОГРАФИЯЛЫҚ ҚОРҒАУ ҚҰРАЛЫ 59
6.1 Симметриялық криптоалгоритмдер 61
6.2 Асимметриялық криптоалгоритмдер 66
Өзін-өзі бақылау сұрақтары 69
7 ЦИФРЛЫҚ ҚОЛТАҢБА ТЕХНОЛОГИЯСЫ 73
7.1 Цифрлық қолтанбалардың негізгі түсініктері 73
7.2 Хэштеу функциясы 76
Өзін-өзі бақылау сұрақтары 77

8 ЖЕЛІДЕ КОМПЬЮТЕРЛІК АҚПАРАТТЫ ҚОРҒАУ 81
8.1 Брандмауэрлер 81
8.2 Интернет қызметтерінің кемшіліктері 85
8.3 Желілік қауіпсіздік саясаты 86
8.4 Фильтрлеу әдістері 88
Өзін-өзі бақылау сұрақтары 89
9 АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІҢ ҚАУІПСІЗДІК МОДЕЛЬДЕРІ 92
9.1 Формальды модельдер 92
9.2 Қауіпсіздік модельдері 93
9.3 Қауіпсіздік саясаты және негізгі элементтері 95
Өзін-өзі бақылау сұрақтары 96
10 КОМПЬЮТЕРЛІК ЖЕЛІЛЕРДІҢ ҚАУІПСІЗДІГІ 99
10.1 Жергілікті желілерді қорғау 99
10.2 Корпоративтік желілерді қорғау 102
Өзін-өзі бақылау сұрақтары 110
Белгілеулер мен қысқартулар 113
Глоссарий 114
Пайдаланылған әдебиеттер тізімі 115

КІРІСПЕ

Жаңа ақпараттық технологиялардың пайда болуы және қуатты компьютерлік сақтау мен ақпаратты өңдеу жүйелерінің дамуы ақпаратты қорғау деңгейін арттырды және мәліметтерді сақтау сәулетінің күрделілігімен бірге ақпараттық қорғау тиімділігі өсетінін талап етті. Осылайша біртіндеп экономикалық ақпаратты қорғау міндетті болып табылады: ақпаратты қорғауға арналған барлық құжаттардың түрлері әзірленуде; ақпаратты қорғау бойынша ұсыныстар жасалады; тіпті ақпаратты қорғау мәселелерімен айналысатын ақпаратты қорғау туралы заңмен және ақпараттарды қорғаудың міндеттерімен жүзеге асырылады, сондай-ақ ақпаратты қорғаудың бірегей мәселелерін шешеді.

Осылайша, ақпаратты қорғау қаупі ақпараттық қауіпсіздікті қамтамасыз ету құралдарын ақпараттық жүйенің міндетті сипаттамаларының бірі ретінде жасады.

Ақпараттық қауіпсіздік ақпараттық қатынастар субъектілеріне (соның ішінде ақпарат иелері мен пайдаланушыларға) қолайсыз зиян келтіруі мүмкін кездейсоқ немесе қасақана табиғи немесе жасанды әсерден ақпаратты қорғаудың жағдайы мен ақпараттық ортасы болып табылады.

Ақпаратты қорғаудың негізгі мақсаты: ағып кетуді, ұрлықты, бұрмалауды, жасандылықты болдырмау; жеке тұлғаның, қоғамның, мемлекеттің қауіпсіздігін қамтамасыз ету; ақпарат жүйелерінде рұқсат етілмеген танысудың, жоюдың, бұрмалаудың, көшірудің, бұғаттаудың алдын алу.

Оқу құралының мақсаты білім алушыларды ақпаратты қорғау, ақпараттық қауіпсіздік теориясының негізгі түсініктерімен таныстыру, ақпаратты криптографиялық құралдар көмегімен шифрлауды үйрету, ақпаратты қорғау құралдары мен олардың принциптерін қарастыру болып табылады.

1. АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ АҚПАРАТТЫ ҚОРҒАУ НЕГІЗДЕРІ

1.1 Ақпарат және ақпараттық қауіпсіздік

Ақпарат (лат. Informatio – анықтау, мазмұндау), бастапқыда - адамдар арасында ауызша, жазбаша немесе басқа да техникалық құралдар мен сигналдар көмегімен берілетін мәліметтер. XX ғасырдың ортасынан бастап ақпарат жалпы ғылыми ұғым болып табылады және де төмендегілерден құралады:

– адамдар, адам мен автомат, автомат пен автомат арасында берілетін мәліметтер;
– жануарлар мен өсімдіктер әлемі арасындағы сигналдар;
– жасушадан жасушаға, ағзадан ағзаға берілетін белгілер;
– және т.б.

Басқаша айтқанда, ақпарат іргелі және әмбебап сипатқа ие және де көпмағыналы ұғым болып келеді. Кибернетиканың атасы Н.Винердің сөзімен түйіндеп кетуге болады: «Ақпарат ол ақпарат, материя да, энергия да емес».

Дәстүрлі философиялық көзқарасқа сәйкес, ақпарат адамнан тәуелсіз және материяның қасиеті болып табылады. Қаралып отырған пәннің шеңберінде ақпарат ретінде ақпараттық жүйелерді жинау, сақтау, өңдеу, тікелей пайдалану және беру объектісі болып табылатын мәліеттерді түсінеміз.

Ақпарат мағынасына сүйене отырып, ақпараттық қауіпсіздік және ақпаратты қорғау түсінігін қарастырайық.

Ақпараттық қауіпсіздік дегеніміз мемлекеттік ақпараттық ресурстардың, сондай-ақ ақпарат саласында жеке адамның құқықтары мен қоғам мүдделері қорғалуының жай-күйі.

Ақпаратты қорғау — ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені. Тәжірибе жүзінде ақпаратты қорғау деп мәліметтерді енгізу, сақтау, өңдеу және тасымалдау үшін қолданылатын ақпарат пен қорлардың тұтастығын, қол жеткізулік оңтайлығын және керек болса, жасырындылығын қолдауды түсінеді. Сонымен, ақпаратты қорғау - ақпараттың сыртқа кетуінің, оны ұрлаудың, жоғалтудың, рұқсатсыз жоюдың, өзгертудің, маңызына тимей түрлендірудің, рұқсатсыз көшірмесін жасаудың, бұғаттаудың алдын алу үшін жүргізілетін шаралар кешені. Қауіпсіздікті қамтамасыз ету кезін қойылатын шектеулерді қанағаттандыруға бағытталған ұйымдастырушылық, бағдарламалық және техникалық әдістер мен құралдардан тұрады.

Ақпараттық қауіпсіздік режимін қалыптастыру кешендік мәселе болып табылады. Оны шешу үшін заңнамалық, ұйымдастырушылық, программалық, техникалық шаралар қажет.

Ақпараттық қауіпсіздік деп ақпараттық қарым-қатынасқа қолайсыз зиян келтіруі мүмкін табиғи немесе жасанды сипаттағы (ақпараттық қауіп-қатер, ақпараттық қауіпсіздік қатерлері) кездейсоқ немесе қасақана әсерлерден ақпараттың қорғалуын және қорғау инфрақұрылымын түсінеміз.

Ақпараттық қауіпсіздік – ақпараттық жүйеде ақпарат жинау, сақтау, өңдеу және беру процесінде ақпараттық қауіпсіздіктің қауіп-қатерлерін болдырмау және оның салдарын жоятын құқықтық, ұйымдастырушылық және техникалық шаралар мен іс-шаралар кешені болып табылады.

Ақпараттық қауіпсіздік ақпараттық жүйенің сипаттамаларының бірі екендігін атап өткен жөн, яғни, ақпараттық жүйе белгілі бір мезетте белгілі бір қорғалған күйде (деңгейде) болады, ал ақпаратты қорғау – ақпараттық жүйенің өмірлік циклінің барлық кезеңінде үздіксіз орындалуы тиіс.

Ақпараттық қарым-қатынас субъектілері деп ақпарат пен қолдаушы инфрақұрылымның иелері мен пайдаланушыларын түсінеміз.

Қолдау инфрақұрылымы тек қана компьютерлерді ғана емес, үй-жайларды, электр, су және жылумен жабдықтау жүйелерін, байланыс құралдарын және, әрине, қызмет көрсету персоналын қамтиды.

Зиян келтіру қолайлы немесе қолайсыз болуы мүмкін. Әрине, зиянның барлық түрлерінен сақтандыру мүмкін емес, сонымен қатар қорғаушы құралдар мен іс-шаралар құны күтілетін шығым мөлшерінен көп болған кезде оны экономикалық жағынан тиімді әдіс деп санауға болмайды. Демек, бір нәрседен қорғануды қойып, қорғанбауға болмайтын нәрседен қорғану керек. Кейде мұндай қолайсыз залал адамдардың денсаулығына немесе қоршаған ортаның жағдайына зиян тигізу болып табылады, бірақ жиі қолайсыздықтың табалдырығы материалдық (ақшалай) сипатта болады, ал ақпаратты қорғаудың мақсаты келтірілген зиян мөлшерін қолайлы құнға дейін азайту болып табылады.

Ақпараттық қауіп - ақпаратты жоғалтуға немесе жария етуге әкеліп соқтыратын қорғаныс объектісіне заңсыз немесе кездейсоқ әсер ету мүмкіндігі.

Ақпараттық қауіпсіздік, ақпаратты қорғау секілді кешенді мәселе болып табылады, ол қауіпсіздік жүйесін енгізу арқылы іске асырылады және қауіпсіздікті қамтамасыз етеді. Ақпаратты қорғау мәселесі жан-жақты әрі кешенді және бірқатар маңызды міндеттерді қамтиды. Ақпараттық қауіпсіздіктің проблемалары қоғамның барлық салаларына мәліметтерді өңдеу және берудің техникалық құралдарына, ең алдымен, компьютерлік жүйелерге ену үдерістері арқылы үнемі тереңдейді.

1.2 Ақпараттық қауіпсіздіктің негізгі құрауыштары

Ақпараттық қауіпсіздіктің негізгі үш құрауыштары бар: құпиялылығы, тұтастылығы және мәліметтердің қолжетімділігі

Қауіпсіз ақпараттық жүйе – бұл біріншіден мәліметтерді рұқсатсыз кіруден қоргайтын, екіншіден өзінің пайдаланушыларына оны еруге әрқашан дайын, үшіншіден ақпаратты сенімді сақтайтын және мәліметтер тұтастылығына кепілдік беретін жүйе. Сонымен қауіпсіз жүйе анықтама бойынша құпиялылық, қолжетімділік және тұтастылық қасиеттеріне ие.

Қолжетімділік (availability) — рұқсаты бар пайдаланушылар ғана мәліметтерге қолжтемді екендігіне кепілдік болады.

Құпиялылық (confidentiality) — құпия мәліметтер тек рұқсаты бар пайдаланушыларға қолжетімді екендігіне кепілдік береді.

Тұтастылық (integrity) — рұқсаты жоқ пайдаланушыларға қандай да бір жолмен мәліметтерді өзгертуге, жаңартуға, бұзуға немесе жаңадан құруға тыйым салу алу арқылы ақпараттың дұрыстығы сақталатынына кепілдік берумен жүзеге асады.

Қауіпсіздікдің талаптары жүйенің қолдану орнына, мәліметтердің сипаттамаларына және келетін қауіп-қатер түріне байланысты өзгеруі мүмкін. Тұтастылық пен қолжетімділік керек, бірақ құпиялылық қажет етпейтін жүйені елестету өте қиын. Мысалы, сіз Web-серверде Интернетте ақпарат жариялаған болсаңыз және де оны кең адамдар тобына ашық болғанын қаласаңыз, онда сізге құпиялылықтың қажеті жоқ. Бірақ тұтастылық пен қолжетімділік маңызды болып қала береді.

Егер сіз мәліметтердің тұтастылығын қамтамасыз ету бойынша ешқандай шара қолданбасаңыз, шабуылшы сіздің серверде сіздің ақпараттарыңызды өзгертіп, сіздің өндірісіңізге зиян тигізуі мүмкін. Шабуылшы, мысалға, серверде сақталған прайс-тізімге өзгертулер енгізіп, өндірісіңіздің бәсекеге қабілеттілігін төмендететіндей немесе сіздің фирмаңыздың тегін таратылатын бағдарламалық кодын өзгертумен сіздің іскерлік имиджіңізге әсерін тигізе алады.

Мәліметтердің қолжетімділігін қамтамасыз ету де маңызды. Интернетте серверді құру мен жұмыс жасауын қолдап тұруға үлкен қаражат жұмсап, өндіріс қайтарымды талап ете алады: клиенттер санын үлкеюі, сатылымның жоғарылауын, т.б. Бірақтан шабуылшы серверде орналасқан мәліметтер ешкімге қолжетімді болмайтындай шабуыл әрекеттерін жасауы мүмкін. Мысалы ретінде кері дұрыс емес адресті IP-пакеттермен серверді «бомалау», нәтижесінде бұл хаттаманың жұмыс жасау логикасымен серверде белге бір тайм-ауттар пайда болады да, сервер басқа сұраныстарға қолжетімсіз болып қалады.

Қолжетімділік, құпиялылық және тұтастылық түсініктері ақпараттқа ғана қатысты емес, есептеуіш желінің басқа да қорларына, мысалы сыртқы құрылғылар мен қосымшаларға қатысты. Көптеген жүйелік қорлар бар, және оларды «заңсыз» қолдану мүмкіндігін пайдалану жүйенің қауіпсіздігін бұзады. Мысалы, басып шығаруға шексіз қолжетімділік шабуылшыға басып шығарылып жатқан құжаттар көшірмесін алуға, баптауларды өзгертуге, жұмыстардың басып шығарылу кезегін ауыстыруға және де құрылғыны істен шығаруға толық мүмкіндікке ие бола алады. Басып шығару құрылғысына құпиялылық қасиетін қолжетімділікке рұқсаты бар ғана пайдаланушылар қолдана алумен және оларға бекітілген операцияларды ғана орындай алумен түсіндіріледі. Қолжетімділік қасиетін оны қажет болған кез келген уақытта қолдана алумен түсіндіріледі. Ал тұтастылық қасиеті бұл құрылғының баптауларының әрқашан өзгерілмей қалатынын сипаттайды. Желілік құрылғыларды ресми түрде қолдану мәліметтердің қауіпсіздігіне үлкен әсерін тигізеді. Құрылғылар әртүрлі қызметтер көрсетуі мүмкін: мәтіндерді басып шығару, фактерді жіберу, Интернетке кіру, электронды пошта және т.б., осыларды заңсыз қолдану жүйе қауіпсіздігін бұзумен қатар өндіріске материалдық зиян келтіреді.

Тұтастылықты, құпиялылықты және қолжетімділікті бұзуға бағытталған кез келген әрекет және де желінің басқа ресурстарын заңсыз қолдану қауіп-қатер деп аталады. Орындалған қатерді шабуыл деп атайды. Тәуекел - сәтті орындалған шабуыл нәтижесінде ақпаратты қордың иесі көтеретін мүмкін залалдың ықтимал бағасы. Тәуекелдің шамасы қаншалықты үлкен болса, жүйенің қауіпсіздігі соншама осал жерлері бар және шабуыл жасаудың ықтималдылығы да жоғары болады.

1.3 Қорғау объектілері

Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі қорғау объектілері мыналар болып табылады:

– ақпараттық ресурстардың барлық түрлері. Ақпараттық ресурстар (құжатталған ақпарат) - анықталуға мүмкіндік беретін реквизиттері бар материалдық тасымалдағышқа жазылған ақпарат;

– ақпаратты алуға, таратуға және пайдалануға азаматтардың, заңды тұлғалардың және мемлекеттің құқықтары;

– ақпаратты қалыптастыру, тарату және пайдалану жүйесі (ақпараттық жүйелер мен технологиялар, кітапханалар, мұрағаттар, қызметкерлер, нормативтік құжаттар және т.б.);

– қоғамдық сананы қалыптастыру жүйесі (бұқаралық ақпарат құралдары, әлеуметтік институттар және т.б.).

1.4 Ақпараттың тасымалдауыштары мен категориялары

Кез келген ақпараттық жүйенің ажырамас бөлігі - бұл ақпарат. Ақпараттық салада конституциялық құқықтар мен бостандықтарын шектеу (жүзеге асыру) сипатына қарай құқықтық ақпараттың төрт негізгі түрі (заңмен реттелген) бөлінеді:

- қол жетімдігі шектеулі ақпарат;
- шектеу құқығынсыз ақпарат;
- басқа да қолжетімді ақпарат (мысалы, ақша үшін);
- «зиянды» ақпарат (дәл емес, жалған және т.с.с таратылмайтын ақпарат).

Қолжетімділігі шектеулі ақпарат мемлекеттік құпия және құпиялы ақпарат болып бөлінеді.

Мемлекеттің құпиясы мемлекеттің қорғалатын, әскери, сыртқы саясат, экономикалық, интеллектуалдық, қарақшылық және жедел-іздестіру іс-әрекеттері туралы ақпаратты қамтиды, оларды тарату Қазақстан Республикасының қауіпсіздігіне зиян келтіруі мүмкін. Мемлекеттік құпияның иесі - бұл мемлекеттің өзі. Бұл ақпаратты қорғау және олардың сақталуын бақылау Қазақстан Республикасының «Мемлекеттік құпия туралы» Заңымен реттеледі. Онда Мемлекеттік құпияларды салыстыратын және оған сілтеме жасалмайтын заңмен белгіленген мәліметтер тізбесі бар. Мемлекеттік құпияларды қорғау жөніндегі органдар анықталған:

- мемлекеттік құпияларды қорғау жөніндегі ведомствоаралық комиссия;
- облыста уәкілетті атқарушы биліктің федералды органдары;
- қауіпсіздікті камтамасыз ету;
- Қорғаныс - Қорғаныс министрлігі;
- шетелдік барлау;
- техникалық барлауға және ақпараттың техникалық қорғалуына қарсы әрекет;
- басқа органдар.

Құпия ақпарат - құқықтық режимі мемлекеттік, коммерциялық, өнеркәсіптік және басқа да қоғамдық қызмет саласында қолданыстағы заңнаманың арнайы нормаларымен құрылған құжатталған ақпарат. Бұл ақпарат түрлі мекемелерге, ұйымдарға және жеке тұлғаларға тиесілі. Мемлекет басшысының «Құпиялы ақпараттар тізбесі» туралы Жарлығында құпия ақпарат алты түрге бөлінеді:

- тергеу және сот ісін жүргізу құпиясы;
- қызметтік құпия;
- кәсіптік құпия;

– коммерциялық құпия;

– олар туралы ресми түрдегі мақалада көрсетілетін өнертабыстың, пайдалы модельдің немесе өнеркәсіптік үлгінің мәні туралы мәліметтер;

– жеке мәліметтер.

Жеке мәліметтер нақты немесе анықталған тұлғаға (жеке мәліметтердің субъектісі) тікелей немесе жанама жататын кез келген ақпаратты білдіреді. Бұл ақпараттың шектеулі қолжетімділігіне қарамастан, ол жеке мәліметтердің субъектісіне толығымен ашық болып табылады. Жеке мәліметтерді беру, өңдеу және пайдалану туралы субъект өзі шешеді, сондай-ақ осы мәліметтерді хабарлауға болатын субъектілердің ауқымын анықтайды. Жеке мәліметтердің кейбіреулері жалпыға белгілі (мысалы, тегі, аты және әкесінің аты), яғни қорғау режиміне ие болмауы мүмкін. Ресей Федерациясының «Жеке мәліметтер туралы» Заңы жеке мәліметтер субъектілерінің келесі құқықтарын (азаматтардың жекелеген санаттарын қоспағанда: мемлекеттік құпияларға ие, сотталғандар және басқалар) анықтайды:

– ақпараттың өзін-өзі анықтауы;

– өзінің жеке мәліметтеріне қол жеткізу;

– жеке мәліметтеріңізге өзгерістер енгізу;

– жеке мәліметтерді бұғаттау;

– жеке мәліметтерге қатысты заңсыз әрекеттерге шағымдану;

– шығынның орнын толтыру.

Мемлекеттік органдар мен ұйымдар, жергілікті өзін-өзі басқару органдары қолданыстағы заңдарда белгіленген немесе лицензия негізінде өз құзыреті шегінде жеке мәліметтермен жұмыс істеуге құқылы. Соңғы жағдайда үкіметтік емес заңды және жеке тұлғалар олармен жұмыс істей алады.

Ақпараттың негізгі тасымалдаушылары болып табылады:

– ашық басылым (газеттер, журналдар, есептер, жарнама және т.б.);

– адамдар;

– байланыс құралдары (радио, теледидар, телефон, пейджер және т.б.);

– құжаттар (ресми, іскерлік, жеке және т.б.);

– мәліметтерді автоматты түрде өңдеуге жарамды электронды, магниттік және басқа ақпарат құралдары.

Өзін-өзі бақылау сұрақтары:

1. Ақпаратты қорғау дегеніміз:
a) қорғалатын ақпараттың сыртқа шығуын, қорғалатын ақпаратқа рұқсат етілмеген және кездейсоқ әсерлерді болдырмауға бағытталған іс-әрекет
b) ақпараттың сыртқа шығуын, оның ұрлануын, жоғалуын, рұқсатсыз жойылуын, өзгертілуін, рұқсатсыз көшірмесі алынуын, тежеуін болдырмау үшін жүргізілетін шаралар кешені
c) мәліметтер өңдеу жүйесінде-мәліметтер үшін белгіленген шектеулерді қанағаттандыруға бағытталған ұйымдастырушылық, бағдарламалық және техникалық әдістер мен құралдар
d) қорғалатын ақпараттың сыртқа шығуын, қорғалатын ақпаратқа рұқсат етілмеген және кездейсоқ әсерлерді болдырмауға бағытталған құжаттар тізімі
e) қорғалатын ақпараттың сыртқа шығуын, қорғалатын ақпаратқа рұқсат етілмеген және кездейсоқ әсерлерді болдырмауға бағытталған құралдар жиынтығы

2. Ақпаратты жүйелерді қорғаудың мақсаты (ақпаратты өңдеу жүйесі) – қауіп-қатерге қарсы әрекеттер:
a) өңделген ақпараттың жасырын бұзылу қатері, тұтастылығының бұзылу қатері, жүйенің жұмыс істеуінің бұзылу қатері
b) қол жеткізулік оңтайлығын және жасырындылығын қолдау
c) жүйенің қауіпсіздігін бұзу, жүйедегі өзгерістерді тексеру, тіркеу, жүйедегі қатені анықтау, қателіктерді түзету
d) қауіпсіздікке шабуыл жасауға мүмкіндік тудыратын жағдайды талдау, қорғау жүйесін жоспарлау, қорғау жүйесін жүзеге асыру, қорғау жүйесіне сүйемелдеу
e) қажетті қорғау жүйесін іздеу, жинастыру, пайдасын идентификациялау, аутентификациялау және авторизациялау

3. Ақпараттық қауіпсіздіктің өте маңызды 3 жайы:
a) қолжетімділік, тұтастық, жасырындылық
b) қолжетімділік, тұтастық, құпиялылық
c) тұтастық, жасырындылық, иемдену
d) басқару, қолдану, жасырындылық
e) негізгі, қосымша, аралас

4. Қолжетімділік-
a) саналы уақыт ішінде керекті ақпараттық қызмет алуға болатын мүкіндік
b) ақпараттың бұзудан және заңсыз өзгертуден қорғанылуы
c) заңсыз қол жеткізуден немесе оқудан қорғау
d) ақпаратты өз мақсаттарында қолдануға мүмкіндік береді
e) саналы уақыт ішінде қысқаша түрде ақпараттық қызмет алуға болатын мүкіндік

5. Тұтастық-
a) ақпараттың бұзудан және заңсыз өзгертуден қорғанылуы
b) саналы уақыт ішінде керекті ақпараттық өызмет алуға болатын мүмкіндік
c) заңсыз қол жеткізуден немесе оқудан қорғау
d) ақпаратты өз мақсаттарында қолдануға мүмкіндік береді
e) саналы уақыт ішінде қысқаша түрде ақпараттық қызмет алуға болатын мүкіндік

6. Жасырындылық-
a) заңсыз қол жеткізуден немесе оқудан қорғау
b) саналы уақыт ішінде керекті ақпараттық өызмет алуға болатын мүкіндік
c) ақпараттың бұзудан және заңсыз өзгертуден қорғанылуы
d) ақпаратты өз мақсаттарында қолдануға мүмкіндік береді
e) заңсыз қол жеткізуден немесе түрлендіруден қорғау

7. Қол жеткізуде-
a) логикалық және физикалық басқару құралы бірге қаралуы тиіс
b) техникалық және физикалық басқару құралы бірге қаралуы тиіс
c) логикалық және бағдарламалық басқару құралы бірге қаралуы тиіс
d) техникалық және бағдарламалық басқару құралы бірге қаралуы тиіс
e) логарифмдік және физикалық басқару құралы бірге қаралуы тиіс

8. Қол жеткізудің шектелуі -
a) өндірістік қажеттілікке және ақпараттық қауіпсіздік саясатына негізделуі тиіс
b) техникалық қажеттілікке және ақпараттық қауіпсіздік саясатына негізделуі тиіс
c) бағдарламалық қажеттілікке және ақпараттық қауіпсіздік саясатына негізделуі тиіс
d) криптографиялық қажеттілікке және ақпараттық қауіпсіздік саясатына негізделуі тиіс
e) өндірістік қажеттілікке және құқықтық заңнамаларға негізделуі тиіс

9. Ақпаратты қорғау қасиеттеріне жатпайтыны
a) Қарапайымдылық қасиет
b) Құндылық қасиет
c) Конфеденциалдық қасиет
d) Осалдылық қасиет
e) Аутентикалық қасиет

10. Қол жеткізуді басқару ережесін анықтаған кезде ескерілуі тиіс факторлар саны -
a) 5
b) 4
c) 7
d) 3
e) 6

11. Тұтастықтың екі жайы ажыратылады:
a) бөлек хабардың немесе ақпарат өрісінің тұтастығы және хабарлар ағынының немесе ақпарат өрістерінің тұтастығы

b) қолтаңба құрастыру және қол қойылған мәліметтер бөлігін тексеру
c) құпия кілтті симметриялық және ашық кілтті асимметриялық
d) жүйеге тұтастай әкімшілік ету; қауіпсіздік функцияларына әкімшілік ету;
e) қолтаңба құрастыру және қауіпсіздік функцияларына әкімшілік ету

12. Жасырындылықтың келесі түрлері болады:
a) байланысу орнату арқылы қатынасу кезіндегі мәліметтердің жасырындылығы; байланысу орнатылмай қатынасу кезіндегі мәліметтердің жасырындылығы; жеке өрістердің жасырындылығы; мәліметтер ағынының жасырындылығы
b) байланысу орнатылатын немесе орнатылмайтын, барлық мәліметтер немесе олардың тек қана жеке өрістері қорғанылатын, тұтастығы бұзылған сәтте бұрыңғы қалпына келтірілуі қамтамасыз етілетін немесе етілмейтін
c) мәліметтер көзінің шынайылығын растаумен қатарлас бастартпаушылық және мәліметтердің жеткізілгендігін растаумен қатарлас бастартпаушылық
d) жеке өрістердің жасырындылығы, мәліметтер ағынының жасырындылығы
e) тұтастығы бұзылған сәтте бұрыңғы қалпына келтірілуі қамтамасыз етілетін немесе етілмейтін

13. Ақпарат қауіпсіздігінің аймағы-
a) бұл ақпаратты қорғау емес оны жекеменшік ету құқығынан қорғау
b) жеке меншік ерекшеліктерінен қорғау
c) ақпараттық ресурстарды қорғау
d) ақпараттың қолданылу аймағын қорғау
e) ақпараттың сақталу аймағын қорғау

14. Ақпаратты қорғау мәселелері келесі бағыттарда қарастырылады -
a) негізгі, өздік-салыстырмалы, толықтырушы
b) қосымшы, өздік-салыстырмалы, толықтырушы
c) қосымшы, салыстырмалы, толықтырушы
d) негізгі, салыстырмалы, толықтырушы
e) негізгі, өздік-салыстырмалы, айырбастаушы

15. Заңды орындаушылық –
a) ақпараттық қатынастар процесінде қалыптасқан заңдылық, нормативтік, құқықтық актілер мен этикалық мінез-құлық ережелерін сақтауды қамтамасыз ету
b) заңды орындаушылыққа, дәл сондай ақпараттық қатынастарды бұзушылыққа дәлелдер беру мен қалыптастыру жағдайларын қамтамасыз ету
c) ақпаратты кездейсоқ немесе әдейі бұрмалаудан қорғауды қамтамасыз ету
d) ақпаратты сақтаушыларды жоюдан, бүлінуден, ұрлықтан, техникалық жүйе мен жабдықтарды физикалық қорғауды қамтамасыз ету
e) ақпаратқа рұқсатсыз енуден қорғауды қамтамасыз ету

2. АҚПАРАТТЫ ҚОРҒАУДЫҢ ӘДІСТЕМЕСІ

2.1 Ақпараттық қауіпсіздік жүйесін құру принциптері мен құру бағыттары

Ақпараттық қауіпсіздік жүйесін құру принциптері

Жүйелік принцип. Жүйелік көзқарас қауіпсіздікті қамтамасыз ету проблемасын түсіну мен шешу үшін маңызы бар барлық өзара байланысты, өзара әрекеттесетін және уақытша өзгеретін элементтер, жағдайлар мен факторларды ескеру қажеттілігін білдіреді.

Кешенділік принципі қауіп-қатерлерді іске асыру үшін болуы мүмкін барлық арналарды жабатын және жеке құрамдас бөліктерінің бірігуінде әлсіз нүктелерден құрылмайтын тұтас ақпараттық қауіпсіздік жүйесінің құрудағы әртүрлі құралдарды келісілген қолдануды білдіреді.

Қорғаудың үздіксіздік принципі. Ақпаратты қорғау – бұл бір-ақ рет жүргізілетін шара емес, сонымен қатар ақпараттық жүйе өмірлік циклінің барлық кезеңдеріне (жұмыс істеу кезеңінде ғана емес, бастапқы жобалау кезеңдерінен бастап) сәйкес тиісті шараларды қабылдауды қамтитын үздіксіз мақсатты үрдіс.

Ақылға жеткілікті принципі. Абсолютті шешілмейтін қауіпсіздік жүйесін құру мүлдем мүмкін емес. Мүмкін болатын шығындардың, қауіп-қатердің және ықтимал залалдың мөлшері дұрыс болатын қорғаудың жеткілікті деңгейін таңдау маңызды.

Басқару мен қолданудың икемділік принципі. Қабылданған шаралар мен орнатылған қорғау құралдары, әсіресе олардың жұмыс істеп тұрған алғашқы кезеңінде, шамадан тыс және жеткіліксіз қауіпсіздікті қамтамасыз етуі мүмкін. Бұл принцип сыртқы жағдайлар мен уақыт бойынша талаптардың өзгеруіне байланысты қорғау деңгейін өзгерту мүмкіндігін білдіреді.

Қорғау алгоритмдері мен механизмдерінің ашықтық принципі. Бұл принциптің мәні мынада, бұл қорғаныс тек қана құрылымдық ұйымның құпиялылығы мен оның кіші жүйелерінің жұмыс істеу алгоритмдері есебінен қамтамасыз етілмеуі керек. Қорғаныс жүйесінің алгоритмдерін білу тіпті оны қорғауды әзірлеуші адамға жеңуге мүмкіндік бермейді.

Қорғау шаралары мен құралдарын пайдаланудың қарапайымдылық принципі. Қорғаныс жабдығын пайдалану арнайы тілдерді білуімен немесе заңды пайдаланушылардың қалыпты жұмысында елеулі қосымша жұмыс күшін талап ететін іс-әрекеттерді жүзеге асырумен байланысты болмауы керек және пайдаланушыға түсініксіз күнделікті операцияларды орындауды талап етпеуі керек.

АҚЖ (ақпараттық қауіпсіздік жүйесі) құру бағыттары

АҚЖ-нің дамуы үш параллельді бағыт бойынша жүргізілуі керек: әдістемелік, ұйымдастырушылық және техникалық.

Әдістемелік нұсқаулық келесі мәселелерді шешуге мүмкіндік береді:

– Ақпараттық ағындарды (АА) анықтау және синаттау әдістемесін әзірлеу, яғни, ақпаратпен жұмыс істеу тәртібін ресми және нақты сипаттау;

– құпия ақпарат санаттарын анықтау және осы санаттар бойынша ақпаратты жіктеуді дамыту;

– құпиялылық матрицасын құру;

– құпия ақпаратты жариялаудың ықтимал жолдарын анықтау, яғни қауіпті модельдер;

– әрбір қауіп пен шабуыл үшін бұзушы моделін анықтау;

– барлық құпиялылық матрицасы үшін қауіп деңгейлерін анықтау, яғни, әр шабуылдың жүзеге асырылу ықтималдығы мен әрбір шабуылдың шығындарының мүмкіндігін анықтау.

Ұйымдастыру жұмысының аясында ережелер жиынтығы (басқару құжаттары) жасалады, олар ұсыну нысанына қарамастан ақпаратпен жұмыс жасаудағы қызметкерлердің жұмыс реттейді.

Ұйымдастыру бағыты:

– кәсіпорынның ақпараттық құрылымын талдау;

– қауіпсіздікпен қамтамасыз ету ережелерін әзірлеу;

– қызметкерлермен жұмыс істеу кезінде әдіснаманы қолдану;

– жүйенің қауіпсіздігінің сипаттамаларына қойылатын талаптарды нақтылау жөніндегі жұмыс;

– ақпараттық қатынастардың субъектілерінің және объектілерінің құпиялылық санаттары бойынша жіктеу;

– олардың өзара әрекеттесуінің қолжетімді нысандарын анықтау және т.б.

Қауіпсіздікті қамтамасыз ету туралы ереже - оны өңдеудің фазасына және құпиялылық санатына қарай құпия ақпаратты (ҚА) өңдеу ережелерін реттейтін құжаттар жиынтығы. Ережелерде әдістемелік, әкімшілік және техникалық шаралар кешені анықталуы тиіс, соның ішінде:

– ҚА-ты қамтамасыз ету үшін жауапты бөлімше құру;

– қызметкерлердің ҚА-ға қолжетімділік ретін және оларға жүктелген міндеттерді, шектеулер мен шарттарын анықтау;

– ҚА-қа жіберілген қызметкерлерді анықтау;

– ҚА классификациясы және онымен санаттар бойынша жұмыс істеу;

– жұмыстар мен ақпараттардың құпиялылық санатын өзгерту тәртібі;

– санаттар бойынша құпия жұмыстар жүргізілетін және ҚА өңделетін бөлмелерге қойылатын талаптар;

– құпия іс жүргізуге қойылатын талаптары;

– құпия құжаттарды есепке алу, сақтау және өңдеуге қойылатын талаптар;
– жұмыстар мен ақпараттардың құпиялылығын қамтамасыз етуді бақылау жөніндегі шаралар;
– ҚА-қа шабуылына қарсы іс-шаралар жоспары;
– ҚА-ты қалпына келтіру бойынша іс-шаралар жоспары;
– ҚА-ты тарату бойынша жауапкершілікті анықтау.

Жұмыстың техникалық саласы шеңберінде оны өңдеуге, сақтауға және таратуға, криптографиялық құралдармен қоса, АҚ үшін техникалық құралдар мен технологиялар кешені құрылады. Осы мақсатта қорғаудың қажетті деңгейін жүзеге асыруға мүмкіндік беретін АҚ арқылы ақпаратты өңдеу, сақтау және берудің автоматтандырылған жүйесін жабдықтау бойынша техникалық ұсыныстар әзірлеу үшін бастапқы мәліметтерді жинақтау жүргізіледі.

2.2 Ақпараттық қауіпсіздікті қамтамасыз етудің әдістері мен құралдары

АҚ-ті қамтамасыз ету әдістері

Қолжетімділікті басқару - барлық АЖ ресурстарын пайдалануды реттеу арқылы ақпаратты қорғау әдісі. Қолжетімділікті басқару келесідей қорғау қызметтерін қамтиды:
– жүйенің пайдаланушыларын, қызметкерлерді және ресурстарды сәйкестендіру,
– объектілер мен субъектілердің түпнұсқалылығын,
– субъекттің қауіпсіздік ережелеріне сай келетін өкілеттігін тексеру,
– регламенттердің шеңберінде еңбек жағдайларына рұқсат ету және құру,
– қорғалатын ресурстарға өтініштерді тіркеу,
– рұқсатсыз іс-шараларға жауап беру (өтініштен бас тарту, жұмысты кешіктіру, өшіру, дабыл).

Кедергі - АЖ ресурстарына зиянкестердің жолын физикалық түрде кедергі жасау әдісі.

Бүркемелеу - крипографиялық және стиганографиялық қорғау әдісі.

Регламентация - рұқсатсыз қол жеткізу мүмкіндігі барынша азаюға ұшырайтын, қорғалатын ақпаратты автоматтандырылған өңдеу, сақтау және беру ортасын жасайтын ақпаратты қорғау әдісі.

Мәжбүрлеу - бұл пайдаланушылар мен АЖ қызметкерлері материалдық, әкімшілік немесе қылмыстық жауапкершілік қаупі бар қорғалған ақпаратты өңдеу, беру және пайдалану ережелерін сақтауға мәжбүрлейтін қорғау әдісі.

Қозғау салу (побуждение) - пайдаланушылар мен жүйелік қызметкерлерді белгіленген моральдық нормаларды бұзбауға шақыратын қорғау әдісі.

Қауіпсіздікті қамтамасыздандырудың аталған әдістері іс жүзінде әр түрлі қорғаныс құралдарын пайдалану арқылы іске асырылады, олар екі класқа бөлінеді:

Формальды - адамның тікелей қатысуынсыз алдын-ала белгіленген рәсімге сәйкес қорғау функцияларын орындау;

Бейресми - адамның мақсатты қызметі арқылы анықталады немесе осы қызметті реттейді.

Ақпаратты қорғау құралдары:

Техникалық құралдар электрлік, электромеханикалық және электронды құрылғылар түрінде жүзеге асырылады. Аппараттық және физикалық болып бөлінеді.

Аппараттық құралдар деп тікелей АЖ ендірілген құрылғылар немесе стандартты интерфейсті (электрондық кілттер, аппараттық шифрлау схемалары) пайдаланып, осы жабдықпен тіркелетін құрылғыларды түсінеміз.

Физикалық құралдар автономдық құрылғылар мен жүйелер (дабыл жабдығы, есіктер, торлар) түрінде жүзеге асырылады.

Бағдарламалық құрал ақпараттық қауіпсіздік функцияларын орындау үшін арнайы жасалған бағдарламалық қамтамасыздандыру болып табылады. Бұл құралдар ақпараттық қауіпсіздік технологияларын дамытудың бастапқы сатыларында қорғау механизмдерінің негізін құрды. Бағдарламалық құралдар қызметтері бойынша былай бөлінеді:

– қолжетімділікті бақылау құралдары,
– аудит құралдары,
– шабуылды бұғаттау құралдары (желіаралық экрандар),
– осалдығын іздеу құралдары (қауіпсіздік сканерлері),
– бағдарламалық кодтарды талдау құралдары.

Қорғаудың ұйымдастыру құралдары АЖ-нің өмірлік циклінің (үй-жайлардың құрылысы, АЖ-ні тестілеу, монтаждау және құрал-жабдықтарды жөндеу, тәжірибеден өткізу және пайдалану) барлық кезеңдерінде жүзеге асырылатын ұйымдастырушылық-техникалық және ұйымдастырушылық -құқықтық іс-шаралар болып табылады.

Құқықтық қорғау құралдары құпия ақпаратты пайдалану, өңдеу және беру ережелерін реттейтін және де ережелерді бұзу жөніндегі жауапкершіліктерді белгілейтін заңдармен және басқа да құжаттармен анықталады.

Моральды-этикалық қорғау құралдары АТ-ның дамуының мүмкіндігіне қарай пайда болатын нормативтік құқықтық нысандары күйінде жүзеге асырылады. Бұл ережелер заңдар сияқты міндетті емес, бірақ олардың сақталмауы ұйымның немесе адамның беделінің жоғалуына әкелуі мүмкін.

Қазіргі уақытта АҚН құралдарын дамытудың келесі үрдістері бар:

– негізгі қорғау функцияларын аппараттық жүзеге асыру,
– бірнеше қорғаныш функцияларын орындайтын кешенді қорғаныс құралдарын құру,
– алгоритмдерді және техникалық құралдарды біріктіру және стандарттау.

Өзін-өзі бақылау сұрақтары:

1. Қорғау құрылғылары:
a) формальды және формальды емес
b) ұйымдық, бағдарламалық
c) құқықтық және аппататтық
d) физикалық және моральды-этикалық
e) негізгі және резидентті

2. Формальды қорғау құрылғыларына жатады:
a) адамның қатысуынсыз алдын-ала қарастырылған процедура бойынша қорғаныс функцияларын орындайтын құрылғылар
b) белгілі бір адамның басқаруымен орындалатын басқару функциялары
c) адамдардың белгілі бір мақсатпен бағытталған қызметтері арқылы анықталатын қорғау түрлері
d) қоғамда ақпараттық технологияларды тарату және дамыту процесінде қалыптасқан дәстүрлі нормалар
e) адамның көмегімен гана алдын-ала қарастырылған процедура бойынша қорғаныс функцияларын орындайтын құрылғылар

3. Формальды емес қорғау құрылғыларына жатады:
a) адамдардың белгілі бір мақсатпен бағытталған қызметтері арқылы анықталатын қорғау түрлері
b) ұйымдық-құқықтық және ұйымдық-техникалық шаралар
c) криптографиялық түрлендіру арқылы ақпаратты қорғау құрылғылары
d) жүйе ресурстарының қолданылу жолдарын қорғау әдістері
e) адамдардың белгілі бір мақсатпен бағытталған іс-әрекеттері арқылы анықталатын қорғау түрлері
4. Қорғау құрылғыларының категориялары:
a) өзіндік қорғау, ЕЖ құрамында қорғау, активті қорғау, пассивті қорғау
b) активті қорғау, пассивті қорғау
c) өзіндік қорғау, ЕЖ құрамында қорғау
d) желілік және реляциялық қорғау
e) өзіндік қорғау, ЕЖ құрамында қорғау, активті қорғау

5. Ақпаратты техникалық қорғау құрылғылары бөлінеді:
a) электронды және оптикалық. қорғау құрылғылары
b) ішкі және сыртқы
c) локальды және өшірілген
d) бақылау және тексеру
e) каоксиалды және талшықты оптикалық

6. Ақпаратты қорғау жүйелері тұрады:
a) ұйымдық және технологиялық шаралар, бағдарламалық-техникалық құрылғылар, құқықтық және моральды-этикалық нормалардан
b) ұйымдық және технологиялық шаралар, бағдарламалық-техникалық құ рылғылар, әкім-әміршілік шаралардан
c) құқықтық және моральды-этикалық нормалар, технологиялық шаралардан
d) каоксиалды және талшықты оптикалық кабельдерден
e) ұйымдық және технологиялық шаралар, бағдарламалық-техникалық құрылғылар, құқықтық және биометриялық нормалардан

7. Ұйымдық-әкімшілік қорғау құрылғыларының мақсаты:
a) қауіпсіздік қатерлерін жүзеге асыру мүмкіндіктерін қиындату немесе жою
b) қауіпсіздік шараларын жүзеге асыру үшін мүмкіндік жасау
c) объект немесе қорғаныс элементі аймағында физикалық тұйық орта жасау
d) ұйымдық және технологиялық шаралар, бағдарламалық-техникалық құ рылғылар, әкім-әміршілік шараларды іске асыру
e) қорғалатын ақпараттың сыртқа шығуын, қорғалатын ақпаратқа рұқсат етілмеген және кездейсоқ әсерлерді болдырмау

8. Биометриялық қорғау-
a) адамның бір анатомиялық қасиетіне негізделеді
b) техникалық құрылғыларға негізделеді
c) оптикалық-талшықты кабельдерге негізделеді
d) адамның бір келбетіне негізделеді
e) адамның бір мінез-құлық қасиетіне негізделеді
9. Ақпаратқа құқықсыз ену келесі әдістер арқылы іске асады:
a) пассивті және активті әдістер
b) техникалық, кәсіптік
c) оперативті және мекеме аралық
d) ұйымдық және әміршілдік
e) негізгі және қосымша

10. Компьютерлік ақпарат берілетін байланыс каналдары келесі түрлерге бөлінеді:
a) өткізгіш сымды, талшықты-оптикалық, өткізгіш сымдарсыз
b) өткізгіш сымды, өткізгіш сымдарсыз
c) талшықты-оптикалық, өткізгіш сымдарсыз
d) телеканал байланысы, радиобайланыс
e) мобильді, талшықты-оптикалық, өткізгіш сымдарсыз

11. Байланыссыз қосылу неше жолмен жүргізіледі?
a) 2
b) 1
c) 3
d) 4
e) 5

12. Талшықты-оптикалық байланыс линияларына құқықсыз ену тәсілдері:
a) байланысты және байланысты емес
b) активті және пассивті
c) оң және теріс
d) кездейсоқ және арнайы
e) негізгі және қосымша

13. Ақпарат қорғаудың физикалық құралдары:
a) қорғалатын ақпаратқа қатынас құрылатындай орындарға ықтимал бұзушылардың жетуін қиындататын немесе жол бермейтін техникалық құралдар, инженерлік құрылғылар және ұйымдастырушылық шаралар
b) ақпаратты қорғау бойынша көзқарастар мен жалпы техникалық талаптар жүйесі
c) ақпараттың дұрыстығын көрсету үшін компьютер жадындағы сөзге үстемеленетін разряд
d) ақпараттың адамның көздеген қызметінің алуан түрлі саласындағы пайдалануға жарамдық қасиеті
e) ақпараттық технологияларды жеке және заңды тұлға ақпараттық қажеттіліктерін қанағаттандыру мақсатын қорғайды

14. Ақпаратқа рұқсатсыз қатынас құру:
a) ақпаратқа қатынас құру тәртіптерін бұза отырып оған қатынас құру
b) ақпаратқа қатынас құру тәртіптерін сақтай отырып қатнаыс құру
c) ақпаратпен танысу, оны өңдеу
d) қатынас құруға құқығы жоқ тұтынушыларға қорғалған ақпаратты рұқсатсыз жеткізу
e) ақпараттық технологияларды жеке және заңды тұлға ақпараттық қажеттіліктерін қанағаттандыру мақсатын қорғайды

15. Ақпаратқа рұқсатты қатынас құру:
a) ақпаратқа қатынас құру тәртіптерін сақтай отырып қатынас құру
b) ақпаратқа қатынас құру тәртіптерін бұза отырып оған қатынас құру
c) ақпаратпен танысу, оны өңдеу
d) қатынас құруға құқығы жоқ тұтынушыларға қорғалған ақпаратты рұқсатсыз жеткізу
e) ақпаратқа қатынас құру тәртіптерін өзгерте отырып қатынас құру

3 АҚПАРАТТЫҚ ҚАУІПСІЗДІК МЕХАНИЗМДЕРІ

3.1 Идентификация және аутентификация

Ақпараттық қауіпсіздіктің төмендегідей концептуалды механизмдері бар: идентификация және аутентификация; енуді бақылау және басқару; протоколдау және аудит; шифрлау; тұтастылықты бақылау; экрандау.

Ақпаратты сенімді қорғау үшін жоғарыда аталған механизмдер кешенін жүзеге асыру қажет. Олардың кейбіреулері толығымен іске асуы мүмкін, ал басқалары - жоқ. АЖ-ны қорғау бірінші кезекте идентификация және аутентификация механизмін іске асыруға байланысты

Идентификатор - берілген жүйеде объектіге немесе субъектіге сәйкес келетін символдар жиынтығы.

Идентификация - ақпараттық өзара байланыс үрдісінің қатысушысын, оған қандай да бір ақпараттық қауіпсіздік аспектілерін қолданбай тұрып тану.

Пароль – ұсынылатын идентификаторға субъектінің сәйкестігін растауға мүмкіндік беретін құпия символдар жиынтығы.

Аутентификация - ақпараттық өзара байланыс қатысушысының дұрыс анықталуына сенімділікті қамтамасыз ету.

Профиль - берілген объект пен субъект үшін параметрлер мен конфигурациялар жиынтығы және оның АЖ-дегі жұмысын анықтау.

Авторизация – ақпараттық өзара байланыстың белгілі бір қатысушысы үшін құқықтық профилін қалыптастыру.

Субъект кемінде төмендегі бір мәнін көрсете отырып, өзінің түпнұсқалығын растауы мүмкін:

– ол білетін бір нәрсе (пароль, криптографиялық кілт және т.б.);

– оған тиесілі бір нәрсе (электронды кілт, смарт-карта және т.б.);

– бұл оның бір бөлігі (оның биометриялық сипаттамалары).

Аутентификация бір жақты (әдетте субъект жүйеге өзінің түпнұсқалығын дәлелдейді) және екі жақты (өзара).

Сенімді идентификация және аутентификация бірнеше себептер бойынша қиындатылған.

АЖ тараптар арасында сенімді маршрут болмауы мүмкін; бұл жалпы алғанда, субъектіден алынған мәліметтер түпнұсқаландыру үшін алынған және қолданылған мәліметтермен сәйкес келмеуі мүмкін дегенді білдіреді.

Барлық дерлік түпнұсқалық мәндерді анықтауға, ұрлауға немесе түрлендіруге болады.

Бір жағынан аутентификацияның сенімділігі мен субъектінің жайлылығы арасында карама – қайшылық бар. Қауіпсіздік мақсатында, белгілі бір жиілікте, пайдаланушыға аутентификация туралы ақпаратты қайта енгізуді талап ету қажет.

Қорғау құралдары қаншалықты сенімді болса, соғұрлым қымбатқа түседі.

Сурет 1. Идентификация және аутентификация жүйелерінің түрлері

Парольді аутентификация

Парольді аутентификацияның негізгі артықшылығы - қарапайымдылық. Кемшілік - түпнұсқалықты тексеретін ең әлсіз құрал.

Парольдерді жасау және пайдалану кезінде негізгі бұзушылықтар:

– қарапайым пароль,

– ешқашан өзгертілмейтін кез келген құжаттан стандартты мәндерді пайдалану,

– оқуға болатын, оқылатын және т.б. заттарға парольді жазу.

– басқа қызметкерге парольді хабарлау.

Парольді қорғау сенімділігін арттыруға мүмкіндік беретін шаралар:

– техникалық шектеулерді қою (ұзындық, әріптерді, сандарды, белгілерді пайдалану);

– парольдердің жарамдылық уақытын басқару;

– парольдің файлға қолжетімділігін шектеу;

– жүйеге сәтсіз кіру әрекеттерінің санын шектеу;

– пайдаланушыларды оқыту;

– белгілі бір ережелерге негізделген күрделі, бірақ есте сақталатын парольдерді тудыратын парольдің бағдарламалық генераторларын пайдалану;

– бір реттік парольдер.

Бір реттік парольдер

Мысалы, бір жақты f функция (ягни, қолайлы уақытта қайта есептеу мүмкін емес функция) бар делік. Бұл функция пайдаланушыға және аутентификация серверіне де белгілі.

Пайдаланушыға ғана белгілі K құпия кілті болсын.

Бастапқы басқару сатысында f функциясы K кілтіне n-рет қолданылады, содан кейін нәтиже серверде сақталады.

Осыдан кейін пайдаланушының түпнұсқалықты тексеру процедурасы келесідей:

– сервер n-1 санын пайдаланушы жүйесіне жібереді;

– пайдаланушы f функциясын K кілтіне (n-1) рет қолданады және желі арқылы нәтижені аутентификация серверіне жібереді;

– сервер f функциясын пайдаланушыдан алынған мәнге қолданады және нәтижені бұрын сақталған мәнмен салыстырады. Сәйкестік жағдайында, пайдаланушының түпнұсқалығы құрылады деп есептеледі, сервер жаңа мәнді (пайдаланушы жіберген) сақтайды және есептегіш (n) біреуге азаяды.

F функциясы қайтарылмайтын болғандықтан, парольді тоқтатып, аутентификация серверіне ену, K құпия кілтін біліп, келесі бірреттік парольді болжауға мүмкіндік бермейді.

Бір реттік парольдерді енгізудің тағы бір тәсілі қысқа уақыт өткеннен кейін (мысалы, әрбір 60 секунд) жаңа құпия сөзді құру болып табылады, ол үшін бағдарламалар немесе смарт-карталар қолданылуы мүмкін. Бұл үшін келесі шарттар орындалуы тиіс:

– аутентификация сервері парольді генерациялау алгоритмін және байланысты параметрлерді білуі керек;

– клиент пен сервердің сағаттары синхронды болуы керек.

Токендер қолданылған аутентификация

Келесі нұсқаларда болуы мүмкін:

Жүйенің сұранысы бойынша токен оған түпнұсқалығын растауға қызмет ететін құпия мәнді көрсетеді. Бұл жауапты бір рет ұстап алғаннан кейін, шабуылдаушы токеннің жауаптарын имитациялауы мүмкін.

Токен мен жүйе бір реттік парольдерді генерациялау үшін ортақ, үндестірілген жүйеге ие. Жүйенің сұранысына токен белгілі бір уақыт ішінде жарамды парольді береді. Осы уақытта жүйе парольдің өз нұсқасын жасайды және ол оны алынған парольмен салыстырады.

Токен жүйеде тіркелген (ол оның құпия параметрін біледі). Аутентификациялау үшін токен өз параметрін пайдаланып, түрлендіретін кездейсоқ мәнді жасайды. Жүйе ааналогты түрлендіруді орындайды және нәтижені токеннен алынған нәтижемен салыстырады. Бұл жағдайда сұраныс пен жауапты ұстап алу шабуылдаушыға ештеңе бермейді. Және токен мен жүйені синхрондау талап етілмейді.

Токендердің парольмен бірге пайдалану нұсқалары:

– Парольдер парольсіз жұмыс істемейтін токендерге енуге арналған.

– Пароль токендер параметрімен бірге бірреттік парольдер жасауға негіз болып табылады.

– Токендер жүйеге пайдаланушының пароліне және оның параметріне негізделген кездейсоқ мәнінің сұранысына жауап береді.

Биометриялық мәліметтерді пайдаланып аутентификациялау

Биометрия физиологиялық және мінез-құлық сипаттамаларына негізделген адамдарды идентификациялау және аутентификациялау үшін автоматтандырылған әдістер жиынтығы болып табылады.

Биометриялық әдістің жіктелуі 2-суретте көрсетілген.

Сурет 2. Биометриялық әдіс

Физиологиялық сипаттамалардың қатарына мыналар жатады:

– саусақ іздері,
– көздің тор қабығы,
– қол мен бет геометриясы.

Мінез-құлық сипаттамаларына жатады:

– қол қою динамикасы,
– пернетақтамен жұмыс істеу стилі.

Сипаттамаларға, физиология мен мінез-құлықты қоса алғанда, дауыс ерекшеліктері мен сөз тану жатады.

Жалпы, биометриялық мәліметтермен жұмыс келесі түр ұйымдастырылады. Біріншіден, әлеуетті пайдаланушылардың сипаттамаларының мәліметтер базасы құрылады және сақталады. Ол үшін

пайдаланушының биометриялық сипаттамалары алынады, өңделеді және өңдеудің нәтижесі (биометриялық үлгі деп аталады) мәліметтер базасына жазылады. Бұл жағдайда бастапқы мәліметтер, яғни саусақты немесе маңдайшаны сканерлеу нәтижелері әдетте сақталмайды.

Ары қарай, пайдаланушыны идентификациялау және аутентификациялау үшін алу және өңдеу процесі қайталанады, одан кейін үлгі мәліметтер базасында іздеу жүргізіледі.

Табысты іздестіру жағдайында пайдаланушының сәйкестендіруі және оның түпнұсқалылығы белгілеу қарастырылған. Аутентификация үшін бұрын енгізілген мәліметтер негізінде таңдалған бір биометриялық үлгіні салыстыру жеткілікті.

Әдетте биометрияны басқа да аутентификаторлармен, мысалы, смарт-карталармен бірге қолданады. Кейде биометриялық аутентификация смарт карталарды белсендіруге қызмет етеді, бұл жағдайда биометриялық үлгі сол картада сақталады.

Биометрия басқа аутентификация әдістерімен бірдей қауіптерге ұшырайды.

Биометриялық үлгіні пайдаланушының сипаттамаларының бастапқы өңдеудің нәтижесімен емес, салыстыру орнына келгендегімен салыстырады.

Биометриялық әдістер үлгі мәліметқорына қараганда сенімді емес.

Бақыланатын аумақта және «далалық» жағдайда биометрияны қолдану арасындағы айырмашылықты ескеру қажет.

Адамның биометриялық мәліметтері өзгереді, сондықтан үлгілердің базасы сүйемелдеуді қажет етеді.

Бірақ басты қауіп мынада - егер биометриялық мәліметтер бұзылса, кем дегенде бүкіл жүйені маңызды модернизациялау қажет болады.

3.2 Ақпараттық жүйедегі енуді басқару

Ақпараттық жүйедегі енуді басқару мен бақылаудың екі бағыттары бар: физикалық және логикалық. Енуді физикалық басқару аппараттық және багдарламалық қамтамасыз етуге, сондай-ақ баспа, визуалды және аудио форматтарда ұсынылған ақпаратқа қолданылады. Енуді логикалық басқару - бағдарламалық қамтамасыз ету құралдарына және электронды түрде ұсынылған ақпаратқа қолданылады. Ол бағдарламалық құралдар арқылы жүзеге асырылады.

Енуді логикалық басқару - объектілердің құпиялылығы мен тұтастығын қамтамасыз ету және белгілі бір дәрежеде олардың қолжетімділігін қамтамасыз етуге арналған (рұқсат етілмеген пайдаланушыларды қызмет етуге тыйым салу арқылы) бірнеше пайдаланушы жүйелердің негізгі механизмі.

Енуді басқару негізінде идентификация және аутентификация жатыр.

Егер сұбъект мен АҚЖ аумақтық бөлінсе, онда қауіпсіздік тұрғысынан екі аспектіні қарастырған жөн:

– аутентификатор ретінде қызмет етеді;

– идентификация және аутентификация мәліметтерімен алмасу қалай ұйымдастырылған (және қорғалған).

Субъектілер мен объектілер жиынтығы бар. Енуді логикалық басқару міндеті болып әрбір «субъект-объект» жұптарының (кейбір қосымша шарттарға байланысты) көптеген рұқсат етілген операцияларын анықтау және белгіленген тәртіппен орындалуын бақылау табылады.

«Субъект-объект» қатынасын ену матрицасы түрінде қарастыруға болады, олардың жолдарында субъекттер, бағандарында – объектілер, ал жолдар мен бағандардың қиылысында орналасқан ұяшықтарда қосымша шарттар (мысалы, уақыт пен әрекет орны) және енудің кеңейтілген түрлері тіркеледі. Матрицаның фрагменті келесі 1-кестеде көрініс табады:

Кесте 1 – Ену матрицасының фрагменті

/	Файл	Бағдарлама	Байланыс желісі	Реляциялық кесте
Пайдаланушы 1	консольдан ORW	E	RW 8:00 бастап 17:00 дейін	
Пайдаланушы 2				A

"O" – ену құқығын басқа пайдаланушыға беруге рұқсат етуді білдіреді,

"R" – оқу

"W" – жазба,

"E" – орындау,

"A" – ақпарат қосу

Енуді логикалық басқару пәні ақпараттық қауіпсіздік саласындағы ең күрделісі болып табылады. Объект тұжырымдамасы (әсіресе ену түрлері) бір қызмет көрсетуден екінші қызмет көрсету үшін өзгереді. Операциялық жүйелер үшін объектілерге файлдар, құрылғылар және үрдістерді жатады.

Файлдар мен құрылғыларға қатысты көбінесе оқу, жазба, орындау (бағдарлама файлдары үшін), кейде жою және қосу құқығын қарастырады. Жеке құқығы ретінде басқа субъектілерге ену құқықтарын (иелену құқығы деп аталатын) беру мүмкіндігі болуы мүмкін. Үрдістерді құруға және жоюға болады. Қазіргі заманғы операциялық жүйелер басқа объектілерді де қолдана алады.

Реляциялық мәліметтер базасын басқару жүйелері үшін объект - мәліметтер базасы, кесте, процедура болып табылады. Кестелер үшін басқа да объектілердегі мәліметтерді іздеу, қосу, өзгерту және жою операциялары қолданылады.

Әртүрлі объектілер мен оларға қолданылатын операциялар енуді логикалық басқаруды орталықсыздандыруға әкеледі. Әрбір қызмет нақты бір субъектке белгілі бір операцияларды орындауға мүмкіндік беру туралы өзі шешім қабылдауы керек. Бірақ бұл заманауи объектілі-бағытталған көзқарасқа сай болса да, ол елеулі қиындықтарға алып келеді.

Көптеген объектілерге әр түрлі қызметтер арқылы енуге болады. Сондықтан, реляциялық кестелерге тек МББЖ құралдары арқылы емес, сонымен қатар тікелей файлдарды оқу арқылы да жетуге болады.

Мәліметтерді импорттау/экспорттау кезінде ену құқықтары туралы ақпарат (ол жаңа қызметте еш мағынасы жоқ) жоғалады.

Енуді логикалық басқарудың үш тәсілі бар:

– Ерікті басқару,
– Міндетті басқару,
– Рөлдік басқару.

Ерікті басқару кезінде қолжетімділік матрицасы тізімдер түрінде сақталады, яғни әрбір объект үшін «рұқсат етілген» субъекттердің тізімі олардың құқықтарымен бірге көрсетіледі. Көптеген операциялық жүйелер мен мәліметтер базасын басқару жүйесі қолжетімділікті басқаруды ерікті түрде жүзеге асырады. Ерікті басқарудың басты артықшылығы - әрбір «субъект-объект» жұбына тәуелсіз қолжетімділік құқығын беру. Бірақ ерікті басқаруда бірқатар кемшіліктер бар.

Жүйелік операторлар немесе әкімшілер ғана емес, сонымен қатар көптеген пайдаланушылар да сенімді болуы керек.

Ену құқықтары мәліметтерден бөлек болады. Құпия ақпаратқа қол жеткізетін пайдаланушыға ақпаратты қол жетімді файлға жазуға немесе зиянды бағдарламамен пайдалы утилитаны ауыстыруға ешнәрсе кедергі келтірмейді.

Мәжбүрлі бақылау жағдайында матрица анық түрде сақталмайды, тиісті ұяшықтардың мазмұны әр уақытта есептеліп отырады. Мұны істеу үшін әр субъект пен әрбір объектке қауіпсіздік белгілері беріледі. Қолжетімділікті басқару субъектінің және объектінің қауіпсіздік белгілерін сәйкестендіруге негізделген. бір мезгілде келесі екі шартты орындалған жағдайда субъект объектідегі ақпаратты оқи алады:

– субъектінің құпиялылық деңгейі объектінің деңгейінен төмен емес,
– объект қауіпсіздігі белгісінде тізімделген әрекеттердің барлық категориялары субъект белгілерінде болады.

Енуді рөлдік басқару

Көптеген пайдаланушылармен енуді басқарудың алғашқы екі түрі басқаруға өте қиын болып табылады. Ондағы байланыстар‘ саны объектілердің саны бойынша тұтынушылардың санына пропорционалды.

Енуді рөлдік басқарудың мәні – пайдаланушылар мен олардың артықшылықтары арасында аралық мәндер – рөлдер пайда болады (сурет 3). Әрбір пайдаланушы үшін бірнеше бір мезгілде рөлдер белсенді болуы мүмкін, олардың әрқайсысы оған белгілі бір құқықтар береді.

Сурет 3. Рөлдік ену құқықтары

Рөлдік ену құқықтардың нақты түрлеріне және оларды тексеру әдістеріне қатысты бейтарап болып табылады; ол объектілі-бағытталған әдісті қолданады, яғни объектілерге бағытталған жүйелердегі мұраға ұқсас рөлдер арасындағы қатынастарды орнату арқылы еркін түрде көптеген пайдаланушыларда басқарылатын кіруді бақылаудың жүйеастын жасауға мүмкіндік береді.

Рөлдер пайдаланушылардан айтарлықтай аз. Нәтижесінде басқарылатын байланыстар саны пайдаланушылар мен объектілердің санына пропорционалды болады.

Енуді рөлдік басқару келесі негізгі ұғымдармен жұмыс істейді:

- пайдаланушы;
- пайдаланушың жұмыс жасау сеансы;
- рөлі (ұйымдық құрылымға сәйкес анықталады);
- объект;
- операция (объектіге байланысты);
- ену құқығы (белгілі бір объектілерде белгілі бір операцияларды орындауға рұқсат беру).

Тұтастай алғанда, рөлдер пайдаланушылар мен құқықтар арасында «көптен көпке» қатынасына ие. Көптеген пайдаланушыларға рөлдерді тағайындауға болады; бір пайдаланушы бірнеше рөлге тағайындалуы мүмкін. Пайдаланушының сеансы кезінде, ол тағайындалған рөлдердің жиыны белсендіріледі, яғни ол белсенді рөлдерге жатқызылған құқықтар бірлестігінің иесі болады.

Пайдаланушы бір уақытта бірнеше сеанстарды аша алады.

Рөлдер арасында мұра байланысы анықталуы мүмкін. Егер R2 рөлі R1-нің мұрагері болса, онда R1-дің барлық құқықтары R2-ге жазылады, ал барлық R2 пайдаланушыларына R1 тағайындалады. Рөлдер мұрасы объектілі-бағытталған бағдарламалаудағы класстар мұрасына сәйкес

келеді, тек ену құқығына класс әдістері, ал пайдаланушыларға класстар объектісі (даналары) сәйкес келеді.

Пайдаланушылар құрамын біртіндеп нақтылау және құқықтарды бірте-бірте толықтыра отырып, «қызметкердің» рөліне жататын минималды құқықтардан (және максималды пайдаланушыларды) бастап, рөлдердің иерархиясының қалыптасуын елестете аламыз (сурет 4). Бірақ басшыға басқа рөлдер сиякты шексіз құқығы болмайды. Әрбір рөл үшін қызметтік міндеттерін атқару үшін қажет нәрсені ғана шешуге болады.

Сурет 4. Рөлдер иерархиясы

Рөлдік басқаруды енгізу үшін міндеттерді бөлудің екі тұжырымдамасы қарастырылады: статикалық және динамикалық.

Міндеттердің статикалық бөлінуі пайдаланушылар рөлдеріне қатысты шектеулерді енгізеді. Бір рөлге иелік ету пайдаланушыға басқа рөлдердің белгілі бір жиынтығына тыйым салады.

Міндеттердің динамикалық бөлінуі статикалық бөлінуден айырмашылығы олар тек белгілі бір пайдаланушы үшін бір мезгілде белсенді (соның ішінде әртүрлі сеанстарда) болып саналатын рөлдерде қарастырылады. Мысалы, бір пайдаланушы кассир мен контроллердің рөлін атқара алады, бірақ бір мезгілде емес; контролер болу үшін ол алдымен кассалық тіркеуді жабуы керек. Осылайша, сенімнің уақытша шектелуі жүзеге асырылады.

Енудің рөлдік басқаруын әкімшілендіру келесі функциялардың үш категорияларын дамытуды қарастырады:

Әкімшілендіру функциялары:

– рөлді немесе пайдаланушыны жасау/жою,

– пайдаланушыны немесе рөлді тағайындау немесе бар бірлестікті жою,

– бар рөлдер арасындағы мұра қатынасын жасау/жою,

– міндеттерді бөлуге арналған шектеулерді жасау/жою.

Басқару функциялары:

– пайдаланушының жұмыс жасау сеансын ашу,

– жаңа рөлді белсендіру,

– рөлді ажырату,
– енудің заңдылығын тексеру.

Ақпараттық функциялар:

– рөлдерді тағайындаған пайдаланушылар тізімін алу,
– пайдаланушымен байланысқан рөлдердің тізімін алу,
– рөлге тіркелген құқықтар туралы ақпарат алу,
– берілген пайдаланушының құқықтары туралы,
– сол уақыттағы белсенді рөлдер мен құқықтар туралы,
– пайдаланушы объект бойынша жұмыс істей алатын операциялар туралы,
– статикалық/динамикалық міндеттерді бөлу туралы.

3.3 Протоколдау және аудит

Протоколдау деп АЖ-де болып жатқан оқиғалар жөніндегі ақпараттарды жинау және жинақтауды түсінеміз. Аудит - жинақталған ақпараттарды нақты уақыт режимінде немесе мерзімді түрде талдау. Белгілі бір жағдайларға автоматты жауап беретін оперативті аудит белсенді деп аталады.

Протоколдау мен аудиттің жүзеге асырылуы келесі мақсаттарды шешеді:

– пайдаланушылар мен әкімшілердің есеп берушілігін қамтамасыз ету; ұстаушы құрал болып табылады;
– оқиғалардың кезектілігін қайта қалпына келтіру мүмкіндігін қамтамасыз ету - сервистерді қорғаудағы осалдылықтарды анықтайды, шабуылдың себепшісін табады, келтірілген зиян мөлшерін және қалыпты жұмысқа қайта оралуын бағалайды;
– ақпараттық қауіпсіздікті бұзу әрекеттерін анықтау;
– проблемаларды анықтау және талдау үшін ақпарат беру.

Тиімді протоколдауды жүзеге асыру үшін қандай оқиғаларды тіркеу керектігін және қандай дәрежеде егжей-тегжейлі қарастыру керектігін анықтау керек. Тым кең және егжей-тегжейлі протоколдау АЖ-нің өнімділігін төмендетіп қана қоймай (ол қолжетімділікке кері әсерін тигізеді), сонымен қатар аудитті қиындатады, яғни ақпараттық қауіпсіздікті жоғарылатпайды, керісінше төмендетеді.

Протоколдауды міндетті түрде талап ететін басты оқиғалар:

– жүйеге кіруге тырысу (сәтті немесе сәтсіз);
– жүйеден шығу;
– қашықтағы жүйеге кіру;
– файлдармен операциялар (ашу, жабу, атын өзгерту, жою);
– қауіпсіздіктің артықшылықтарын немесе басқа да атрибуттарын ауыстыру.

Оқиғаны протоколдау кезінде кем дегенде мынадай ақпаратты жазу ұсынылады:

- оқиғаның күні мен уақыты;
- пайдаланушының бірегей идентификаторы - әрекет бастамашысы;
- оқиға түрі;
- әрекеттің нәтижесі (сәттілік немесе сәтсіздік);
- сұраныстың көзі (мысалы, терминалдың атауы);
- қозғалған объектілердің атаулары (мысалы, ашылған немесе жойылған файлдар);
- қорғау мәліметқорларына енгізілген өзгерістердің сипаттамасы (мысалы, жаңа объектінің қауіпсіздік белгісі).

Белгілі бір пайдаланушылар мен оқиғалар үшін таңдамалы протоколдауды қолдануға болады.

Протоколдау мен аудиттің тән ерекшелігі - басқа қауіпсіздік құралдарына тәуелділігі болып табылады. Идентификация және аутентификация пайдаланушы есептілігінің жөнелту нүктесі болып табылады, логикалық қол жеткізуді басқару тіркеу мәліметтерінің құпиялылығы мен тұтастығын қорғайды.

Әртекті жүйедегі протоколдау мен аудитті жүзеге асырудың күрделі болуының кем дегенде екі себебі бар:

- қауіпсіздік үшін маңызды (мысалы, маршрутизаторлар) кейбір құрамдас бөліктер өздерінің протоколдау ресурстарына ие болмауы мүмкін, демек оларды протоколдау функцияларын орындайтын басқа элементтермен экрандауға болады,
- жүйенің әр түрлі элементтеріндегі оқиғаларды өзара үйлестіру қажет.

3.4 Шифрлау

Шифрлау – ақпаратты кілттің көмегінсіз дұрыс мәліметтер алу қиын немесе мүмкін емес формаға түрлендіру.

Дешифрлау – бастапқы ақпаратты кілт пайдалану арқылы қалпына келтіру.

Қайта шифрлау – бастапқы ақпаратты кілтсіз қалпына келтіру.

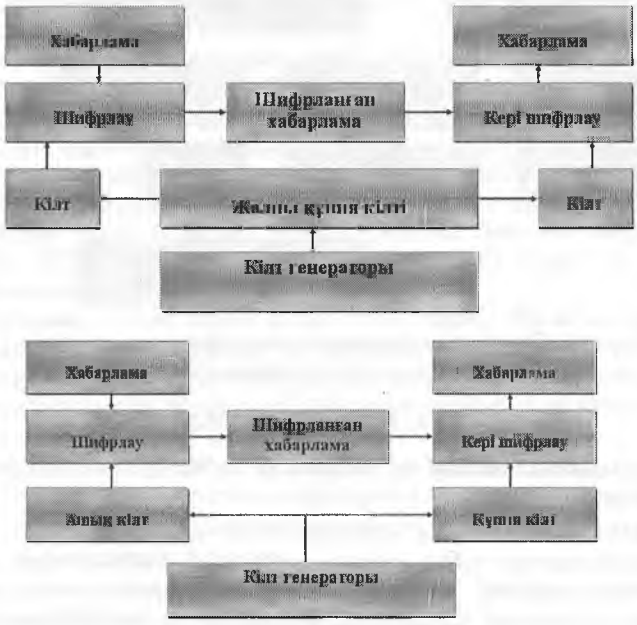
Шифрлаудың екі түрі қарастырылады: симметриялық және асимметриялық.

Кілт - шифрлау және дешифрлау алгоритмдерінің параметрлерін анықтайтын мәліметтер жиынтығы.

Симметриялық шифрлау кезінде мәліметтерді шифрлау және дешифрлау үшін бір кілт қолданылады. Егер мәліметтер бір АЖ субъектісінен екіншісіне берілсе, онда бұл кілт жөнелтушіге де, хабардың қабылдаушыға да белгілі болуы керек. Кілт мәліметтерді алмасудағы

қатысушылардың біреуімен жасалуы және екіншісіне берілуі тиіс. Бұл кілтті сенімді беру проблемасына әкеледі. Жіберу проблемасына қосымша, симметриялық шифрлаудың тағы бір кемшілігі, хабардың алушысы бұл хабар белгілі бір жіберушіден келгенін дәлелдей алмайды, себебі сол хабарламаны жіберушінің өзі жасаған да болуы мүмкін.

Егер мұндай мәліметтер болмаса, бұл мәселелер туындамайды. Мысалы, қатты дискідегі мәліметтерді шифрлау жағдайында (5-сурет).



Сурет 5. Қатты дискідегі мәліметтерді шифрлау

Асимметриялық әдісте екі кілт қолданылады. Олардың біреуі ашық, шифрлау үшін пайдаланылады, екіншісі - құпия, кері шифрлау үшін. Екі кілт бір-бірімен байланысты болуы қажет және хабарды алушымен жасалуы керек. Ашық кілт хабарламаның жіберушісіне жөнелтіледі. Ашық кілтті білу хабарды кері шифрлауға мүмкіндік бермейді.

Асимметриялық шифрлау әдістерінің айтарлықтай кемшілігі олардың төмен жылдамдығы (асимметриялық әдістер 3-4 ретке баяу болып табылады), сондықтан бұл әдістер симметриялық әдістермен біріктірілуі керек (6-сурет).

Жіберуші қолданатын құпия кілтін беру арқылы тиімді шифрлау мәселесін шешу үшін хабарлама алдымен кездейсоқ кілтпен симметриялы түрде шифрленеді, содан кейін бұл кілт алушының ашық кілтімен шифрленеді, содан кейін хабар мен шифрланған кілт алушыға жіберіледі.

Сурет 6. Симметриялық және асимметриялық шифрлау әдістерінің біріктірілуі

3.5 Тұтастылықты бақылау

Тұтастылықты бақылау негізінде екі ұғым жатыр:

- хэш-функциясы;
- электронды цифрлық қолтаңба (ЭЦҚ).

Хэш-функциясы – бұл, әдетте блоктарды байланыстыру арқылы симметриялы шифрлау әдісімен жүзеге асырылатын қиындатылған мәліметтерді түрлендіру. Соңғы блокты шифрлау нәтижесі (бұрынғыларға байланысты) осы хэш функциясының нәтижесі болып табылады.

Тұтастығы тексерілуі қажет мәліметтер, хэш функциясы және бастапқы мәліметтерге қолданудың алдын-ала есептелген нәтижесі болуы керек (дайджест деп аталатын). Хэш-функцияны – H, T – алынған мәліметтер, T' – тексерілетін мәліметтер деп белгілейміз. Мәліметтер тұтастығын бақылау h(T') = h(T) теңдік арқылы орындалады. Егер ол орындалса, онда T' = T болып саналады.

Әртүрлі мәліметтер бойынша дайджесттердің сәйкестігі соқтығысу деп аталады. Негізінен, соқтығысу әрине мүмкін, көптеген дайджест жиынтықтарының күші жинақталған мәліметтер жиынтығының күшінен аз, бірақ H біржақты функция болғандықтан, қолайлы уақытта арнайы соқтығысуды ұйымдастыру мүмкін емес екенін білдіреді.

Электронды цифрлық қолтаңба хабардың тұтастығын қорғайды және жіберушінің жеке басын куәландырады, яғни мәліметтер көзінің тұтастығын қорғайды және бас тартудың негізі болып табылады.

ЭЦҚ әзірлеу және тексеру үшін келесідей шарттар орындалу қажет:
E'(D(T)) = D'(E(T)) = T
мұндағы, T – шифрланған хабарлама,
D – T құпия кілтпен шифрлау нәтижесі,
E – T ашық кілтпен шифрлау нәтижесі,
D' – T құпия кілт көмегімен дешифрлау нәтижесі,
E' – T ашық кілт көмегімен дешифрлау нәтижесі.

Ассиметриялық шифрлауды пайдалану айтарлықтай кемшіліктерге ие. Зиянкес өзін басқа пайдаланушы ретінде көрсете отырып, кілт жұптарын (жалпыға ортақ және жеке) жасауы, ашық кілтті жариялауы және осы пайдаланушыға жіберілген хабарларды алуы мүмкін. Бұл кемшілікті жою үшін сандық сертификаттар қолданылады.

Мұның барлығы сертификаттау орталығы (СО) деп аталатын сенімді үшінші тараптың цифрлық қолтаңбасы арқылы бекітілген.

Цифрлық сертификат сертификат иесінің ашық кілті мен оның сәйкестендіру мәліметтерінен тұрады. Мұның барлығы сертификаттау орталығы (СА) деп аталатын сенімді үшінші тараптың цифрлық қолтаңбасы арқылы қол қойылады.

Пайдалану СО-на өзінің жеке кілтін сенімді түрде жеткізеді және оның түпнұсқалығын растайды. СО сертификатты құрайды. Сертификатты алғаннан кейін пайдаланушы оны жариялайды. Егер басқа пайдаланушыға осы пайдаланушының ашық кілті хабарлама жіберу үшін қажет болса, ол ЭЦҚ тексеру арқылы куәліктің шынайылығын тексере алады.

Цифрлық сертификат келесідей элементтерден тұрады:
- сертификаттың реттік нөмірі (әр сертификатқа бірегей бүтін сан);
- электронды қолтаңба жасау алгоритмінің идентификаторы;
- цифрлық сертификат аты;
- сертификаттың қолданыылу мерзімі (басталу және аяқталу мерзімі);
- сертификат иесінің аты;
- сертификат иесінің ашық кілті (кілттер бірнеше болуы мүмкін);
- сертификат иесінің ашық кілттерімен байланысты алгоритмдердің идентификаторлары;
- электронды қолтаңба – барлық бұрынғы өрістегі СО құпия кілтімен шифрланған хэш-код.

ЭЦҚ жасау үшін келесі әрекеттер жүзеге асырылады:
- хабарламаның хэш-түрлендірілуі орындалады T – H(T),
- турлендіру нәтижежесі СО құпия кілтімен шифрланады СО – D(H(T)).

ЭЦҚ – ны тексеру үшін:
- ашық кілт көмегімен қолтаңба дешифрланады E'(D(H(T)))=H(T) ,
- хабарламаның хэш-түрлендірілуі орындалады T' – H(T'),
- теңдік тексеріледі H(T)=H(T').

3.6 Экрандау

Экран – екі жүйе арасындағы ақпараттық ағындарды бақылау арқылы бір ақпараттық жүйелер жиынтығындағы клиенттердің екінші жиынтыққа қолжетімділігін шектейтін құрал болып табылады. Ағындарды бақылау оларды сүзгілеуден және кейбір өзгертулерден тұрады.

Желілік ортаға тән қатерлермен әмбебап операциялық жүйелердің көмегімен күресу келесі себептерге байланысты мүмкін емес:

Әмбебап ОЖ әрдайым қателіктерден басқа, артықшылықтарға да ие, олар рұқсатты заңсыз алу үшін қолданылуы мүмкін. Бағдарламалаудың заманауи технологиясы мұндай үлкен бағдарламаларды қауіпсіз етуге мүмкіндік бермейді.

Күрделі жүйемен айналысатын әкімші жасалған өзгертулердің барлық салдарларын ескере алмайды.

Көп пайдаланушысы бар әмбебап жүйедегі осалдықтарды (оңай құпия сөздер, қолжетімділік құқығын заңсыз орнату, қараусыз қалған терминал) әрдайым пайдаланушылардың өздері тудырады.

Экранды сүзгілердің тізбегі ретінде елестетуге болады. Әрбір сүзгі мәліметтерді талдап оны өткізуі немесе өткізбеуі мүмкін, оны өзгертіп, мәліметтердің кей бөлігін келесі сүзгіге жіберуі немесе мәліметтерді пайдаланушының атынан өңдеп, жіберушіге қайтаруы мүмкін.

Қолжетімділікті шектеу функциясынан басқа, экрандар ақпарат алмасуды протоколдауды жүзеге асырады.

Әдетте экранда симметриялы емес, ол үшін «ішінде» және «сыртында» түсініктері анықталған. Экрандаудың міндеті ішкі аланды ықтимал шабуылшы сыртқыдан қорғау болып табылады.

Экрандау ішкі қызметтің қолжетімділігін қамтамасыз етуге, сыртқы әсерлерді азайтуға немесе тіпті алып тастауға, ішкі қауіпсіздік қызметтерінің осалдығын төмендетуге көмектеседі.

Экрандау сонымен қатар ұйымның АЖ-нің құпиялылығын сақтау үшін сыртқы ортаға бағытталған ақпараттық ағындарды бақылауға мүмкіндік береді.

Экрандау қауіпсіздік қызметі ретінде тек желілік ортада ғана емес, сонымен қатар хат алмасулар болып тұратын кез-келген басқа да ортада қолданылуы мүмкін. Мысал – объект әдістерін іске қосу үшін хат алмасу жүріп жатқан кезде объектілі-бағдарланған бағдарламалық жүйелердегі объектілерге қолжетімділікті шектеу.

Экрандау белгілі бір ақпараттық қызметтерді, мысалы, электрондық поштаны қорғайтын ішінара болуы мүмкін.

Өзін-өзі бақылау сұрақтары:

1. Объектіні аутентификациялау-
a) объектінің шынайылығын тексеру
b) тұтынушыны тексеру
c) пайдаланушының қатынау мүмкіндіктерін тексеру
d) телекатынас арналарымен тасымалданатын мәтіндерді аутентификациялау
e) қолтаңба қою және қолтаңбаны тексеру

2. Идентификатор көмегімен-
a) жүйе тұтынушыны таниды
b) объектінің шынайылығын тексереді
c) пайдаланушының қатынау мүмкіндіктерін тексеру
d) телекатынас арналарымен тасымалданатын мәтіндерді аутентификациялауға болады
e) қолтаңба қою және қолтаңбаны тексеруге болады

3. Ақпаратты қорғауға бағытталған іс- әрекеттердің идентификациялау процедурасы:
a) ақпаратқа қол жеткізгісі келген субъектің заңдарын тексеру
b) қол жеткізулік оңтайлығын және жасырындылығын қолдауды түсінеді.
c) жүйедегі өзгерістерді тексеру, тіркеу
d) ақпаратқа қол жеткізгісі келген заңды субъектің ішінен нақты аттарын белгілейді
e) өкілділікті ұсыну. Заңды субъектінің ішінен нақты аттарын белгілейді, заңды субъектердің қол жеткізе алатын ресурстарын белгілейді

4. Ақпаратты қорғауға бағытталған іс- әрекеттердің аутентификциялау процедурасы:
a) ақпаратқа қол жеткізгісі келген заңды субъектің ішінен нақты аттарын белгілейді
b) өкілділікті ұсыну. Заңды субъектінің ішінен нақты аттарын, заңды субъектердің қол жеткізе алатын ресурстарын белгілейді
c) қол жеткізулік оңтайлығын және жасырындылығын қолдауды түсінеді
d) ақпаратқа қол жеткізгісі келген субъектің заңдарын тексеру
e) жүйедегі өзгерістерді тексеру, тіркеу

5. Ақпаратты қорғауға бағытталған іс- әрекеттердің авторизациялау процедурасы:
a) өкілділікті ұсыну. Заңды субъектінің ішінен нақты аттарын белгілейді, заңды субъектердің қол жеткізе алатын ресурстарын белгілейді

b) ақпаратқа қол жеткізгісі келген субъектің заңдарын тексеру
c) ақпаратқа қол жеткізгісі келген заңды субъектің ішінен нақты аттарын белгілейді
d) жүйедегі өзгерістерді тексеру, тіркеу
e) қол жеткізулік оңтайлығын және жасырындылығын қолдауды түсінеді

6. Аутентификация (шынайылықты тексеру)-
a) Хабарды алушы хабарды жіберуші көзді анықтай алуы керек. Хабар жіберуші өзінің шынайылығын дәлелдеу кажет
b) Хабар алушы колына түскен мәліметтің жол жөнекей өзгермегендігіне көз жеткізуі керек
c) Хабарды жіберуші кейіннен жасаған іс— әрекеттерінен тайынбауы кажет
d) Хабар жіберуші немесе алушы кейбір мәліметті жасыра алатындай болуы керек
e) Қасқұнем шын хабарды жалған хабармен ауыстыра алмауы кажет

7. Парольдер –
a) тек қана пайдаланушыға мәлім мәліметтің негізінде бірдейлестіруді және сәйкестендіруді қамтамасыз ететін ең таралған әдіс
b) қол жеткізуді басқарудың белгілі бір саясатына сәйкес ақпаратқа және қолданбалы жүйенің қызметіне пайдаланушының қол жеткізуін басқарады
c) кез келген жүйелік қосалқы бағдарламаны, операциялық жүйені бағдарламалық қамтамасыз етеді
d) ақпаратты пайдаланатын басқадай жүйені қатерге қоймауды қамтамасыз етеді
e) бағдарламалық кодтарды, жүйелерді немесе қосымшаларды басқару құралдарының жұмысын рұқсатсыз қол жеткізуден қорғайды

8. A -
a) Пароль алфавитінің қуаты
b) Пароль ұзындығы
c) Парольдық кеңістіктің қуаты
d) Парольды таңдау жылдамдығы
e) Парольдың жарамдылық мерзімі

9. L -
a) Пароль ұзындығы
b) Пароль алфавитінің қуаты
c) Парольдық кеңістіктің қуаты
d) Парольды таңдау жылдамдығы
e) Парольдың жарамдылық мерзімі

10. S -
a) Парольдық кеңістіктің қуаты
b) Пароль ұзындығы
c) Пароль алфавитінің қуаты
d) Парольдың жарамдылық мерзімі
e) Парольды таңдау жылдамдығы

11. V -
a) Парольды таңдау жылдамдығы
b) Парольдық кеңістіктің қуаты
c) Пароль ұзындығы
d) Пароль алфавитінің қуаты
e) Парольдың жарамдылық мерзімі

12. T -
a) Парольдың жарамдылық мерзімі
b) Парольды таңдау жылдамдығы
c) Парольдық кеңістіктің қуаты
d) Пароль ұзындығы
e) Пароль алфавитінің қуаты

13. Парольдер қарастырылады -
a) жүйеге ену үшін қажетті кілттер ретінде
b) құжатты сақтау үшін
c) ақпаратты жасыру үшін
d) ақпаратты сақтау үшін
e) жүйені тұйықтау үшін қажетті кілттер ретінде

14. Парольдер неше топқа бөлінеді ?
a) 7
b) 5
c) 3
d) 4
e) 2

15. Парольдер ұзындығы неше символдан аспау керек ?
a) 6
b) 7
c) 8
d) 5
e) 1

4 АҚПАРАТТЫ ҚОРҒАУ ҚҰРАЛДАРЫ

Жалпы ақпаратты қорғауды қамтамасыз ету құралдары, жүзеге асу тәсіліне байланысты, бірнеше топтарға бөлуге болады: техникалық (аппараттық), бағдарламалық, аралас аппаратты-бағдарламалық, ұйымдастырушы.

Техникалық (аппараттық) құралдар – аппаратты құралдармен ақпаратты қорғау тапсырмаларын шешетін типтері бойынша әртүрлі құрылғылар (механикалық, электромеханикалық, электронды және т.б.). Олар физикалық енуге төтеп береді, немесе, егер ену болған жағдайда, онда бүркемелеу көмегімен ақпаратқа енуге кедергі жасайды. Тапсырманың бірінші бөлігі кілттер, терезедегі торлар, қорғау сигнализациялары және т.б. Екіншісі – дыбыс (шу) генераторы, желілік фильтрлер, сканерлейтін видеобақылағыштар және де ақпараттың ағып кету арналарын жабатын немесе оларды табатын көптеген басқада құрылғылар.

Техникалық құралдар артықшылықтары: сенімділігі, субъектілі факторларға тәуелсіздігі, түрлендіруге төзімділігі.

Қорғаудың аппараттық құралдарына әртүрлі электронды, электронды – механикалық, электронды – оптикалық құрылғылар жатады. Қазіргі таңда аппараттық құралдардың бірнеше түрлері жасалды, олардың кең тарағаны келесілер:

– қорғау реквизиттеріне арналған арнайы регистрлер: парольдер, сәйкестендіру коды, грифтар немесе құпиялық деңгейі;

– идентификациялау мақсатында адамдардың жеке сипаттамаларын (дыбыс, іздер) өлшеу құрылғылары;

– шығарылатын мәліметтер адресін тексеру мақсатында байланыс желісіндегі ақпаратты жіберуді үзу сызбалары;

– ақпаратты шифрлауға арналған құрылғылар (криптографиялық әдістер).

Аппараттық қорғау құралдарының әлсіз тұстары – икемділіктің жетіспеуі, көлем мен массаның көптігі, құнының жоғарылығы.

Бағдарламалық құралдар пайдаланушыны идентификациялауға, енуді бақылауға, ақпаратты шифрлауға, қалған ақпаратты, қорғау жүйесін мәтіндік бақылауды жоюға арналған бағдарламалар. Бағдарламалық құралдар артықшылығы – әмбебаптылығы, икемділігі, сенімділігі, орнату қарапайымдылығы, түрлендіру мен дамуға қабілеттілігі.

Кемшілігі – желі функционалдылығының шектеулілігі, файл-сервер мен жұмыс жасау станцияларының ресурстарының бөлігін қолдану, кездейсоқ өзгертулерге сезімталдылығының жоғары болуы, компьютер типтеріне тәуелділігінің мүмкіндігі (олардың аппараттық құралдары).

Аралас аппаратты-бағдарламалық құралдар бөлек аппараттық және бағдарламалық құралдардың функцияларын жүзеге асырады және аралық қасиеттерге ие.

4.1 Ақпаратты қорғаудың инженерлік-техникалық принциптері

Жалпыға белгілі, ақпаратты қорғаумен айналысатын қауіпсіздік бөлімдеріне ақпаратқа енудің ақпаратты құралдарымен жабдықталған әртүрлі ұйымдар мен шабуылшыларға қарсы тұрады.

Осыған байланысты, қауіпсіздік бөлімдерінің қорғау құралдары мен тәсілдерінің мүмкіндіктері шабуылшылар мүмкіндіктерінен кем болмауы тиіс. Сондықтан, ақпаратты қорғау негізін ақпарат алу принциптеріне аналогты принциптерінен құралуы қажет, соның ішінде:

1. Ақпаратты қорғау үздіксіздігі. Кез келген уақытта ақпараттық қауіпсіздікке төнетін қауіп-қатерді бейнелеудегі қорғау жүйесінің тұрақты дайындығын сипаттайды;
2. Белсенділігі;
3. Жасырындылығы;
4. Мақсаттылығы.

Бұл принциптер, нақты ұсыныстар болмағанымен, алайда ақпаратты қорғау құралдары мен тәсілдерге қойылатын жалпы талаптарды анықтайды.

Келесі принцип топтары ақпаратты қорғауды ұйымдастырудағы негізгі кәсіби көзқарастарды сипаттайды, қорғаудың рационалды деңгейін қамтамасыз етеді және шығындарды қысқартуға мүмкіндік береді:

1. ақпарат құндылығын қорғау деңгейінің сәйкестігі;
2. қорғау икемділігі;
3. көпаймақтық қоргау;
4. ақпаратты қорғау көптілігі.

Бірінші принцип қорғау құралдары мен тәсілдеріне қолданатын экономикалық орындылығын анықтайды. Ол дегеніміз ақпаратты қорғауға кеткен шығын қорғалатын ақпарат бағасынан жоғары болмауы тиіс.

Өйткені, ақпарат бағасы – айнымалы мән, уақыт пен ақпарат көзіне байланысты. Ақпаратты қорғауға кеткен уақыт икемді болуы қажет.

Қорғау икемділігі ақпараттық қауіпсіздіктің өзгерген талаптарына сәйкес қорғалу деңгейінің өзгеру мүмкіндігімен сипатталады.

Ақпараттық қауіпсіздіктің қажетті деңгейіне ақпараттың көптігі мен көпаймақтылығы жетеді.

Типтік зоналарға жатады: қорғау объектісі алатын қоршаумен немесе шартты сыртқы шекарамен шектелген территория (аумақ), территориядағы ғимарат, дәліз немесе оның бөлігі, шкаф, сейф, қойма.

Зоналар тәуелсіз (ғимарат, бөлім), қиылысқан және кірістірілген (бөлмедегі сейф, ғимараттағы бөлмелер, территориядағы ғимарат) болуы мүмкін.

Шабуылшылардың зонаға енуіне қарсы тұру мақсатындағы сол аймақта, ережеге сәйкес, бір немесе бірнеше қорғау шекаралары (рубежи) жасалады.

Қорғау шекаралары зоналар ішінде, яғни шабуылшылардың мүмкін болатын қозғалысына да немесе басқа да тасымалдағыштар, соның ішінде электромагниттік және акустикалық өрістер таралуына да жасалынады. Мысалы, акустикалық ақпаратты тыңдаудан қорғау үшін ғимаратта акустикалық экран түріндегі қорғау шекарасы орнатылуы мүмкін. Әрбір зона ондағы ақпараттық қауіпсіздік деңгейімен сипатталады.

Зонадағы ақпараттық қауіпсіздік тәуелді:

1. ақпарат көздері мен шабуылшылар немесе ақпаратқа ену құралдарының арасындағы арақашықтық.

2. Шабуылшылар қозғалысына немесе ақпарат тасымалдаушыларды таратудағы қорғау шекараларының саны мен деңгейі.

3. Зонаға автокөліктер мен адамдар енуін басқару құралдары мен тәсілдер тиімділігі.

4. Зоналар ішіндегі ақпараттық бойынша шаралар.

Жоғары қарастырылған принциптер жалпы ақпараттық қорғауға жатады:

1. Ақпараттық қорғау бойынша шаралар ұйымдастыратын ұйым қызметкерлерінің талаптары мен қосымша тапсырмаларының азайтылуы.

2. Жүйенің техникалық құралдар жұмысының сенімділігі.

3. Ақпараттық қауіпсіздікті қамтамасыз ету жүйесі элементтеріне шектеулі және бақыланған енуі.

4. Қорғау объектісін кез келген уақытта функциялаудағы жүйе жұмысының үзділіксіздігі, соның ішінде, мысалы, электроэнергияның қысқа уақытты өшірілуі.

5. Қоршаған ортаның өзгеруіне жүйенің бейімделуі.

Аталынып көрсетілген принциптердің мәні айқын, бірақ соңғы принципіне толықтай тоқталған жөн.

Себебі, нақты ұйымдағы ақпараттық қауіпсіздік құралдары мен тәсілдері жөнінде жабық ақпарат уақыт өте келе көптеген адамдарға белгілі бола бастайды, нәтижесінде бұл ақпараттың шабуылшыға жету мүмкіндігі артады. Сондықтан мақсатты түрде ақпараттық қрғау жүйесі құрылымын мерзімді немесе қорғау жүйесі жөнінде ақпараттың ағып кету мүмкіндігі жеткілікті көрінгенде, мысалы, қауіпсіздік қызметінің ақпараттық қызметкері кенеттен жұмыстан шыққанда өзгертуі қажет.

4.2 Техникалық құралдармен ақпаратты қорғаудың негізгі әдістері

Жалпы ақпараттық қорғаудың техникалық құралдары келесідей кеңістікті – уақытша жиектер мен шарттар қамтамасыз етеді:

– Ағып кету арналарының шығысындағы кедергі мен тасымалдағыш энергиясының арақатынасы

– Шабуылшы ақпарат көзі мен тасымалдағышты таба алмайды

– Ақиқат ақпарат орнына шабуылшы жалған ақпарат алады және ол бұл ақпаратты ақиқат деп санайды.

Бұл тізім келесідей қорғау әдістерін жүзеге асырады;

– Дұрыс ақпаратты жасыру;

– Шабуылшыға жалған ақпарат жіберу;

– Инженерлік конструкторлар, техникалық құралдар көмегімен шабуылшының ақпарат көзіне енуін тікелей тоқтату.

Жасырын ақпараттар құрылымдар мен энергия тасымалдаушыларға өзгерістер қарастырады, яғни шабуылшы ақпаратты тікелей немесе техникалық құралдар көмегімен белгілей алмайды.

Екі түрге бөлінеді: ақпараттық және энергетикалық жасырын.

Ақпараттық жасырын – семантикалық хабарлама, физикалық объект немесе сигналдардың жалған ақпараттық портретін жасау немесе өзгерту болып табылады.

Ақпараттық портрет деп хабарлама мәнін, объект немесе сигналдар белгілерін көрсететін элементтер жиынтығы мен олардың арасындағы байланысты атауға болады.

Дискретті семантикалық хабарламалар элементтері болып, мысалы әріптер, сандар немесе басқа да белгілер табылады, ал олардың арасындағы байланыс олардың тізбектілігін анықтайды.

Бақылау объектілері, сигналдар және заттардың ақпараттық портреттері болып олардың эталонды белгілік құрылым табылады. Келесідей ақпараттық портреттің өзгеру тәсілдері болуы мүмкін:

– портреттің ақпараттық түйінін туғызатын элементтер мен байланыс бөлігін жою;

– қалған элементтер арасындағы байланысты сақтау кезіндегі ақпараттық портрет элементтер бөлігін өзгерту;

– олардың санын сақтау кезіндегі ақпараттық портрет элементтерінің арасындағы байланысты өзгерту немесе жою.

Объектінің ақпараттық портретін өзгерту оның сыртқы түр бейнесінің, электрлік сигналдар мен олардан шығатын өрістер сипаттамаларының, құрылымдарының өзгеруіне алып келеді.

4.3 Ақпараттың ағып кету арналары

Ақпараттардың ағып кетуінің мүмкін болатын арналарын төрт топқа бөлуге болады.

1-ші топ – мәліметтерді өңдеу жүйесінің элементтеріне енуге байланысты, бірақ жүйенің компоненттеріне өзгерістер енгізуді талап етпейтін арналар. Бұл топқа мынандай арналар кіреді:

– қашықтан жасырын бейнебақылау немесе фотосурет;

– тыңдау құрылғыларын пайдалану;

– электромагниттік сәулелеуді тоқтату және т.б.

2-ші топ - жүйенің элементтеріне ену және оның компоненттерінің құрылымын өзгертуге байланысты арналар. Екінші топқа мыналар кіреді:

- өңдеу кезінде оны есте сақтау мақсатында ақпаратты бақылау;
- ақпаратты тасымалдаушыларды ұрлау;
- өңделген ақпараты бар өндірістік қалдықтарды жинау;
- басқа пайдаланушылардың файлдарынан мәліметтерді қасақана оқу;
- қалдық ақпаратты, яғни тапсырмаларды орындағаннан кейін магниттік таспада қалған мәліметтерді оқу;
- ақпаратты тасымалдаушыларды көшіру;
- пайдаланушылар тіркелген терминалдар туралы ақпаратқа енуді қасақана қолдану;
- өңдеу жүйелерінде қолданылатын ақпаратқа қол жеткізу парольдері мен басқа да реквизиттерді ұрлау үшін тіркелген пайдаланушылар арқылы бүркемелеу;
- ақпаратқа ену үшін «люктер», «тесіктер» және «айла-амалдарды» қолдану, яғни жүйелік бағдарламалық қамтамасыз ету компоненттерін (операциялық жүйелер, мәліметтер базасын басқару жүйелері және т.б.) жетілмегендігінен туындайтын, пайдалануға және пайдаланылатын бағдарламалау тілдері мәліметтерді өңдеудің автоматтандырылған жүйелерінде кіруді бақылау механизмін айналып өту қабілеті болып табылады.

3-ші топ - бұл топқа мыналар кіреді:

- арнайы тіркеу құрылғыларын жүйенің немесе байланыс желілерінің құрылғыларына заңсыз қосу (модемді және факсимильді байланысын басып алу);
- бағдарламаларды зиянды түрлендіру, бұл бағдарламалардың ақпаратты өңдеудің негізгі функцияларымен қатар, қорғалмаған ақпаратты рұқсатсыз жинау және тіркеуді жүзеге асыруы тиіс;
- қорғау механизмдерін зиянды түрде істен шығару.

4-ші топ - бұл топқа мыналар кіреді:

- тиісті қызметтердің лауазымды тұлғаларын парақорлық немесе бопсалау арқылы ақпаратты рұқсатсыз алу;
- қызметтің түрін білетін қызметкерлерді, таныстарды, қызмет көрсететін персоналдар мен туыстарын парақорлық пен бопсалау арқылы ақпарат алу.

Өзін-өзі бақылау сұрақтары:

1. Инженерлік-техникалық қорғау –

a) бұл ақпаратты қорғау мақсатында белгілі міндеттер атқаруға арналған арнайы органдардың, техникалық құралдар мен шаралардың жиынтығы

b) бұл қауіпсіздікті қамтамасыз ету үшін керек құрылғы жабдық және т.б техникалық шешімдер жиынтығы

c) бағдарламалар кешендері және әр түрлі мәліметтерді өңдейтін әдістер жиынтығы
d) бұл ақпаратты қорғаудағы арнайы математикалық және алгоритмдік әдістерінің жиынтығы
e) электрондық сұлба элементтерінің құраушыларының міндеттері және орындалуының жиынтығы

2. Техникалық қорғау әдісі келесі түрлерге бөлінеді:
a) аппараттық, бағдарламалық, аралас аппаратты-бағдарламалық
b) аппараттық, криптографиялық, аппаратты-бағдарламалық
c) аппараттық, криптографиялық, бағдарламалық
d) аппараттық, бағдарламалық, аппаратты- алгоритмдік
e) аппараттық, сызықтық, аппаратты-бағдарламалық

3. Ақпаратты қорғаудың әдістері мен құралдардың жіктелуі
a) Ұйымдастырушылық, ақпараттық, бағдарламалық, криптографиялық
b) Толықтық, анықтық, басқарушылық, конфеденциалдық
c) Қолданушылық, тасымалдылық, динамикалық, статикалық
d) Базалық, аймақтық, бүкіләлемдік, жергілікті
e) Қорғаушылық, заңдық, деңгейлік, бөліктік

4. Инженерлік-техникалық қорғау құралдары бөлінеді-
a) физикалық, аппараттық, бағдарламалық, криптографиялық
b) бағдарламалық және криптографиялық
c) физикалық, аппараттық, инженерлік, криптографиялық
d) физикалық, аппараттық, математикалық, криптографиялық
e) математикалық, технологиялық, бағдарламалық, криптографиялық

5. Инженерлік-техникалық қауіпсіздікті жабдықтау бөлінеді:
a) инженерлік және техникалық іс шаралар
b) инженерлік және аппараттық іс шаралар
c) физикалық және оптикалық іс шаралар
d) техникалық және криптографиялықіс шаралар
e) инженерлік және криптографиялық іс шаралар

6. Инженерлік іс-шараларға жатады:
a) ДК көмегімен қорғау, дабыл, акустикалық арнаны қолдану, бөлмені экрандау
b) физикалық, аппараттық, бағдарламалық, криптографиялық құралдар
c) аппараттық, бағдарламалық, аппаратты-бағдарламалық
d) математикалық, технологиялық, бағдарламалық, криптографиялық
e) аппараттық, бағдарламалық, техникалық

7. Техникалық іс-шараларға жатады:
a) физикалық, аппараттық, бағдарламалық, криптографиялық құралдар
b) ДК көмегімен қорғау, дабыл, акустикалық арнаны қолдану, бөлмені экрандау
c) аппараттық, бағдарламалық, аппаратты-бағдарламалық
d) математикалық, технологиялық, бағдарламалық, криптографиялық
e) инженерлік және криптографиялық іс шаралар

8. Аппараттық қорғау -
a) қауіпсіздікті қамтамысз ету үшін керекті құрылғы, жабдықтар және техникалық шешімдерден тұрады
b) арнайы бағдарламалық кешендер және әр түрлі мәліметтерді өңдейтін әдістерден тұрады
c) ақпаратты қорғаудағы арнайы математикалық және алгоритмдік әдіс
d) қорғау қабілеті жоғары, қорғалған аймақ, нашар қорғалған аймақты қамтиды
e) персоналдың жеке басының қауіпсіздігін қамтамасыз ету міндетін атқарады

9. Бағдарламалық қорғау
a) арнайы бағдарламалық кешендер және әр түрлі мәліметтерді өңдейтін әдістерден тұрады
b) қауіпсіздікті қамтамысз ету үшін керекті құрылғы, жабдықтар және техникалық шешімдерден тұрады
c) ақпаратты қорғаудағы арнайы математикалық және алгоритмдік әдіс
d) қорғау қабілеті жоғары, қорғалған аймақ, нашар қорғалған аймақты қамтиды
e) персоналдың жеке басының қауіпсіздігін қамтамасыз ету міндетін атқарады

10. Криптографиялық қорғау-
a) ақпаратты қорғаудағы арнайы математикалық және алгоритмдік әдіс
b) арнайы бағдарламалық кешендер және әр түрлі мәліметтерді өңдейтін әдістерден тұрады
c) қауіпсіздікті қамтамысз ету үшін керекті құрылғы, жабдықтар және техникалық шешімдерден тұрады
d) қорғау қабілеті жоғары, қорғалған аймақ, нашар қорғалған аймақты қамтиды
e) қол жеткізуді басқару қызметін атқарады

11. Физикалық қорғау-
a) қорғау қабілеті жоғары, қорғалған аймақ, нашар қорғалған аймақты қамтиды
b) ақпаратты қорғаудағы арнайы математикалық және алгоритмдік әдіс

c) арнайы бағдарламалық кешендер және әр түрлі мәліметтерді өңдейтін әдістерден тұрады
d) қауіпсіздікті қамтамысз ету үшін керекті құрылғы, жабдықтар және техникалық шешімдерден тұрады
e) қол жеткізуді басқару қызметін атқарады

12. Тұтастықты қолдау үшін -
a) аутентификация, өрістердің тұтастығын бақылау және тоқтапқалмастықты қамтамасыз ету тетіктері қолданылады
b) хаттамалар мәліметтердің тұтастығын қолдау мүмкіншіліғіне ие болу керек
c) тораптық ақпараттық қауіпсіздікті қамтамасыз ететін барлық шаралар барлық бөліктерінен қалыптасуы керек
d) тоқтапқалуларды бейтараптандыру құралдарының бар болуы керек
e) торапшаларды ажыратужәне пайдаланушылар топтарын бір-бірінен оңашалау керек

13. Аналитикалық түрлендіруде -
a) алгебраның матрицалық әдісі қолданылады
b) алгебраның логарифмдік әдісі қолданылады
c) бағдарламалау тілдері қолданылады
d) алгебраның интегралдау әдісі қолданылады
e) алгебраның көпмүшелерді қосу әдісі қолданылады

14. Интеграцияланған енуді басқару жүйесінің құрамына мыналар енеді:
a) енуді басқару және сақтық-дабыл сигналын беру
b) объектілерді бақылау; объектілерді қорғауды қамтамасыз ету; бейне жазуларды тіркеу, сақтау мен іздеу; енуді басқару жүйесімен интеграциялану
c) бейне бақылауды қорғау және РЕ компьютерді қорғаудың бағдарламалық-аппараттық кешенін орнату
d) телефондық сөйлесулерді жазу жүйесі; техникалық каналдар бойынша ақпараттарды жойылудан қорғау аппараттарын қолдану
e) ашық кілтті инфрақұрылым және желі аралық экрандарды анықиау

15. Қатынас құруды басқару функциясы -
a) торап арқылы қол жеткізуге болатын қорларды заңсыз (рұқсатсыз) пайдаланудан қорғауды қамтамасыз етеді
b) ақпаратты заңсыз (рұқсатсыз) алудан қорғауды қамтамасыз етеді
c) мәліметтер көзінің шынайылығын растауды қамтамасыз етеді
d) қолтаңба құрастыру және қол қойылған мәліметтер бөлігін тексеруді қамтамасыз етеді
e) байланысу орнатылмай қатынасу кезіндегі мәліметтердің жасырындылығын қамтамасыз етеді

5 КОМПЬЮТЕРЛІК ВИРУСТАР ЖӘНЕ ОЛАРДЫ ҚОРҒАУ

5.1 Компьютерлік вирустар және олардың түрлері

Компьютерлік вирус дегеніміз компьютерлік техника және ақпараттық технологиялар даму үрдісі кезінде пайда болған өзгеше құбылыс. Өз атауына компьютерлік вирустар биологиялық вирустармен белгілі ұқсастығына міндетті, олар:

– жоғары таралу жылдамдығына;

– өздігінен көбею қабілеттілігіне;

– әлі зақымдалмаған жүйелерді зақымдау қабілеттілігіне;

– жүйелерді замқымдау талғамдығына (әр вирус тек белгілі жүйелерге немесе біртекті жүйелер тобына ғана зиян келтіреді);

– олармен күресу қиыншылықтарына және т.б.

Компьютерлік вирустар ақпараттық жүйеге енген кезде залалсыз визуалді немесе дыбыс әсерлерімен шектелуі мүмкін, әйтпесе мәліметтердің жоғалуына немесе бұрмалануына, құпия ақпараттың жайылып кетуіне әкелуі мүмкін.

Вирустардың ең алғашқы мысалы ретінде 60-жылдары мейнфреймдерде пайда болған «қояндар-бағдарламалар» (the rabbit) жатқызуға болады. Олар ештеңе бүлдірген жоқ, бірақ жүйенің көбінен-көп ресурстарын тартып алып және басқа есептерден процессорлық уақытын алып, өзін бірнеше рет көбейту мүмкіншіліктері болды. «Қояндар» жүйеден жүйеге берілмеді және жергілікті құбылыс ретінде – компьютерге қызмет көрсететін бағдарламашылардың қателіктері болды.

1970-жылдардың басында ғаламдық компьютерлік желілер бойынша өздігінен көбейетін «The Creeper» (шырмауық) вирусы пайда болды. Ол зиянсыз, бірақ компьютерге оның иесінің келісімсіз және тілегіне қарсы кіруге болатынын көрсетті. Осы вируспен күресуге арналған алғашқы танымал «The Reaper» (орақшы) вирусқа қарсы бағдарлама құрылды. Ол Шырмауық тәрізді қалпына келіп отыратын және оған кездесетін соңғы барлық көшірмелерін жойып тастайтын.

Компьютерлік вирус дегеніміз не? Тарихта бірінші анықтама 1984 ж. Ф. Коэнмен берілді: «Компьютерлік вирус – бұл басқа бағдарламаларды жұқтыратын, оларға өзінің өзгертілген, көбею қабілеттілігінің сақталған көшірмесін енгізіп өзгертетін бағдарлама».

Қазіргі кезде компьютерлік вирус ретінде келесі қасиеттерге ие болған бағдарламалық кодты қабылданады:

– есептеу жүйесінің атқарушы объектілеріне жасалатын көшірмелерін енгізуін қамтамасыз ететін механизмнің бар болуы;

– өзінің көшірмелерін жасау қабілеттілігі, міндетті түрде түпнұсқамен дәл келмейтін, бірақ түпнұсқаның барлық қасиеттеріне ие болу (өздігінен қалпына келтіруі).

Мұндай қасиеттер қажетті, бірақ жеткіліксіз. Берілген қасиеттерді есептеу жүйесіндегі бұл зиянды бағдарламаның деструктивті және жасырынды әрекеттердің қасиеттерімен толықтыруы керек.

Компьютерлік вирустың міндетті қасиеті өз көшірмелерін (міндетті түрде түпнұсқамен дәл келмеуі) жасау мүмкіндігі және оларды есептеуіш желілерге және файлдарға, компьютердің жүйелік аумақтарына және басқа атқарылатын объектілерге енгізуі болып табылады. Сонымен қоса, көшірмелер ары қарай таралу қабілеттілігін сақтайды. Бұл шарттың ақырғы емес екенін ескерту керек.

Вирустарды жіктеуге мүмкіндік беретін негізгі төрт белгіні келтіруге болады (сурет 7):

- мекендеу ортасы;
- мекендеу ортасын жұқтыру әдісі;
- жұмыс істеу алгоритмнің ерекшеліктері;
- бұлдіргіш (деструктивті) мүмкіншіліктері.

Сурет 7. Компьютерлік вирустардың жіктелуі

Мекендеу ортасы бойынша компьютерлік вирустар файлдық, жүктейтін, желілік және макровирустар боп бөлінеді.

Файлдық вирустар атқарушы файлдарда орналасады – бұл ең көп таралған вирустардың түрі. Файлдық вирустар барлық танымал операциялық жүйелердің барлық атқарушы файлдарына ену мүмкін.

Бүгінгі күнге атқарылатын объектердің барлық типтерін зақымдандыратын вирустар белгілі: әмірлі файлдар (bat), жүктелетін драйверлер (sys) және орындалатын екілік файлдар (exe, com).

Жүктелуші вирустар өздерін не дискінің жүктелуші секторына (boot-сектор), не винчестердің жүйелік жүктемелеуіш (Master Boot Record) бар секторына көшіріп алады. Кейде жүктелуші вирустарды бутты деп атайды. Дисктерді жұқтыру кезінде жүктелуші вирустар өз кодын қандай да бір жүйені жүктеген кезде басқаруды алатын бағдарламаның орнына «алмастырады». Вирус жүйені қайта жүктелу кезінде жадыға оқытып және басқаруды жүктемелеушінің түпнұсқалық кодына емес, вирус кодына беруге мәжбүрлейді. Дискті жұқтыру кезіуде вирус көптеген жағдайда түпнұсқалық boot-секторды (немесе MBR) қандай да бір басқа (мысалы, бірінші бос) диск секторына көшіреді. Егер вирустың ұзындығы сектордың ұзындығынан үлкен болса, онда жұқтыратын секторға вирустың бірінші бөлігі, ал басқа бөліктері басқа (мысалы, бірінші бос) секторларға орналастырылады.

Желілік вирустар өздерін тарату үшін компьютерлік желілердің хаттамаларын немесе командаларын және электронды поштаны пайдаланады. Желілік вирустарды кейде «құрт» типті бағдарламалар деп атайды. Желілік құрттар nternet-құрттар (Internet бойынша таратылады), LAN-құрттар (жергілікті желі бойынша таратылады), IRC-құрттар (Internet Relay Chat) (чат арқылы таратылады) боп бөлшектенеді. Тағы аралас түрлері де бар.

Макровирустар кейбір мәліметтерді өндеу жүйелеріне (әсіресе Microsoft Word, Microsoft Excel редакторларына) енгізілген макротілдерде жазылған бағдарламалар болып табылады. Өзіндерінің көбеюі үшін маркотілдердің мүмкіндіктерін қолданады және олардың көмегімен өздерін бір зақымданған файлдан (құжат немесе кесте) басқаларға көшіреді. Вирустар басқаруды зақымданған файлды ашқан немесе жабқан кезде алады, стандартты файлдық функцияларын ұстап алады және содан кейін қандай да бір түрде үндеу жүретін файлдарды жұқтырады.

Мекендеу ортасын зақымдауына қарай компьютерлік вирустар резидентті және резидентті емес боп бөлінеді. Вирус және ол енген объект операциялық жүйеге біртұтас бөлік болғандықтан, жүктелу кезінде олар бір адрестік кеңістікте орналастырылады. Объектің жұмыс істеуі аяқталған кезде ол операциялық жадынан жүктеледі, сонымен коса бір уақытта сақталудың пассивті сатыға көшетін вирус та жүктеледі. Бірақ вирустардың кейбір түрлері жадыда сақталу және вирус тасымалдағыштың жұмысы аяқталған кезде де белсенді болу қабілеттілігі бар. Мұндай вирустарды резидентті деп аталады.

Сонымен, резидентті вирустар – бұл компьютерді жұқтыру кезде оперативтік жадында операциялық жүйенің жұқтыру объектілеріне үндеулерін ұстап қалып, содан кейін оларға еніп, өздерінің резиденттық

бөлшектерін қалтыратын вирустар. Осындай вирустар жадында сақталып компьютерді өшіргенше немесе операциялық жүйені қайта жүктегенше белсенді болып қалады.

Резидентті емес вирустар компьютердің жадын жұқтырмайды және белсенділігін шектеулі уақытта сақтайды.

Алгоритмнің жұмыс істеу ерекшелігіне байланысты компьютерлік вирустар серіктер-вирустар (companion), құрттар-вирустар (worm), стелс-вирустар (көрінбейтін вирустар) және еполиморфты вирустар болып боленеді.

Серіктер-вирустардың әрекет ету механизмі атқарылатын файлдардың (exe) көшірмелерін жасаудан тұрады. Көшірмеге атқарылатын файлдың атына сәйкес ат қойылады, бірақ кеңейтілуі com болып өзгереді. Ортақ атты файлды іске қосқанда операциялық жүйе бірінші вирус болып табылатын, com кеңейтілуі бар файлды жүктейді. Содан соң вирус-файл exe кеңейтулі файлды іске қосады.

Құрттар-вирустар желіден жұмыс станцияға кіреді, олар вирусты жіберу мекенжайдарын желінің басқа абоненттер бойынша есептейді және вирусты жібереді. Вирус файлдарды өзгертпейді және дисктердің жүктемелеу секторларына жазылмайды.

Стелс-вирустар операциялық жүйенің зиян келтірілген файлдарға, секторларға үндеулерін ұстап алуы жолымен өздерінің тұратын ортасында барын жасырайды, және операциялық жүйені ақпараттың жұқтырмаған учаскілеріне жібереді, сөйтіп жұққан файлдардың «тазалығын» боямалайды. Вирус резидентті болып саналады, операциялық жүйенің бағдарламалары болып көрінеді және жадында жылжый алады. Мұндай вирустар үзгіштер пайда болған кезде жандандырылады, белгі бір әрекеттерді орындайды, соның ішінде жасырыну да бойынша, тек содан кейін сол үзгіштерді өндейтін операциялық жүйенің бағдарламаларына басқару беріледі. Сонымен, стел-вирустар жүйеде өз барын сездірмейді және вирусқа қарсы бағдарламалармен табылуынан аулақ жүреді.

Полиморфты вирустарға вирустық маскалардың (сигнатуралардың) – мәліметті вирусқа тұрақты кодтардың аймақтары – көмегімен оларды детекторлау мүмкін емес (немесе өте қиын) вирустар жатады. Бұл екі негізгі әдістермен жеткізіледі. Бірінші әдіс – вирустың негізгі кодын тұрақсыз кілтпен шифрлау. Бірақ, жүктеу сатында шифрді ашуға қамтамасыз ететін вирустың бөлшегі ашық түрінде сақталу қажет. Сондықтан екінші әдіс вирустың кодының осы бөлшегінің алғашқы түрі мәтінмен айырмашылық пайда болған, дегенмен жұмыстың нәтижесі өзгермес болып қалған түрлендірумен байланысты. Сондықтан көбінесе бір полиморфтық вирустың екі үлгісі бір бірімен ешқандай ұқсаушылық ие болмайды. Вирустардың барлық түрлерінде – файлдық, жүктеу және макровирустарда – полиморфизм кездеседі.

Деструктивті мүмкіндігіне қарай компьютерлік вирустар зиянсыз, қауіпсіз, қауіпті және өте қауіпті болып бөлшектенеді.

Зиянсыз вирустар – компьютердің жұмысына ешқандай әсер тигізбейтін вирустар, олар тек дискте бос жадты кішірейтеді. Оларда тек өздігінен таралу механизмі ғана орындалған.

Қауіпті емес вирустар – дискте бос жадты, сонымен қоса графикалық, дыбыстық және басқа эффектілерді кішірейтумен ғана шектеледі. Олар қосымшалардың жұмысына және мәліметтерге ешқандай әсер етпейді.

Қауіпті вирустар – компьютер жұмысының маңызды жаңылыстарға және осының әсерінен мәліметтердің бүлдіруіне әкеп соқтыратын вирустар.

Өте қауіпті вирустар – бағдарламалардың жоғалуына, мәліметтерді жойып тастауға, компьютер жұмыс істеу үшін керекті жүйелік ақпаратты өшіріп тастауға әкеп соқтыратын рәсімдерін жұмыс істеу алгоритмдеріне енгізілген вирустар.

5.2 Вирустардың өмір сүру циклі және олардың әсер ету белгілері

Компьютерлік вирустардың өмір сүру циклін басты екі кезеңге бөледі:

– сақтау және орындау.

Сақтау кезені вирус дискте енгізілген объектпен бірге сақталатын мерзімге сәйкес келеді. Осы кезенде вируске қарсы бағдарламаны қамтамасыз ету жағынан вирус ең осал болады, себебі ол белсенді емес және өзін өзі қорғау мақсатымен операциялық жүйенің жұмысын бақылауға мүмкіндігі жоқ. Кейбір вирустар (стелс-вирустар, полиморфтық вирустар) осы кезенде өз кодтарын табудан қорғау механизмдерін пайдаланады.

Компьютерлік вирустардың орындау кезеңі бес мерзім қосады: вирусты жадыға енгізу, құрбанды іздеу, табылған құрбанның жұқтыруы, деструктивті функцияларды орындау, басқаруды вирустың бағдарлама-сақтаушыға табыс ету.

Вирустың жадыға жүктеуі операциялық жүйемен вирус енгізілген орындалатын объектіні жүктеумен бір мезгілде асырылады. Мысалы, егерде пайдаланушы орындауға вирусы бар бағдарламалық файылды іске асырса, вирустық код бұл файылдың бөлігі болып жадыға жүктеледі. Ең жабайы уақигада вирустың жүктеу үдерісі дисктан оперативтік жадысына көшіру болып табылады, содан кейін вирустың денесінің кодына басқарма тапсырылады. Осы әрекеттер операциялық жүйемен орындалады, ал вирустын өзі енжар күйде болады.

Құрбанды іздеу екі әдістермен жүзеге асырылады

Бірінші әдіс – бұл операциялық жүйенің міндеттерін пайдаланумен «белсенді» іздеу. Мысалға, қазіргі каталогтағы орындау файлдерінің іздеу механизмдерін пайдаланылатын файл вирустары.

Екінші әдіс – бұл іздеудің «пассивті» механизмі. Тап осы жағдайда вирустар бағдарламалық файлдерге «қақпан» құрып қояды. Әдеттегідей, файлдық вирустар осындай қақпандарды операциялық жүйенің Exec функциясын ұстап қалумен құрады, ал макровирустар – File мәзірінен Save as командасының ұстап қалуы көмегімен.

Құрбанның жұқтыруы вирустың кодын құрбан ретінде тандалған объектіге өз-өзін көшірмелеу болады. Тіршілік орта бойымен топтастырылған вирустар түрлердің әрқайсылары үшін жұқтырудың өз ерекшеліктері болады.

Деструктивті функцияларды орындау. Өз-өзін көшірмелеуден басқа вирустар деструктивті функцияларды орындайды. Берілген белгі бойынша вирустардың топтастырылуы жоғарыда қарастырылған.

Басқаруды вирустың бағдарлама-сақтаушыға табыс ету мерзімі кейбір вирустарда болмауы мүмкін, себебі олар жұқпаланған бағдарламалардың жұмысқа қабілеттілігін сақтау тұралы қам жемейді. Басқа вирустарға бұл мерзім жадында дұрыс орындалу түрінде бағдарламаны қалпына келтірумен және басқаруды вирустың бағдарлама-сақтаушыға табыс етумен байланысты.

Компьютерді вируспен жұқтырылған кезде вирустарды табу өте маңызды. Ол үшін вирустардың пайда болуының негізгі белгілерін білу керек. Оған келесі белгілерді жатқызуға болады:

1. жұмыстың аяқталуы немесе жақсы қызмет етіп тұрған бағдарламалардың дұрыс жұмыс істемеуі;
2. компьютердің баяу жұмыс істеуі;

– операциондық жүйені жүктеудің мүмкін болмауы;

– файлдар мен каталогтардың жоғалып кетуі немесе олардың мазмұнының жойылуы;

– файлдардың түрлендірудің уақыты мен күнінің өзгеруі;

– файлдардың көлемінің өзгеруі;

– дискідегі файлдардың саны аяқ астынан көбеюі;

– бос жедел жадтың көлемінің маңызды кішіреюі;

– күтпеген хабарлар мен суреттердің экранға шығуы;

– қарастырылмаған дыбыстық сигналдарды беруі;

– компьютердің жиі тұрып қалуы және дұрыс жұмыс істемеуі.

Жоғарыда келтірілген белгілер міндетті түрде вирустар бар екенін білдірмейді, яғни басқа да белгілері болуы мүмкін.

5.3 Вирустарды анықтау әдістері және вирусқа қарсы бағдарламалар және кешендер

Компьютерлік вирустарды анықтау негізгі әдістеріне төмендегілерді жатқызуға болады:

- сканерлеу (эталонмен салыстыру әдісі);
- өзгерістерді табу;
- эвристикалық талдау;
- резидентті күзетшілерді қолдану (антивирустік мониторинг);
- вирустардан аппараты-бағдарламалық қорғанысы.

Сканерлеу – вирустарды анықтаудың ең қарапайым әдістерінің бірі. Сканерлеу іздестіру кезінде вирустың айрықша бөлігінің – сигнатураның – мәліметті вирус үшін ерекше кодтың тұрақты бір іздігі – файлдардан қарап шығуын түсінеді. Бағдарлама әр жолы сигнатураны өзгертіп, вирустың денесінің шифрлеуін пайдаланатын полиморфтық вирустарды қоспағанда, белгілі болып қалған вирустарды тіркейді.

Өзгерістер табылудың әдісін іске асырғанда тексерушібағдарламалар дисктің барлық шабуылға ұшырай алатын тұстарының алдын ала сипаттамаларын еске сақтайды, ал содан кейін оларды тексеріп тұрады. Вирустардың болжалды бар болу туралы мәліметтерді бағдарлама тексеру нәтижелері бойынша береді. Бұл әдістің құндылығы мынада: барлық вирустардың әр түрлерін, сонымен бірге жаңа белгісіз вирустерді табу мүмкіндігі бар. Кемшіліктер – жүйеге жұқтырылған түрінде түсетін файлдардың вирустарын анықтауға мүмкіндігі жоқ, макровирустарды табу үшін жарамсыз.

Эвристикалық талдаудың негізі келесідерден тұрады: вирустардың болуы мүмкін тұратын орталарының тексеруі және вирустарға сипатты командаларды табу, мысалы, оперативтік жадында резиденттік модульдердің жасау командалары, ОЖ тоқтамай дискілерге тікелей байланысу командалары. Күдікті командалар табылған кезде жұқтыру мүмкін екенін білдіретін хабар беріледі.

Резидентті күзетшілерді қолдану ЭЕМ оперативтік жадынында әрдайым болатын және қалған бағдарламалардың әрекеттерін байқап отыратын бағдарламалардың қолдануымен реттелген. Кейбір бағдарламамен күдікті әрекеттерді орындаған кезде (жазу үшін жүктеу секторларға үндеу, резидентті модульдарды жүйелі жадынға орналастыру, доғару әрекеттері қағып алу және т.б.), резидентті күзетші пайдаланушыға хабар береді. Бұл әдістің елеулі кемшілігі – жалған дабылдардың едәуір пайызы.

Вирустардан аппаратты-бағдарламалық қорғау арнайы тексерушілерді және олардың бағдарламалық жасақтамасын пайдалануын негіздейді. Тексеруші кеңейтудің тіркеуішіне орналатылады және жалпы шинаға қатынауға ие болады. Бұл дисктік жүйеге барлық сұрауларын

бақылауға мүмкіндік береді. Тексерушінің бағдарламалық жасақтамасында дисктегі әдеттегі жұмыс тәртібінде өзгертуге жол берілмейтін аймақтарды есте сақтандырылады. Сонымен, басты жүктеу жазбаның өзгеруіне, жүктеу секторларына, конфигурация файлдарына, орындалатын файлдарға және т.б. қорғау орналастыру болады. Кез келген бағдарламамен тиым салынған әрекеттер жасаған кезде,тексеруші сәйкес хабарлама жіберіп, ЭЕМ жұмысын блоктайды.

Аппаратты-бағдарламалық вирусқа қарсы жабдықтар бағдарламалық жабдықтардың алдында келесі құндылықтарға ие болады:

– үздікті жұмыс істейді;

– әсер ететін механизымына қарамай, барлық вирустрады анықтайды;

– вирустың немесе біліктігі жоқ пайдаланушыдың жұмыс істеу натижесінің әрекеттерін блоктайды.

Берілген қорғау жабдықтардың кемшілігі олардың ЭЕМ аппараттық жабдықтарынан тәуелділігі болады.

Вирусқа қарсы бағдарламаларында вирустардың қандай табу әдістері іске асырылғанына байланысты, олардың келесі түрлерін анықтайды:

– фаг-бағдарламалар (сканерлер);

– тексеруші-бағдарламалар (CRC-сканерлер);

– оқшалау бағдарламалар;

– иммунизатор-бағдарламалар.

Фаг-бағдарламалар вирусты табу үшін сканерлеу әдісін, эвристикалық талдау әдісін және т.б. қолданады. Дегенмен, олар вируспен жұққан файлдарды табып, оларды «емдейді», яғни файлдан вирус-бағдарламасының денесін жояды, файлды негізгі күйге қайтарады. Фаг-бағдарламалары резидентті мониторларға, сканерлеуді «ұшып келе жатқанда» жасайтын, және резидентті емес сканерлерге, жүйенің тексеруін сұрау арқылы қамтамасыз ететін, бөлінеді. Фаг-бағдарламаларының құндылығына олардың әмбебаптығы, кемшіліктеріне – вирустарды іздеу аз жылдамдығы және вирусқа қарсы базаларының үлкен көлемдері жатады. Ең белгілі фаг-бағдарламалары – Scan, Norton Antivirus, Doctor Web, Kaspersky Anti-Virus Scanner.

Тексеруші бағдарламалар (CRC-сканерлер) вирусты табу үшін өзгерістерді табу әдісін қолданады. CRC-сканерлердің жұмыс істеу қағидаты файлдармен жүйелі секторларға CRC-қосындысын (циклдық бақылаудың кодтарын) санауында негізделген. Сол қосындылар, сонымен катар кейбір басқа ақпарат (файлдардың ұзындығы, олардың соңғы түрлендірудің уақыттары және т.б.) вирусқа қарсы бағдарламаның мәліметқорында сақталады. Келесі қосқан кезде CRC-сканерлер нақты түгенделген маңыздарды мәліметқорындағы мәліметтермен салыстырып тексереді. Егерде олар бір біріне келмесе, CRC-сканерлер файл өзгертілген немесе вируспен жұқтырылған тұралы белгі береді. Кейбір CRC-

сканерлерде антистелс алгоритмы салынған. Бірақ олар жаңа файлдарда вирусты таба алмайды, себебі мәліметқорында олар тұралы ақпарат жоқ. CRC-сканерлер санына ADinf бағдарламасы (Advanced Disk in foscope) және AVP Inspector тексеруші жатады.

Оқшалау бағдарламалар резиденттік күзетшілер әдістерін іске асырады. Олар «вирусқауіпті» жағдайды ұстап қалады, бұл тұралы пайдаланушыға хабарлайды және тиісті әрекетке тиым салуға ұсыныс жасайды. Оқшалау бағдарламалардың құндылығына вирустын көбеюін ерте кезеңде табып және оны тоқтату қабілеттілігі жатады. Бірақ олар файлдармен дисктерді «емдемейді».

Өзін-өзі бақылау сұрақтары:

1. Компьютерлік вирус – бұл:
a) өздерін ендіре отырып басқа бағдарламаларды зақымдайтын бағдарлама;
b) оператордың айқын командаларынсыз жасырын көшіріп алу;
c) оператордың командаларының көмегімен көшіріп алу;
d) қатты дискіде файлдарды жою бағдарлаасы;
e) компьютердің жеке компоненттерін физикалық істен шығаратын бағдарлама.

2. Өмір сүру ортасына қарай компьтерлік вирустар бөлінеді –
a) жүктеуші, файлдық, файлдық - жүктеуші, желілік
b) резидентті, компоньон
c) зиянды, зиянсыз
d) резидентті және резидентті емес
e) жүктеме, резидентті, файлдық жүктеме, желілік

3. Жүктеме вирустар –
a) дискінің жүктеме секторына орналасады
b) файлдарды зақымдаушы вирустар
c) зиянды вирустар
d) тұрақты жадыда орналасады
e) дискінің қосымша секторында орналасады

4. Файлдық вирустар –
a) орындаушы файлдарды зақымдаушы вирустар
b) зиянды вирустар
c) дискінің жүктеме секторына орналасады
d) компьютер жадын зақымдаушы вирустар
e) орындаушы файлдарды өшіруші вирустар

5. Вирустар өмір сүру ортасындағы тәсіліне қарай бөлінеді:
a) резидентті және резидентті емес
b) көрінбейтін және макро
c) паразитті және құрт вирустар
d) файлдық және файлдық емес
e) ішкі және кірме

6. Резидентті вирус-
a) вирус тасымалдаушы программа жұмысы тоқтатылғаннан кейін де жедел жадта сақталатын компьютерлік вирус
b) вирус тасымалдаушы программа жұмысы тоқтатылғаннан кейін жедел жадта сақталмайтын компьютерлік вирус
c) өзінің құрылымын өзгертетін компьютерлік вирус
d) орындаушы файлдарды зақымдаушы вирустар
e) жұққан бағдарламада өз кодтарын түрлендіретін вирус

7. Резидентті емес вирус-
a) вирус тасымалдаушы программа жұмысы тоқтатылғаннан кейін жедел жадта сақталмайтын компьютерлік вирус
b) вирус тасымалдаушы программа жұмысы тоқтатылғаннан кейін де жедел жадта сақталатын компьютерлік вирус
c) өзінің құрылымын өзгертетін компьютерлік вирус
d) орындаушы файлдарды зақымдаушы вирустар
e) жұққан бағдарламада өз кодтарын түрлендіретін вирус

8. Полиморфты вирус-
a) өзінің құрылымын өзгертетін компьютерлік вирус
b) вирус тасымалдаушы программа жұмысы тоқтатылғаннан кейін де жедел жадта сақталатын компьютерлік вирус
c) вирус тасымалдаушы программа жұмысы тоқтатылганнан кейін жедел жадта сақталмайтын компьютерлік вирус
d) орындаушы файлдарды зақымдаушы вирустар
e) өзінің құрылымын тұрақты сақтайтын компьютерлік вирус

9. Вирустық бағдарламалар неше топқа бөлінеді:
a) 2
b) 3
c) 4
d) 8
e) 9

10. Нысаналық вируспен шабуыл жасағанда қандай драйверге жұғады?
a) DESCREET
b) DES
c) CVJS
d) FENCE
e) NAT

11. Антивирустың ең маңызды критериі
a) жұмыс істеу сенімділігі
b) жылдам сканерлеу
c) жадыда аз орын алуы
d) компьютерді аз жүктеу
e) түсінікті интерфейс

12. Мекендеу ортасына қарай вирустарды нешеге бөлуге болады?
a) 5
b) 3
c) 2
d) 4
e) 8

13. Логикалық бомбалар-
a) белгілі ақпаратты енгізуде жіберілетін бағдарлама бөлігі
b) екі немесе бірнеше желілер арасында қорғаныс барьерін құрушы жүйелер комбинациясы
c) үш немесе бірнеше желілер арасында қорганыс барьерін құрушы жүйелер комбинациясы
d) шифрланатын мәтіннің бөлігіне қолданылатын түрлендірудің негізгі әдістерінің тізбегі
e) белгілі ақпаратты сақтауда жіберілетін бағдарлама бөлігі

14. Детектор-бағдарламалар:
a) әрбір вируспен сипатталатын «маска» бойынша вирустардың белгілі түрлерін іздеуді жүзеге асырады.
b) пайдаланушылардың әрекеттерін шектеуге арналған;
c) файлдарды өзгерту және жою бойынша операцияларды бақылап отырады;
d) бағдарламаның бақылау санын санап, оны эталондымен салыстырады;
e) үнемі өзгеріп отыратын модульдарды архивациялайды.

15. Операциялық жүйенің жіктеуіші мен қатты дискінің ең басты мәлімет жіктеу (нулевой сектор) жазбасын зақымдайтын вирустар қалай аталады?
a) «жүктегіш» вирустар
b) нольдік вирустар
c) жай вирустар
d) осал вирустар
e) зиянсыз вирустар

6 АҚПАРАТТЫҚ КРИПТОГРАФИЯЛЫҚ ҚОРҒАУ ҚҰРАЛЫ

Абоненттер арасындағы ақпарат алмасудағы қорғау мәселелерін шешумен адамзат өз тарихы бойы айналысады. Адамзатпен берілетін хабарламаның мәнін барынша қарсыластан жасыруға мүмкіндік беретін көптеген амалдар ойлап табылған.

Бірінші тәсіл материалдық ақпарат тасығышты қарсыластан физикалық қорғау болып табылады.

Ақпаратты қорғаудың екінші тәсілі ежелгі уақыттан белгілі – ақпаратты стенографиялық қорғау. Бұл қорғау тәсілі қарсыластан оны ықыластанатын ақпараттың бар фактын жасыру әрекетіне негізделген.

Стенографиялық қорғау әдіс кезінде қарсыластардан мәліметтерді физикалық тасушыны жасырып немесе құпиялы хабарларды ашық құпиялы емес ақпараттың арасында бүркемелейді.

Ақпарат қорғаудың үшінші тәсілі – қазіргі кезде ең таралған және ең кепілді – криптографиялық. Бұл ақпарат қоғау әдісі ақпараттың мәнін қарсыластан жасыру үшін оны түрлендіреді.

Түрлендіру жолымен ақпаратты қорғау мәселелерімен криптология айналысады (kryptos – құпиялы, logos - ғылым).

Криптология бір біріне қарама қарсы екі бағытқа бөлінеді – криптография және криптоталдау.

Криптография ақпаратты түрлендірудің математикалық әдістерін іздеумен зерттеумен айналысады.

Криптоталдау ықыласы аймағы – кілтті білусіз ақпарат шифрын шешу мүмкіндігін зерттеу.

Қазіргі криптография өз ішіне төрт ірі тараудан тұрады:

– симметриялық криптожүйелер;
– ашық кілтті криптожүйелер;
– электронды қолтаңба жүйелері;
– кілттермен басқару.

Криптографиялық әдістерін қолданудың негізгі тараудары – байланыс каналдары бойымен құпиялы ақпаратты жіберу, жіберілетін хабарлардың ақиқаттылығын анықтау, ақпартты шифрланған түрде тасығыштарда сақтау.

Криптологияда қолданылатын негізгі түсініктерді қарастырайық. Бастапқы мәтін бар, оны ашық, шифр және шифрлау кілті деп атайды. Шифр – ақпаратты шифр кілті бойынша шифрлау және шифрын ашу үшін қолданылатын криптографиялық түрлендірулердің ережелері мен әдістері жиынтығы.

Шифр кілті – ақпаратты бөгетсіз шифрлау және шифрын ашу үшін керекті ақпарат.

Шифрлау – ашық мәтін шифрланған мәтінмен (шифрмәтінімен, криптограммамен) ауыстырылатын түрлендіру үдерісі.

Дешифрлау – шифрлауға кері үдерісі – кілтті қолданумен криптограмма бойынша бастапқы мәтінді қалыптастыру.

Шифрлау және дешифрлау операциясын келесі функциялар түрінде жазуға болады.

$$C=E_k(P) \text{ шифрлау}$$
$$P=D_k^*(C) \text{ дешифрлау}$$

C– шифрланған мәтін;
P – ашық мәтін;
*k, k** - шифрлау және дешифрлау кілттері;
E_k - шифрлау функциясы;
D_k^* - дешифрлау функциясы.

Кез-келген ашық мәтін үшін теңдік дұрыс болады

$$D_k^*(E_k(P)) = P.$$

Нағыз кілті жоқ ашық мәтін Р-ны алу үшін С шифрмәтіннің шифрын ашуға деген кез-келген әрекеті криптоталдаулық шабуыл деп аталады. Сәтті шабуыл бұзып ашу немесе ашу деп аталады.

Шифрдың криптошабуылдарға қарсылық қылу қабілеттілігі беріктілік деп аталады. Өмірдегі Кирхгофф пікірі дейтін көзқарас бойынша, шифрдың берiктiлiгi тек кілттің құпиялылығы бойынша анықталады.

Тіпті, шексіз есептеу мүмкіндіктеріне ие криптоталдаушы криптограмма білімінің негізінде де белгісіз криптограмма бағалауымен салыстырғанда, бастапқы мәлімет бағасын жақсарта алмаса, бұндай шифрлар берік болып табылары сөзсіз. Әрине, беріктілік тек қана біркелкі ықтималды кездейсоқ ұзындығы бастапқы мәтінге тең кілтті қолданғанда ғана алынады, сонымен қатар әрбір жаңа мәліметке тең кездейсоқ кілт қолданылады.

Хабарлама ұзындығына тең біркелік ықтималды кілтті қолданатын криптоалгоритмдерді бір рет қолданылатын таспасы бар шифр немесе шексіз кілттік гаммасы бар шифр деп те атайды.

Егер есептеу қорлары бар жағдайындағы ықтималдық оларды әшкерелеу уақытында, ягни көрсеткен ақпарат бағалығы осы ағымда өте аз болса, шифрлар шартты немесе есептеулі берік деп аталады.

Қазіргі шифрлау әдістері келесі талаптарға сай болу керек:

– шифрдың криптоталдауға қарсы тұру қабілеті оның ашуы тек қана барлық мүмкін болатын кілттерді толық іріктеу жолымен ғана жүзеге асатындай болу керек;

– криптоберiктiлiк шифрлау алгоритмнің құпиялығына емес кілттің құпиялығымен қамтамалы болу керек;

– шифрмәтін бастапқы ақпарат көлемінен аса аспау керек;

– шифрлау кезінде пайда болатын қателер ақпараттың бұрмалауына және жоғалуына әкелмеу керек;

– шифрлау уақыты ұзақ болмау керек;

– шифрлаудың бағасы қорғалатын ақпараттың бағасымен үйлесімді болу керек.

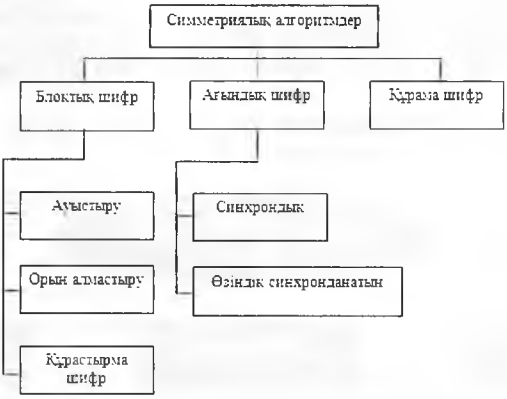
Барлық криптоалгоритмдердің негізгі жіктелу сызбасы 8 суретте көрсетілген.

Сурет 8. Криптоалгоритмдердің жіктелу

6.1 Симметриялық криптоалгоритмдер

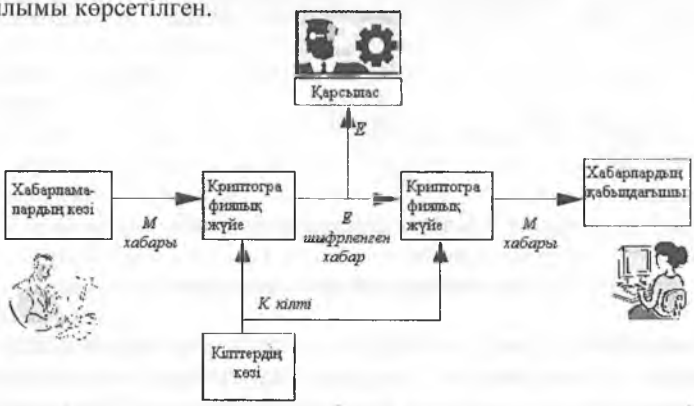
Тарихи бірінші боп симметриялық криптоалгоритмдік жүйелер пайда болды. Симметриялық шифрлау криптожүйесінде аспаратты шифрлау және шифрын ашу үшін бір кілт қолданылады. Яғни шифрлау кілтіне қатынау алған кез келген тұлға хабарламаның шифрын аша алады. Сәйкесінше шифрланған ақпаратты рұқсат етілмеген жасырудың алдын алу үшін симметриялық криптожүйедегі барлық шифрлау кілттері құпияда ұстанлынуы керек. Сондықтан симметриялық криптожүйелерді құпиялы кілті бар криптожүйелер, біркілтті криптографиялық жүйелер немесе жабық кілті бар криптожүйелер деп атайды.

Криптожүйе мәліметтері шифрлаудың жоғары жылдамдығымен сипатталады, және оның көмегімен құпиялылық пен ақиқаттылық, ақпаратты жіберу тұтастылығы қамтамасыз етіледі.



Сурет 9. Симметриялық криптографиялық жүйедегі шифрлау тәсілдерінің классификациясы

10-суретте симметриялық шифрлауды қолданатын құпиялы жүйенің құрылымы көрсетілген.



Сурет 10. Симметриялық шифрлауды қолданатын құпиялы жүйенің жалпы құрылымы

Ағынды шифрлар. Ағынды шифрлауда кодпен жазу бірлігі 1 бит болып табылады, яғни ашық мәтін бит бойынша өңдейді. Бастапқы ақпараттың әр биті басқалардан тәуелсіз гаммалау көмегімен шифрланады.

Гаммалау деген – ашық хабарламаға белгілі әдіспен шифр гаммасын беттестіру, ол дегеніміз кездейсоқ немесе жалған кедейсоқ кезекпен 1 және 0.

Әдетте XOR логикалық операциясы қолданылады (НЕМЕСЕ-ні қоспайды). Дешифрлау үшін сол гамма шифрланған мәтінге беттестіріледі.

Кесте 2 – XOR логикалық операциясының сызбасы

x	y	*x* XOR *y*
0	0	0
0	1	1
1	0	1
1	1	0

Кесте 3 – Гаммалау көмегімен шифрлаудың мысалы

	Операция	Нәтиже
Бастапқы мәтін		10010
Гамма	XOR	01011
Шифрмәтін	=	11001
Гамма	XOR	01011
Бастапқы мәтін	=	10010

Бұл сызба ақпарат ағымдарын беру жүйелерінде қолданылады. Ол дегеніміз, хабарламаны блоктарға бөлуге мүмкіндік жоқ кездер, сонымен қатар ақпараттың берілісі кез келген уақытта басталып және аяқталуы және кездейсоқ үзілуі мүмкін болатын кездер.

Блокты шифрлар. Кодтау бірлігі бірнеше биттен тұратын блок болып табылады. Ақпарат алдын ала ұзындығын тіркелген блоктарға бөлінеді. Блоктар бір бірінен тәуелсіз, сонымен қатар «ілініспен» шифрлана алады, яғни ағымдағы мәліметтер блогын шифрлау нәтижесі алдындағы блок мәнінен немесе алдындағы блокты шифрлаудың нәтижесінен тәуелді болады.

Блокты шифрлар келесі типтерге бөлінеді:

– Орын ауыстыру шифрлары;

– Алмастыру шифрлары:

а) моноалфавитті, мұнда бастапқы мәтіннің символы алдын ала белгіленген символмен алмастырылады;

б) көпалфавитті, мұнда бастапқы мәтіннің символы әр уақытта белгілі бір мәліметтер жиынтығынан алынған әр түрлі символдармен алмастырылады;

– Құрылымды, орын ауыстыру мен алмастыру әдістерінің үйлесімін білдіреді:

а) DES – Data Encryption Standard (АҚШ);

б) Lucifer (АҚШ);

в) FEAL – Fast Enciphering Algorithm (Жапония);

г) IDEA (Швейцария);

д) МЕМСТ 28147-89 (Ресей);

е) AES – Advanced Encryption Standard (АҚШ).

Тұрақты блоктық шифрын шифрлау функциясына келесі шарттар қойылады:

– функция қайтымды болуы керек;

– криптограмма бойынша бастапқы хатты оқудың, кілттерді толық іріктеу әдісінен басқа әдістер («дөрекі күш» әдісі) болмау керек;

– қай кілтпен түрлену жүргізілгендігін анықтау, кілттерді толық іріктеу әдісінен басқа әдістер болмау керек.

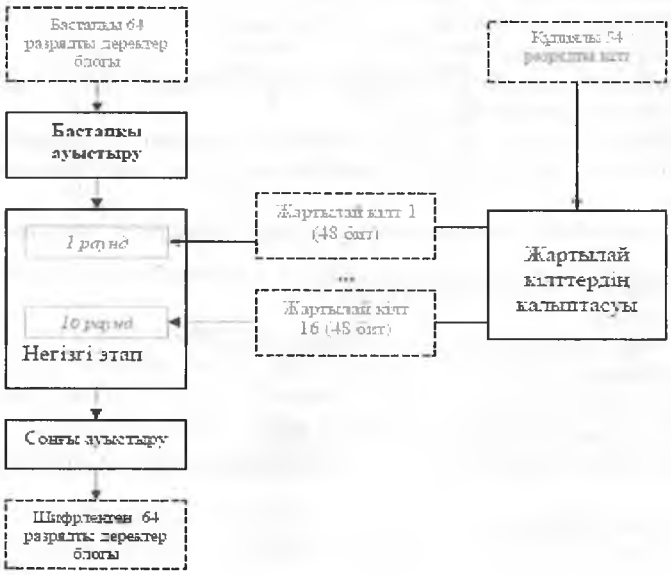
Орын ауыстыру әдістерінде бастапқы мәтіннің символдары орнын белгілі бір ереже бойынша ауыстырады. Алмастыру (немесе орнына қою) әдістерінде ашық мәтін символдары шифрланған мәтіннің кейбір эквиваленттерімен алмастырылады. Мәтінді шифрлау беріктілігін жоғарлату мақсатымен бір әдіс көмегімен шифрланған мәтін екінші әдіс көмегімен тағы шифрлана алады. Бұл жағдайда үйлесімді немесе композициялық шифр пайда болады.

Бүгінгі күнде іс жүзінде қолданылатын блоктық және ағынды симметриялық шифрлар үйлесімді шифрларға да жатады, себебі оларда хабарламаны шифрлау үшін бірнеше операциялар қолданылады.

Алмастыру шифрлау әдісі (орнына қою) блоктарға бөлінген және бір алфавитте жазылған бастапқы мәтін символдары қабылданған түрлендіру ережелеріне сай басқа алвафиттің бір немесе бірнеше символдарымен алмастырылатынына негізделеді.

DES шифрлау алгоритмі (Data Encryption Standard) 1994 жылы жарық көрген және коомерциялық ақпаратты қорғау жүйелерінде қолданылатын ең таралған блоктық алгоритм болып табылады.

DES алгоритмі орын ауыстыру мен орнына қою алмасатын тізбегінен тұрады. Алгоритм 64-битті мәліметтер блоктарын 56-битті К кілті көмегімен шифрлауды жүзеге асырады (11-сурет).



Сурет 11. DES жалпы сызбасы

64-битті бастапқы мәліметтер блогын шифрлау үдерісін үш кезеңге бөлуге болады:

1. мәліметтер блогын бастапқы дайындау;
2. «негізгі циклдің» 16 раунды;
3. мәліметтер блогын түпкі өңдеу.

Бірінші кезеңде 64-битті бастапқы мәтін блогының бастапқы орын ауыстыруы жүзеге асырылады, бұл кезде биттер белгілі ретпен реттеледі.

Келесі (негізгі) кезеңде блок 32 битті екі бөлікке (тармаққа) бөледі. Оң тармағы белгілі бір F функциясы мен шифрлаудың арнайы кілттерді түрлендіру алгоритміндегі негізгі кілттен алынатын сәйкес жартылай кілт көмегімен түрленеді. Одан кейін оң және сол тармақтардың арасында мәліметтер алмасуы жүзеге асады. Бұл циклде 16 рет қайталанады.

Үшінші кезеңде негізігі циклдың он алты қадамында алынған нәтиженің орнын алмастыруы жүзеге асырылады. Бұл орын ауыстыру бастапқы ауыстыруына кері болып табылады.

Ресейлік мәліметтерді шифрлау стандарты МЕМСТ 28147-89 1999 жылы мәліметтерді шифрлау мемлекеттік стандарты ретінде қолдану үшін жасалған. МЕМСТ алгоритмінің блок-сызбасы DES алгоритмдерінің блок-сызбаларынан бастапқы және соңғы орын ауыстыруының жоқтығымен және шифрлау айналымы санымен (32 қарсы 16) ерекшеленеді. Берілген шифрда 256-битті кілт қолданылды. Оның кемшілігі – бұл бағдарламалық жүзеге асуының күрделілігі мен жұмысын жылдамдығының жоғарылығының жеткіліксіздігі. Бірақ ресейлік стандарт үлкен қормен жобаланды, тұрақтылығы бойынша ол DES алгоритмін бірнеше тәртіптерінен асып түседі.

МЕМСТ 28147-89 мәліметтерді түрлендіруді криптографиялық алгоритмнің негізгі параметрлері келесі: блок өлшемі 64 бит, кілт өлшемі – 256 бит, раунд саны – 32.

Шифрланатын мәліметтер блогы екі бірдей бөлікке бөлінеді,оң R және сол L. Оң бөлігі раунд ішкі кілтімен қалыптасады және қайсібір алгоритмнің көмегімен сол бөлігін шифрланады. Келесі раунд алдында оң және сол бөліктері орындарымен ауысады. Осындай құрылым блокты шифрлау және дешифрлау үшін бір алгоритмді қолдануға мүмкінік береді.

Шифрлау алгоритмдерінде келесі оперциялар қолданады:

1. 2^{32} модулі бойынша сөздерді қосу;
2. нұсқалған биттер санына сөздердің солға айналмалы жылжуы;
3. 2 модулі бойынша бит бойынша қосу;
4. кесте бойынша алмастыру.

AES шифрлау стандарты – 2000 жылдан бастап АҚШ тағы мәліметтерді шифрлаудың жаңа стандарты. Берілген алгоритм өңделетін әр блокты орнатылған блок ұзындығына байланысты 4х4, 4х6 немесе 4х8 өлшемді екі өлшемді байтты массив ретінде ұсынады. Келесіде сәйкес

кезеңдерде не тәуелсіз бағаналарға, не тәуелсіз жолдарға, немесе жеке байттарға түрлендіру жүргізіледі. Алгоритм белгілі раундтар санынан құрылады (10 нан 14 дейін) және төрт түрлендіруді жүзеге асыралы:

- BS (Byte Sub) – массивтің әр байтын кестелік алмастыруы;
- SR (Shift Row) – массив жолдарын жылжыту;
- MC (Mix Column) – бағаналарды тәуелсіз матрицаға көбейту;
- AK (Add Round Key) – кілтті қосу (2 модулі бойынша қосу).

AES алгоритмі артықшылықтар қатарының арқасында шифрлаудың жаңа стандарты болды – шифрлаудың жоғары жылдамдығы мен ресурстарға деген минималды талаптар.

6.2 Асимметриялық криптоалгоритмдер

Симметриялық криптожүйелер қандай күрделі және сенімді болғанымен олардың іс жүзіндегі жүзеге асудағы әлсіз орны – кілттерді үлестіру мәселесі. Оларды шешу үшін алгебралық нәтижелер негізінде асимметриялық криптожүйелер ұсынылды. Мұнда хабарларды шифрлау үшін барлығына мәлім бір (ашық) кілт, ал дешифрлау үшін алушыға ғана мәлім басқа (жабық) кілт қолданылады.

Дректермен алмасу сұлбасы осындай: алушы ашық және құпиялы кілттерді есептейді. Құпиялы кілтті жасырып сақтайды, ашық кілтті жіберушіге қолжетімді етеді. Жіберуші алушының ашық кілтін қолданып, хабарды алушыға шифрлап жібереді. Алушы өзінің құппиялы кілтін қолданып хабарламаның шифрын шешеді.

Сонымен қатар асимметриялық жүйелерді екі кілтті криптожүйелері немесе ашық кілтті криптожүйелері деп атайды.

Мысалы, бір біріне электрондық хаттарды жіберу мүмкіндігі бар А және Б пайдаланушылары ашық шифрлау сұлбасын қолдансын. А пайдаланушысы Б пайдаланушысына басқа ешкім оқи алмайтындай етіп құпиялы хат жіберсін. Ол үшін келесі әрекеттерді жүзеге асыру керек:

1. Б пайдаланушысы А пайдаланушысына кез келген байланыс каналы арқылы, мысалы, электронды поштамен, өз U ашық кілтін жібереді.

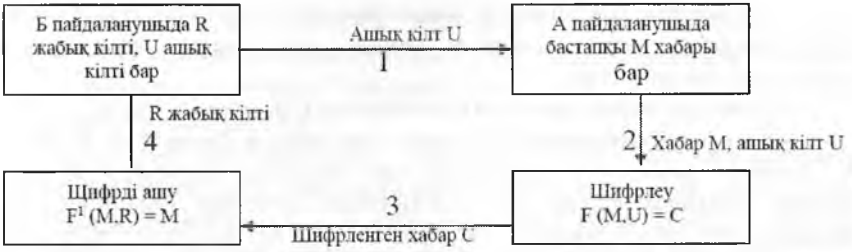
2. А пайдаланушысы өзінің М хатын алынған U кілті көмегімен шифрлап, шифрланған С хатын алады.

3. Шифрланған С хаты

4. Б пайдаланушысына жіберіледі.

5. Б пайдаланушысы алынған С хатының өзінің R құпиялы кілтімен шифрын ашады.

Егер шифрлау операциясын F деп, ал дешифрлау операциясын F-1 деп белгілесек, пайдаланушылар арасындағы ақпарат алмасу хаттамасының сұлбасын 12-суретте көрсетілгендей бейнелеуге болады.



Сурет 12. Ашық шифрлау сызбасы

Асимметриялық криптожүйелердің концепциясы бір бағытталған функцияларды қолдануға негізделген. Бұл функциялар келесі қасиетті иеленеді: *x* аргументінің берілген мәнінде *F(x)* функциясың мәнін есептеп шығу салыстырмалы жеңіл болады, бірақ егер тек *F(x)* мәні белгілі болса, *x* аргументін есептеудің жеңіл жолы жоқ.

Есептеуі жеңіл, бірақ айналдыру күрделі болатын функцияларды бір бағытталған функцияларға жатқызады, мысалы бүтін санды көбейту.

Бірбағытталған функцияларды біржақты немесе қайтымсыз функциялар деп те атайды.

Бірбағытталған функциялардың ерекше түрі болып табылатын өтетін түтікшесі бар бір бағыттаған функциялар. Яғни берілген *x*-те *F(x)* табу жеңіл, және керісінше – тек *F(x)* мәнін біліп *x* табу қиын. Бірақ у құпиялы ақпараты бар, егер, у пен *F(x)* белгілі болса *x* есептеу жеңілдірек болады.

Симметриялық крипторафиялық жүйелер жағдайындағы сияқты, симметриялық емес криптожүйелердің көмегімен құпиялық ғана емес, сонымен қатар жіберілетін ақпараттың тұтастлығы мен ақиқаттылығы қамтамасыз етіледі. Симметриялық криптожүйелердің алдында асимметриялық криптожүйелердің артықшылығы:

- пайдаланушылар арасындағы кілттерді үйлестіру күрделі мәселесі шешілді, себебі әр пайдаланушы өз кілт жұбын өндіре алады, ал пайдаланушылардың ашық кілттері еркін жариялана алады және желілік коммуникациялар бойымен тарай алады;
- кілтердің санының пайдаланушылар санынан квадраттық тәуелдігі жоғалады; асимметриялық криптожүйеде қолданылатын кілттер саны абоненттер санымен сызықты байланысады (жүйеде N пайдаланушыдардан 2N кілттер қолданылады);
- асимметриялық криптожүйелер жабық кілт тек өзінің иесіне мәлім болу керектігі себебінен, бір біріне сенбейтін жақтардың әрекеттрінің хаттамасын жүзеге асыруға мүмкіндік береді.

Асимметриялық криптожүйелердің кемшіліктері:

- бүгінгі таңда қолданылатын функцияның асимметриялық алгоритмінің қайтымсыздығының математикалық дәлелдемесі жоқ;

- асимметриялық шифрлау симметриялыққа қарағанда едәуір баяу, себебі шифрлау мен дешифрлау кезінде ресурстарды талап ететін операциялар қолданылады;

- ашық кілттердің орнынан ауыстырудан қорғау қажеттілігі.

RSA криптоалгоритімін 1978 жылы үш автор Р. Райвест, А. Шамир, А. Адлеман ұсынды. Алгоритмнің атын авторлар тектерінің бірінші әріптері бойынша қойды. Ол мәліметтерді шифрлау режимінде де, цифрлық қол қою режимінде де жұмыс істей алатын ашық кілті бар бірінші алгоритм болды.

RSA алгоритмінің сенімділігі үлкен сандардың факторизациясы ның қиындығына және түпкі есепте дискретті логарифмдерді есептеу қиындығына негізделеді.

RSA алгоритімінде кілттерді құру кезеңі келесі әрекеттерді көздейді:

1. Дәрежелігі бірдей екі үлкен сан таңдалады: p және q. $p = 3$, $q = 11$.
2. n = p*q көбейту есептеледі. n = 33.
3. Эйлер функциясы есептеледі (φ(n) = (p-1)(q - 1) = 20.
4. ЕҮОБ ең үлкен ортақ бөлгіш ((d, φ (n)) = 1. d = 3.) болатындай, кездейсоқ сан генерацияланады d < n.
5. (e*d) mod φ(n) = 1. (e*3) mod 20 = 1. e =7 болатындай e санын таңдаймыз.

Осылайша, *{e,n}* үйлесімі ашық кілт ретінде қолданып, пайдаланушыларға мәліметтенеді, ал *{d, n}*жабық кілт ретінде қолданып, жасырын сақталады. {7, 33 } – ашық кілт,{3, 33} – жабық кілт.

RSA алгоритмі көмегімен *хабарларды шифрлау* келесіні көздейді:

1. Жіберуші шифрланатын хабарламаны m_i бүтін сандар тізбегі ретінде ұсынады. Мысалы, алфавит әріптеріне сәйкес реттік нөмірлерін қояды. А Б В хабарламамасы = {1, 2, 3}.
2. Мұндай әр сан үшін $c_i = m_i^e \bmod n$ өрнегі есептеледі. C_i блоктары – шифрланған мәтін.

$c_1 = 1^7 \bmod 33 = 1$,

$c_2 = 2^7 \bmod 33 = 29$,

$c_3 = 3^7 \bmod 33 = 9$. Шифрланған мәтін {1, 29, 9}.

Хабарламалардың шифрын шешу үшін құпиялы кілт көмегімен ұқсас түрлендіруер жүргізу керек, нақтырақ айтқанда $m_i' = c_i^d \bmod n$ есептеу.

$m_1 = 1^3 \bmod 33 = 1$,

$m_2 = 29^3 \bmod 33 = 2$,

$m_3 = 9^3 \bmod 33 = 3$. Шифры ашылған мәтін {1,2,3}.

RSA криптоалгоритмі жан жақтан зерттеліп, кілттің жеткілікті ұзындығында тұрақты деп мойындалған. Бүгінгі күні кілт ұзындығы – 1024 бит – қолайлы нұсқа ретінде саналады. Кейбір авторлардың ойынша

процессорлардың қуаты өсумен RSA криптоалгоритмі толық іріктеу шабуылына тұрақтылығын жоғалтады. Бірақ процессорлардың қуатының өсуі ұзынырақ кілттерді қолдануға мүмкіндік береді, бұл RSA тұрақтылығын жоғарлатады.

El Gamal криптоалгоритмі жай санды модулі бойынша дәрежеге шығару негізіндегі сұлбаны қолданады. Ол үшін қарапайым үлкен *p* саны беріледі. Хабарламалар (1, *p)* интервалындағы бүтін сандар *C* ретінде ұсынылады. *C* хабарламасын жіберудің түпнұсқа хаттамасының түрі:

Хабарлама жіберуші *A* мен алушы *B* тек *p* біледі. *A* (1, *p)* интервалынан *X* кездейсоқ санын генерациялайды. *B* сол интервалдан *Y* кездейсоқ санын генерациялайды.

A $Ш_A = C^X \bmod p$ криптограммасын құрып хабарламаны шифрлайды да *B* пайдаланушысына жібереді.

B оны $Ш_в = (Ш_A)^Y \bmod p$ өз кілтімен шифрлап $Ш_в$-ны А абонентіне жібереді.

A $ШАА = (Ш_в)^{-X} \bmod p$ өз кілтін шешіп, хабарламаны *B* абонентіне қайтарады.

B алушы хаттың шифрын ашады $C = (Ш_{AA})^{-Y} \bmod p$.

ElGamal криптожүйесі RSA алгоритміне қарағанда, қамтамасыз ететін қорғау деңгейі жоғарырақ болады. Бұл нәтиже дәл сол *N* кезінде болады, бұл өз кезегінде шифрлау және шифр шешу жылдамдығын жоғарлатуға мүмкіндік береді. ElGamal жүйесінің криптотұрақтылығы бүтін санның дәрежесін есептеу оңай, бірақ басқа берілген санды алу үшін берілген санды шығару керек дәреженің көрсеткішін табу қиын деп негізделген.

Екі кілтті жүйелердің артықшылығы, криптотүрлендірулердің өте төмен жылдамдығы болмаса: олар біркілтті жүйелерге қарағанда бірнеше ретке төмен жұмыс істейді, құпиялы кілтті криптожүйелердің жүйелік қолданбалардың көбінен толық ығыстырып кетуші еді. Бұл кемшілік ұзын шифрланатын хабарламаға қарағанда аса елеулі.

Өзін-өзі бақылау сұрақтары:

1. Криптология -
a) акпаратты оны түрлендіру арқылы корғаумен шұғылданады
b) ақпаратты шифрлау арқылы түрлендіреді
c) ақпаратты сақтау жолдарын қарастырады
d) ақпаратты бүлдіруден сақтайды
e) акпаратты қорғау туралы ғылым

2. Криптография-
a) ақпаратты заңсыз пайдаланушылардан қорғау мақсатымен оны түрлендіру әдістері жайындағы ғылым
b) ақпаратты оны түрлендіру арқылы қорғаумен шұғылданады
c) ақпаратты шифрлау арқылы түрлендіреді
d) ақпаратты қорғау жолдарын зерттейтін ғылым
e) ақпаратты заңсыз пайдаланушылардан қорғау мақсатымен оны жою әдістері жайындағы ғылым

3. Криптоанализ -
a) ақпаратты оның кілтін білмей-ақ кері шифрлау мәселесімен айналысады
b) ақпаратты заңсыз пайдаланушылардан қорғау мақсатымен оны түрлендіру әдістері жайындағы ғылым
c) ақпаратты шифрлау арқылы түрлендіреді
d) шифрланған ақпаратты түрлендіреді
e) ақпаратты тек кілттің көмегімен кері шифрлау мәселесімен айналысады

4. Криптожүйе дегеніміз -
a) алуан түрлі кіттердің, ашық және шифрланған мәтіндердің жиынтығы
b) ақпаратты оның кілтін білмей-ақ кері шифрлау
c) ақпаратты түрлендіру тәсілдерінің жиынтығы
d) ақпаратты шифрлау арқылы түрлендіру
e) ақпаратты қорғау жолдарын зерттейтін ғылым

5. Кілт –
a) ақпаратты шифрлау және кері шифрлау, сондай-ақ, оған қол қою үшін арналған цифрлық кода
b) кілтті белгісіз жағдайда шифрдың кері шифрлауға беріктігін анықтайды
c) ашық ақпаратты бастапқы қалпына келтіре алмайтындай етіп тұрлендіру үшін қолданылатын шартты белгілер тізбегі
d) шифрланған ақпаратты шешу үшін қолданылатын цифрлар тізбегі
e) ақпаратты шифрлау және кері шифрлау, сондай-ақ, оған қол қою үшін арналған сандар тізбегі

6. Шифр -
a) ашық ақпаратты бастапқы қалпына келтіре алмайтындай етіп тұрлендіру үшін қолданылатын шартты белгілер тізбегі
b) кілті белгісіз жағдайда шифрдың кері шифрлауға беріктігін анықтайды

c) ақпаратты шифрлау және кері шифрлау, сондай-ақ, оған қол қою үшін арналған цифрлық кода
d) ашық ақпаратты символдармен түрлендіру үшін қолданылатын шартты белгілер тізбегі
e) кілті белгілі жағдайда шифрдың кері шифрлауға беріктігін анықтайды

7. Шифрлау дегеніміз –
a) белгілі-бір адамнан басқалар оқи алмайтындай етіліп ақпаратты математикалық, алгоритмдік түрлендіру әдісі
b) ақпаратты оның кілтін білмей-ақ қалайша кері шифрлау әдісі
c) ақпаратты шифрлау арқылы түрлендіру әдісі
d) ақпаратты әртүрлі әдістерді пайдаланып түрлендіру
e) белгілі-бір адамнан басқалар оқи алмайтындай етіліп ақпаратты математикалық, алгоритмдік, физикалық түрлендіру әдісі

8. Шифрлау түрлері:
a) симметриялық және асимметриялық
b) активті және пассивті
c) байланысты және байланысты емес
d) оң және теріс
e) негізгі және резидентті

9. Симметриялық криптожүйеде шифрлау және кері шифрлау үшін неше кілт пайдаланылады:
a) 1
b) 2
c) 3
d) 4
e) 5

10. Симметриялық криптожүйелерде қолданылатын криптографиялық әдістерді келесі топтарға бөлуге болады:
a) жай ауыстыру, орын ауыстыру, гаммалау және блоктық шифрлар
b) жай ауыстыру, орын ауыстыру
c) гаммалау және блоктық шифрлар
d) кестелік, блоктік, орын ауыстыру
e) жай ауыстыру, аралас орын ауыстыру, гаммалау және блоктық шифрлар

11. Әліпби дегеніміз –

a) ақпаратты кодтау үшін пайдаланылатын таңбалардың шектеулі жиынтығы
b) ақпаратты шифрлау үшін қолданылатын сандар жиынтығы
c) ақпаратты кодтау үшін қолданылатын символ дар жиынтығы
d) ақпаратты шифрлау үшін қолданылатын әріптер жиынтығы
e) ақпаратты кодтау үшін пайдаланылатын таңбалардың қосындысы

12. Мәліметтерді стандартты шифрлеудің «Des» операторы қай жылы АҚШ-тың ұлттық стандарттар бюросымен қабылданды?
a) 1975 жылы
b) 1977 жылы
c) 1979 жылы
d) 1981 жылы
e) 1983жыл

13. Мәліметтерді стандартты шифрлау операторы төмендегілердің қайсысы?
a) Des
b) It
c) Ct
d) Pt
e) Dec

14. DES стандарты-
a) 1977 жылы АҚШ-тың Ұлттық стандарттар бюросында жарияланды
b) АҚШ-та 1992 жылғы қауіпсіз хэштеу стандарты құрамында жасалған
c) мәліметтерді шифрлау және ЭЦҚ режімінде жұмыс жасайды
d) шифрлау үшін де, цифрлық қолтаңба қою үшін де пайдаланылады
e) ұзындығы 60 бит болатын бір ғана кілт пайдаланады

15. DES алгоритмінде-
a) ұзындығы 56 бит болатын бір ғана кілт пайдаланылады
b) ұзындығы 58 бит болатын екі ғана кілт пайдаланылады
c) ұзындығы 50 бит болатын бір ғана кілт пайдаланылады
d) ұзындығы 60 бит болатын үш кілт пайдаланылады
e) ұзындығы 56 бит болатын екі кілт пайдаланылады

7 ЦИФРЛЫҚ ҚОЛТАҢБА ТЕХНОЛОГИЯСЫ

7.1 Цифрлық қолтаңбалардың негізгі түсініктері

Электронды цифрлық қолтаңба (ЭЦҚ) телекоммуникациялық каналдар бойымен жіберілетін мәтіндерді аутентификациялау үшін пайдаланылады. Мұндай алмасу кезінде құжаттарды өңдеу мен сақтауға деген шығындар елеулі азайып, оларды іздеу тезделеді. Бірақ электронды құжат авторын аутентификациялау мәселесі, яғни автордың шын өзі екенін анықтау және алынған электрондық құжаттағы өзгерістердің жоқтығы туындайды.

Электронды құжаттарды аутентификациялау мақсаты оларды түрлі зиянды әрекеттерден қорғау. Мұндай әрекеттерге жатады:

– белсенді қағып алу – бұзушы, желіге қосылып алып, пайдаланушылардың арасындағы хабарламаны қағып алады да, оларды өзгертеді;

– бүркемелеу - С абоненті А абонентінің атынан В-ға хабарлама жібереді;

– ренегаттық – А абоненті В абонентіне хабарламаны жібермегенін мәлімдейді, бірақ шындығында жіберген;

– ауыстыру – В абоненті хабарламаны өзгертіп, жаңа хабарлама жасайды да, оған А абоненті жіберді деп хабарлайды;

– қайталау –А абоненті В–ға бұрын жіберген хабарламаны С абоненті қайталайды.

Мұндай зиянды әрекеттердің түрлері өз қызметінде ақпараттық технологияларды қолданатын банк және коммерциялық құрылымдарға, мемлекеттік кәсіпорын мен ұйымдарға, жеке тұлғаларға зиян келтіреді.

Хабар тұтастығы мен хабарлама авторын растау мәселесі электронды цифрлық қолтаңба әдістемесін тиімді шешуге мүмкіндік береді.

Цифрлық қолтаңба функционалдығы бойынша қарапайым қолтаңбаға ұқсас және оның негізгі артықшылықтарына ие:

– осы тұлғаға қол қойылған мәтінге байланысты міндеттемелерден бас тартуға мүмкіндік бермейді;

– қол қойылған мәтіннің тұтастылығын кепілдейді;

– қол қойылған мәтін қолтаңба қойған тұлғадан екендігін растайды.

Электронды цифрлық қолтаңба қол қойылатын мәтінмен қоса жіберілетін қосымша цифрлық шағын ақпарат мөлшері болып табылады.

Электронды цифрлық қолтаңба асимметриялық шифрлаудың қайтымсыздығына, сонымен қатар хабар құрамы, қолтаңбаның өзі және кілт жұбының өзара байланысына негізделеді. Осы элементтердің біреуінің өзгеруі цифрлық қолтаңба түпнұсқалығын растауды мүмкін емес етеді. ЭЦҚ асимметриялық шифрлау алгоритмдері мен хэш-функцияларының көмегімен жүзеге асады.

Цифрлық қолтаңба жүйесін қолдану технологиясы бір біріне қол қойылған электронды хабарламарды жіберіп отырған абоненттер желісінің бар болуын көздейді. Әр абонент үшін кілт жұбы генерацияланады: құпия және ашық кілт. Құпия кілті абонентпен құпияда сақталынады да, ЭЦҚ құру үшін қолданылады. Ашық кілт басқа пайдаланушыға мәлім және қол қойылған электронды құжатты тексеру үшін арналған.

Алайда, ЭЦҚ – жіберілетін хабарламамен байланысқан және қолтаңба иесі осы хабарламаға сенімін дәлеледейтін мәліметтер. Сондай-ақ хабарламаны алушы қолтаңба иесі осы хабарламаның авторы екенін және жіберу барысында мәліметтердің өзгермегендігін тексере алады. Жалпы жағдайда ЭЦҚ деп қол қойылған құпия кілтті пайдалана отырып, хабарлама бойынша есептелетін сандық мәндер түсіндіріледі. ЭЦҚ-ны тексеру ашық кілт негізіндегі жалпыға ортақ процедура арқылы жүзеге асырылады.

ЭЦҚ жүйесі екі негізгі процедуралардан тұрады:

– цифрлық қолтаңбаны құру процедурасы;

– цифрлық қолтаңбаны тексеру процедурасы.

Берілген процедуралардың жүзеге асуын *қолтаңбаның классикалық сызбасында* қарастырайық.

Цифрлық қолтаңба құру процедурасы. Бұл іс процедураның дайындық кезеңінде *A* абоненті - хабарлама жіберушісі - кілт жұбын генерациялайды: k_A құпия кілті мен K_A ашық кілті. Ашық кілт басқа желі абоненттеріне қолтаңбаны тексеру үшін жіберіледі (13-сурет).

Сурет 13. Электронды цифрлық қолтаңбаны құру сызбасы

Цифрлық қолтаңба құру үшін *A* жіберушісі ең алдымен *M* қол қойылатын мәтіннің *h(M)* хэш-функциясының мәнін есептеу керек (сурет 7.1). Хэш-функция бастапқы қол қойылатын *M* мәтінін *m* дайджестке қысу үшін қызмет етеді. *m*- биттердің белгіленген шағын санынан құралатын және *M* мәтінін толығымен сипаттайтын салыстырмалы қысқа сан. Хэш-функция ретінде берілген мәліметтер бөлігін математикалық немесе алгоритмдік жаңарту саналады. Ол келесі қасиеттерге ие болады: анықтау аймағы шексіз, мәндердің соңғы аймағы бар, қайтымсыз, ақпараттың кіріс

ағымын бір битке өзгеркенде шығыс ағымының барлық битінің жартысындай өзгертеді.

Ары қарай A абоненті m дайджестін өзінің k_A құпия кілтімен шифрлайды. Шыққан сан жұбы осы M мәтінінің цифрлық қолтаңбасы болып табылады. Цифрлық қолтаңбамен қоса M хабарламасы алушы адресіне жіберіледі.

Цифрлық қолтаңбаны тексеру процедурасы. ЭЦҚ тексеру кезінде B абоненті – M хабарламасын алушы – алынған m дайджестін A жіберушісінің ашық K_A кілтімен дешифрлайды. Одан басқа алушының өзі алынған M хабарламасының m' дайджестін $h(M)$ хэш-функциясы көмегімен есептеп, дешифрмен салыстырады. Егер m мени m' бір біріне сәйкес келсе, цифрлық қолтаңба шынайы болып келеді. Басқа жағдайда қолтаңба немесе жалған жасалынған, немесе хабарлама құрамы өзгертілген.

ЭЦҚ жүйесіндегі маңызды жағдай пайдаланушы құпия кілтті білмей ЭЦҚ жалған жасай алмайтыны болып табылады. Сондықтан құпия кілтті рұқсатсыз енуден қорғау қажет.

Цифрлық қолтаңба құру кезінде жіберушінің жабық кілті, ал шифрлау кезінде алушының ашық кілті қолданылады. Цифрлық қолтаңбаны тексеру кезінде жіберушінің ашық кілті, ал дешифрлау кезінде алушының жабық кілті қолданылады (14-сурет).

Сурет 14. Электронды цифрлық қолтаңбаны тексеру сызбасы

Қалыптасқан қолтаңбаны кез келген тұлға тексере алады, себебі тексеру кілті ашық болып табылады. Қолтаңбаны тексерудің оң нәтижесінде алынған хабарламаның тұтастылығы мен шынайылығы туралы қорытынды, яғни хабарламаның шынымен сол жіберушімен жіберіліп, желіде жіберілу кезінде модификацияланбауы туралы қорытынды жасалынады. Егер пайдаланушы алынған хаттың бұрын жіберілген хаттың қайталамасы емес екеніне немесе жүру жолында ұсталынып қалмағанына көз жеткізгісі келсе, осы хаттың уақыт белгісінде жіберілу уақыты мен күнін тексеру керек.

Асимметриялық шифрлеуге ұқсас ЭЦҚ тексеру үшін қолданылатын ашық кілтті алмастыру мүмкін еместігін қамтамасыз ету керек.

RSA алгоритмі негізіндегі қолтаңба үлгісі:

M хабарламасына қолтаңба жасау үшін жіберуші:

1. Сығылған бейнені $R = H(M)$ есептейді (дайджест хабарламасы, хэш-бейне) хэш-функциясының *H* көмегімен.

2. Алынған сығылған бейнені өзінің құпиялы кілтінде шифрлайды және қолтаңба $S = R^d \bmod n$ алады, мұндағы $\{d, n\}$ – жіберушінің жабық кілті.

Қолтаңбаны тексеру үшін алушы:

1. Жіберушінің ашық кілтімен S қолтаңбаның шифрін ашады, яғни R' = Se mod n есептейді, мұндағы {e, n} – жіберушінің ашық кілті.

2. Жіберуші қолданған сол бір H хэш-функцияны қолдана алынған хабарламаның сығылған бейнесін R = H(M) есептейді.

3. Алынған R және R' мәндерді салыстырады, егер олар сәйкес келсе, онда қолтаңба дұрыс.

Сонымен, *ЭЦҚ* – электронды мәліметтердің дұрыстығын, мазмұнының өзгермегендігін және оның тәуелділігін растайтын электронды цифрлы символдар жиынтығы.

ЭЦҚ жабық кілті– ЭЦҚ жасауға арналған және қолтаңба иесіне белгілі электронды цифрлы символдардың реті.

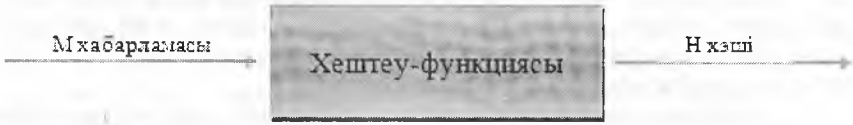
ЭЦҚ ашық кілті– кез-келген тұлғаға белгілі және электронды құжаттардағы ЭЦҚ растауға арналған электронды цифрлы символдардың реті.

ЭЦҚ қол қоятын тұлғаның өз қолымен койған қолтаңбасына тең мағыналы және бірдей заң зардаптарына әкеп соғады. ЭЦҚ жабық кілттері оларды заңды негізде иеленетін тұлғалардың меншігі болып табылады. Қол қоятын тұлға ЭЦҚ қолдануға өкілеттігін өзінің өкіліне тапсыруға құқылы. Алғаш рет цифрлық қолтаңбаны электронды құжаттың авторлығын заңды растау құралы ретінде қолдану идеясы 1976 жылы Диффи және Хеллман жұмыстарында жарық көрді.

7.2 Хэштеу функциясы

ЭЦҚ есептеу үшін бастапқы мән ретінде электронды құжаттың өзі емес, оның хэш-мәні немесе дайджест алынады.

Хэш-мәні *h(M)* – бұл *M* хабарламасының дайджесті, негізгі *M* хабарламасының кез келген ұзындықтағы сығылған екілік көрінісі. *h(M)* хэш-мәні хэштеу функциясымен құрылады. Хэштеу функциясы (хэш-функциясы) кіруіне *M* айнымалы ұзындықтағы хабарлама беріліп, шығуы *H=h(M)* белгіленген ұзындықтағы жолақ болатын түрлендіру болып табылады.



Сурет 15. Хэштеу функциясы

Хэштеу функциясы қол қойылатын *M* құжатын 128 және одан да көп битке (сәйкесінше 128 немесе 256 битке дейін) қысуға мүмкіндік береді, ал *M* құжаты көлемі мегабайт немесе одан да көп бола алады. *h(M)* хэш-функциясы *M* құжатына күрделі тәуелді және *M* құжатының өзін қалпына келтіруге мүмкіндік бермейді.

Хэштеу функциясы келесі қасиеттерге ие:

– хэш-функциясы кез келген өлшемді аргументке қолданыла алады;

– хэш-функциясының тиімді мәнінің өлшемі белгіленген;

– кез келген аргумент үшін хэш-функцияны жай ғана есеп шыға жеткілікті; хэш-функцияны есептеу жылдамдығы хэш-функцияны қолдану кезіндегі ЭЦҚ құру мен тексеру жылдамдығы хабарламаның өзін қолданған кездегі жылдамдығынан елеулі үлкен болу керек;

– хэш-функция М мәтініндегі қою, шығарып салулар, орын ауытыру және т.б. сияқты түрлі өзгерістерге сезімтал;

– хэш-функциясы бір бағытталған, яғни қайтымсыздық қасиетін иеленеді, басқаша айтқанда керекті хэш-функция мәнін иеленетін М ' құжатын сұрыптау есептік шешімі жоқ болуы керек;

– екі түрлі құжаттардың (өзындықтарына қарай) хэш-функция мәндері бірдей болу ықпалдығы өте аз, яғни кез келген белгіленген хүшін есептік көз қарасы бойынша h(x') = h(x) болатындай хүшін х' табу мүмкін емес;

Осылайша, хэштеу функциясы өзгетілген хабарламаларды анықтау үшін қолданыла алады, яғни криптографиялық бақылау сомасын құрылыдау үшін қызмет ете алады. Бұл сипатта хэш-функциясы ЭЦҚ құру және тексеру кезінде хабарлама тұтастығын бақылау үшін қолданылады.

Белгілі хэштеу алгоритмдері:

– MD (Message Digest) – әлемде ең көп таралаған хэштеу алгоритмдерінің қатары; мысалы, MD5 алгоритмі Microsoft Windows соңғы нұсқаларында пайдаланушы кілтсөзін 16-байтты санға түрлендіру үшін қолданылады;

– МЕМСТ Р 34.10-2001 ресейлік стандарты - 32 байт өлшемі бар хэш есептейді;

– SHA-1 (Secure Hash Algorithm) – енгізу мәліметтерінің 160-битті хэш-кодын қалыптастыратын хабарлама дайджестін есептеу алгоритмі; әлемде кең таралған, ақпаратты қорғау жүйелік протоколдарының көбінде қолданылады.

Пайдаланушыларды аутентификациялау үшін Хэш-функциясы кеңінен қолданылады.

Өзін-өзі бақылау сұрақтары:

1. Электрондық цифрлық қолтаңба қолданылады -

a) телекатынас арналарымен тасымалданатын мәтіндерді аутентификациялау үшін

b) объектінің шынайылығын тексеру

c) тұтынушыны тексеру
d) пайдаланушының қатынау мүмкіндіктерін тексеру
e) қолтаңба қою және қолтаңбаны тексеру үшін

2. ЭЦҚ жүйесінің құрамды екі процедурасы -
a) қолтаңба қою және қолтаңбаны тексеру
b) симметриялық және ассиметриялық
c) күрделі және қарапайым
d) орын ауыстыру және жай ауыстыру
e) негізгі және кірме

3. Эль Гамаль шифрлау сұлбасы-
a) шифрлау үшін де, цифрлық қолтаңба қою үшін де пайдаланылады
b) ассиметриялық жүйенің құрамды бөлігі
c) симметриялық жүйенің құрамды бөлігі
d) қолтаңба қою және қолтаңбаны тексеру үшін қолданылады
e) объектінің шынайылығын тексеру үшін қолданылады

4. SHA алгоритмі -
a) АҚШ-та 1992 жылғы қауіпсіз хэштеу стандарты құрамында жасалған
b) кез-келген тізбектелген екілік символдарға арналған функцияны есептейтін алгоритм мен процедураны анықтайды
c) мәліметтерді шифрлау және ЭЦҚ режімінде жұмыс жасайды
d) 1977 жылы АҚШ-тың Ұлттық стандарттар бюросында жарияланды
e) шифрлау үшін де, цифрлық қолтаңба қою үшін де пайдаланылады

5. ГОСТ Р34.11-94 хэш функциясы -
a) кез-келген тізбектелген екілік символдарға арналған функцияны есептейтін алгоритм мен процедураны анықтайды
b) АҚШ-та 1992 жылғы қауіпсіз хэштеу стандарты құрамында жасалған
c) мәліметтерді шифрлау және ЭЦҚ режімінде жұмыс жасайды
d) 1977 жылы АҚШ-тың Ұлттық стандарттар бюросында жарияланды
e) шифрлау үшін де, цифрлық қолтаңба қою үшін де пайдаланылады

6. RSA алгоритмі -
a) мәліметтерді шифрлау және ЭЦҚ режімінде жұмыс жасайды
b) 1977 жылы АҚШ-тың Ұлттық стандарттар бюросында жарияланды
c) АҚШ-та 1992 жылғы қауіпсіз хэштеу стандарты құрамында жасалған
d) кез-келген тізбектелген екілік символдарға арналған функцияны есептейтін алгоритм мен процедураны анықтайды
e) шифрлау үшін де, цифрлық қолтаңба қою үшін де пайдаланылады

7. Хэш функциялар-
a) шифрлау, аутентификациялау, қол қою үшін қолданылады
b) индентификациялау, аутентификациялау, қол қою үшін қолданылады
c) шифрлау, аутентификациялау үшін қолданылады
d) индентификациялау және аутентификациялау үшін қолданылады
e) электрондық цифрлық қолтаңбада қолданылады

8. Электрондық қолтаңба тетігі екі процедурадан тұрады:
a) қолтаңба құрастыру және қол қойылған мәліметтер бөлігін тексеру
b) құпия кілтті симметриялық және ашық кілтті асимметриялық
c) бөлек хабардың немесе ақпарат өрісінің тұтастығы және хабарлар ағынының немесе ақпарат өрістерінің тұтастығы
d) жүйеге тұтастай әкімшілік ету; қауіпсіздік функцияларына әкімшілік ету;
e) қолтаңба құрастыру және қауіпсіздік функцияларына әкімшілік ету

9. Электрондық ақпараттық ресурстар -
a) электрондық түрде сақталатын (ақпараттық мәліметтер қоры), ақпараттық жүйелерде қамтылатын ақпарат
b) аталған объектілерді олардың меншік иесі айқындаған шекте және тәртіппен иелену, пайдалану және оларға билік ету құқығын іске асыратын субъект
c) ақпаратты алу, көшірмесін түсіру, тарату, бұрмалау, жою немесе оны құрсаулау жөніндегі заңсыз іс-әрекеттерді қоса алғанда, электрондық ақпараттық ресурстарды, ақпараттық жүйелерді сақтауға, оларға заңсыз қол жеткізуді болғызбауға бағытталған құқықтық, ұйымдастырушылық және техникалық іс-шаралар кешені
d) мемлекеттік құпияларды қамтымайтын электрондық ақпараттық ресурстар, оларға қол жеткізу Қазақстан Республикасының заңдарына сәйкес немесе оны Қазақстан Республикасының заңнамасында көзделген жағдайларда меншік иесі немесе олардың иеленушісі шектейді
e) өзіне қажетті электрондық ақпараттық ресурстарды алу үшін ақпараттық жүйеге өтініш жасайтын және оларды пайдаланатын субъект

10. «Электрондық әкімдік» -
a) жергілікті атқарушы органдардың электрондық қызметтер көрсетуді ұсыну жөніндегі жұмыс істеу тетігі
b) ақпараттық технологияларды пайдалана отырып жеке және заңды тұлғаларға ақпараттық, интерактивтік және транзакциялық қызмет көрсетуді ұсыну
c) мемлекеттік органдардың электрондық қызмет көрсетулерді ұсыну жөніндегі жұмыс істеу тетігі
d) электрондық ақпараттық ресурстар мен ақпараттық жүйелерді иелену, пайдалану және оларға билік ету құқықтарын толық көлемде іске асыратын
e) электрондық ақпараттық ресурстар мен ақпараттық жүйелер сипаттамаларының жиынтығын қамтитын жүйеленген тізбе

11. Электрондық қызмет көрсету -
a) ақпараттық технологияларды пайдалана отырып жеке және заңды тұлғаларға ақпараттық, интерактивтік және транзакциялық қызмет көрсетуді ұсыну

b) мемлекеттік органдардың электрондық қызмет көрсетулерді ұсыну жөніндегі жұмыс істеу тетігі
c) электрондық ақпараттық ресурстар мен ақпараттық жүйелерді иелену, пайдалану және оларға билік ету құқықтарын толық көлемде іске асыратын
d) электрондық ақпараттық ресурстар мен ақпараттық жүйелер сипаттамаларының жиынтығын қамтитын жүйеленген тізбе
e) жергілікті атқарушы органдардың электрондық қызметтер көрсетуді ұсыну жөніндегі жұмыс істеу тетігі

12. «Электрондық үкімет» -
a) мемлекеттік органдардың электрондық қызмет көрсетулерді ұсыну жөніндегі жұмыс істеу тетігі
b) электрондық ақпараттық ресурстар мен ақпараттық жүйелерді иелену, пайдалану және оларға билік ету құқықтарын толық көлемде іске асыратын
c) электрондық ақпараттық ресурстар мен ақпараттық жүйелер сипаттамаларының жиынтығын қамтитын жүйеленген тізбе
d) жергілікті атқарушы органдардың электрондық қызметтер көрсетуді ұсыну жөніндегі жұмыс істеу тетігі
e) ақпараттық технологияларды пайдалана отырып жеке және заңды тұлғаларға ақпараттық, интерактивтік және транзакциялық қызмет көрсетуді ұсыну

13. RSA криптожүйесін-
a) 1978 жылы Р.Л.Райвест, А.Шамир, Л.Адлеман ойлап тапқан
b) 1979жылы Р.Л.Райвест, А.Шамир, Л.Адлеман ойлап тапқан
c) 1976 жылы Р.Л.Райвест, А.Шамир, Л.Адлеман ойлап тапқан
d) 1978 жылы Р.Л.Райвест, А.Шамир ойлап тапқан
e) 1978 жылы А.Шамир, Л.Адлеман ойлап тапқан

14. RSA криптожүйесі-
a) натурал сандарды жай көбейткіштерге жіктеудің қиындығына негізделген
b) бүтін сандарды жай көбейткіштерге жіктеудің қиындығына негізделген
c) бөлшек сандарды сандарды жай көбейткіштерге жіктеудің қиындығына негізделген
d) теріс сандарды жай көбейткіштерге жіктеудің қиындығына негізделген
e) оң сандарды жай көбейткіштерге жіктеудің қиындығына негізделген

15. N=pq саны
a) RSA модулы деп аталады
b) RSA тұрақтысы деп аталады
c) RSA көбейткіші деп аталады
d) RSA формуласы деп аталады
e) RSA аргументі деп аталады

8 ЖЕЛІДЕ КОМПЬЮТЕРЛІК АҚПАРАТТЫ ҚОРҒАУ

Компьютер желілерінің тез дамуы, ақпарат іздеудің жаңа технологияларының пайда болуы әртүрлі адамдар және мекемелердің интернет желісіне болған қызығушылығын арттырып отыр. Глобальды желіні коммерциялық мақсаттарда және құпия ақпараттарды өңдеуде қолдану тиімді ақпарат қорғау жүйесін құруды талап етеді. Локальды және корпоративті желіні интернет жүйесіне қосар кезде ол желінің ақпараттық қауіпсіздігін қамтамасыз етуіміз қажет.

Интернет глобальды жүйесі ашық жүйе ретінде құрылған. Сондықтан, интернет жүйесі әртүрлі деңгейдегі ақпарат қауіпсіздігін бұзушыларға көп мүмкіндіктерді береді.

Интернет желісі арқылы ақпарат бұзушысы мынадай іс-әрекеттерді орындай алады: мекеме ішкі желісіне еніп конфиденцияльды ақпараттарды, серверлер адрестерін, парольдерін, олардың мазмұнын көшіріп алуы мүмкін. Осы алынған ақпараттар арқылы мекеме бәсекелестігіне өте үлкен зиян келуі және клиенттер сенімін жоғалтуы мүмкін.

8.1 Брандмауэрлер

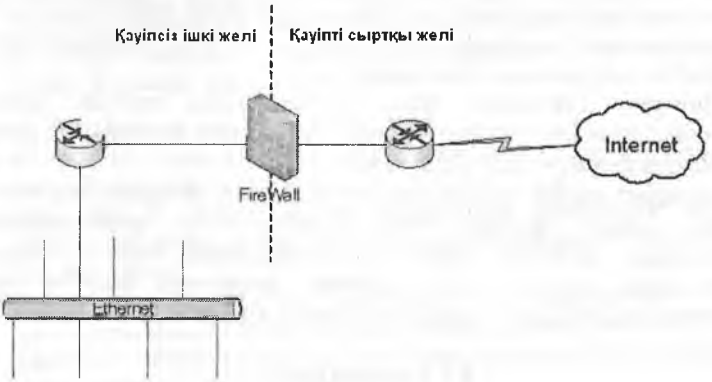
Компьютерлік емес салада брандмауэр (немесе firewall) деп– жанбайтын материалдардан дайындалған қабырғаға айтылады. Ал компьютерлік саладағы брандмауэр деп – ақпарат қауіпсіздігін бұзушылардың ішкі желіге еніп, компьютерлердегі ақпараттарды көшіру, өзгерту немесе жоюға қарсы тұратын бөгеттерге айтылады. Брандмауэрлер сыртқы желіге қауіпсіз шығуды қамтамасыз етіп, ішкі желідегі пайдаланушылардың енуіне шектеу қояды және сыртқы желіден рұқсат етілмеген бағдарламалардың енуіне шектеу қояды. Ол бірнеше компоненттерден (мысалы, брандмауэрдің бағдарламашы жұмыс істейтін маршрутизатор немесе шлюз) тұратын қорғау бөгеттері болып табылады. Брандмауэр ішкі желіге рұқсатты қауіпсіздік саясаты бойынша береді.

Барлық енетін және шығатын пакеттер брандмауэр арқылы өтеді және ол тек авторазацияланған пакеттерді ғана өткізеді. Бірақ, ешқандай да брандмауэр 100% қауіпсіздікті қамтамасыз ете алмайды. Көптеген коммерциялық мекемелер үшін брандмауэрді орнату ішкі желінің қауіпсіздігі үшін қажетті болып саналады.

Интернетте әртүрлі компьютерлер арасында байланыс орнатуды қамтамасыз ететін протокол TCP/IP протоколы. TCP/IP пакеттерді маршрутизациялауға мүмкіндік берғендіктен ол желіаралық протокол ретінде қолданылады. TCP/IP пакет тақырыптарындағы мәліметтер крекерлер тарабынан жиі шабуылданады.

Брандмауэрдің басты міндеті - желі байланысын сырттан да, компьютер желісінен де рұқсатсыз кіруден қорғау. Брандмауэрлер әртүрлі

типте және өлшемдерде болады және жиі бірнеше түрлі компьютерлерде орнатылған кешен болып табылады. Мұнда брандмаузер (firewall) - бұл **сенімді (trusted)** ішкі желілер мен **сенімсіз (untrusted)** сыртқы (мысалы, Интернет) желі арасында орналасқан, желілер арасындағы ағып жатқан трафикті зерттеп отыратын бір немесе бірнеше құрылғы (16-сурет).



Сурет 16. Желідегі брандмауэр

Брандмауэрлер келесі қасиеттерге ие:

1. Барлық байланыс брандмауэр арқылы өтеді.
2. Брандмауэр тек уәкілетті трафикке рұқсат береді.
3. Брандмауэр өзіне бағытталған шабуылдарға қарсы тұра алады.

Брандмауэрді қауіпсіз және қауіпті желілер арасындағы буфер ретінде қарастыруға болады. Брандмауэр (firewall – отты қабырға) термині құрылыс технологиясының атауынан шыққан, өрт кезінде өрттің таралуына жол бермейтін өртке қарсы кедергілерді орнату дегенді білдіреді. Шын мәнінде бұл жай ғана кедергі. Желілік брандмауэр - басқа желілерден кіруге қарсы әрекет ету құралы.

Брандмауэр ретінде зиян тигізуі мүмкін сыртқы хосттарда орналасқан қызметтерден қорғауға арналған маршрутизаторлар, дербес компьютерлер, хост немесе хосттардың түрлері қолданылуы мүмкін. Әдетте, брандмауэр жүйесі ішкі желінің шекарасында, яғни оның Интернетке қосылу нүктесінде орнатылады. Дегенмен, брандмауэр желі ішінде орналасуы мүмкін, бұл шектеулі хосттар үшін қосымша, арнайы қорғауды қамтамасыз етеді.

Қауіпсіз желіні қорғау тәсілі брандмауэр құрылымы мен қолданылатын ережелерге байланысты болады. Қазіргі уақытта брандмауэрлердің төрт негізгі санаты бар:

1. Пакеттік сүзгілер.
2. Қолданбалы деңгейдегі шлюздер.
3. Сілтемелік деңгейлі шлюздер.

4. Күйін тіркеу арқылы пакеттерді тексеру процессорлары.

Барлық басқа бағдарламалық жасақтағы технологиялар секілді, брандмауэр де өмірлік циклге ие, сол цикл бойы оның жобалануы, дайындығы және жетілдірілуі жүреді.

Брандмауэр белгілі бір проблеманы шешудің арнайы құралы болып табылады - рұқсат етілмеген трафикті анықтау, ал оның қолданылуы қорғаныс дәрежесі мен жүйенің функционалдығы арасында ымыраға келу қажеттігін жоққа шығарады.

Жалпы алғанда, брандмауэрлер жүйеде рұқсат етілмеген немесе күтілмеген әрекеттердің (мысалы, хакерлердің қызметі) қауіп-қатерін азайтуға мүмкіндік береді. Қандай қауіп-қатерден брандмауэрлер жүйені қорғайды? Корпоративтік жүйелер мен мәліметтер келесі қауіп-қатерлерден қорғауды қажет етеді:

- Құпиялылықты бұзу қаупі.
- Мәліметтердің тұтастығын бұзу қаупі.
- Қолжетімділікті бұзу қаупі.

Шабуылдардың негізгі түрлері.

Адам факторы (social engineering).

Қажетті ресурстарға қолжетімділігі бар немесе жүйелік операцияларды жүзеге асыруға қажетті құқығы бар әкімшінің немесе басқа қолданушының құпия сөзіне немесе сертификатына ие болуды білдіреді.

Бағдарламалық қамтамасыз етудің қателіктері (software bug).

Шабуылдаушы бағдарламалық қамтамасыз етудің ақауын пайдаланып, қосымшаны немесе қызметті рұқсат етілмеген немесе күтілмеген пәрмендерді орындауға мәжбүрлейді. Мұндай шабуылдар қосымша кеңейтілген немесе әкімшілік құқықтарда жұмыс жасаған кезде аса қауіпті. Осындай шабуылдар буфердің толып кетуі (butteroverflow) және жол форматындағы қателіктер (formatstringvulnerabilities) кезінде орын алу мүмкін.

Вирустар жән немесе трояндық аттар (Viruses and / or Trojan code).

Заңды пайдаланушының зиянды бағдарламаны іске қосуын білдіреді. Әдетте мұндай шабуыл бағдарламасы қарапайым электрондық пошта хабарымен немесе вирустың көмегімен таратылады. Орындалу үшін іске қосылған мұндай бағдарлама көп нәрсеге қабілетті, ол бейтаныс адамға қолжетімділікті ашып қана қоймай, файлдарды және / немесе сертификаттарды ұрлайды, сонымен қатар жүйелік файлдарды жоя алады.

Жүйенің нашар түзетілімі.

Шабуылдаушы жүйе түзетіліміндегі қателерді қолданады: қол жетімді қызметтер және / немесе тіркеу жазбасы. Жаңа әкімшілер көбіне әдепкі парольдерді және тіркеу жазбаларын (жүйеде де, қолданбалы деңгейінде де) өзгертуге ұмытып кетеді (немесе білмейді), сонымен қатар әкімшілік

қосымшаларға кіруді шектемейді және бөтен және пайдаланылмаған қызметтерді өшірмейді.

Брандмауэрлердің артықшылықтары мен кемшіліктері.

Брандмауэр – қауіпсіздік жүйесі архитектурасының фрагменттерінің бірі ғана және архитектураның қандай да бір бөлігі сияқты күшті және әлсіз жақтары бар.

Артықшылықтары

– Брандмауэрлер корпоративтік қауіпсіздік саясатын жүзеге асыруда ерекше болып табылады.

– Олар басқару құралдарына енуді шектейтіндей, ал жалпыға ортақ ресурстарға шектемейтіндей етіп түзетілуі тиіс

– Брандмауэрлер белгілі бір қызметтерге кіруді шектейді.

✓ Мысалы, брандмауэр Веб-серверге еркін қол жеткізуге мүмкіндік береді, бірақ Telnet және жалпы пайдалану үшін арналмаған басқа да қатынастарға енуге тыйым салады. Аутентификация функцияларының көмегімен көптеген брандмауэр таңдаулы қол жеткізуді қамтамасыз етеді.

Брандмауэрлер арнайы құрал болып табылады. Демек, қауіпсіздік пен функционалдылық дәрежесі арасында ымыраға келудің қажеті жоқ.

Брандмауэрлер - тамаша ревизорлар. Жеткілікті дискілік кеңістікке ие немесе журналдарды қашықта сақтау мүмкіндігі бар болғандықтан, брандмауэр өзі арқылы өтетін бүкіл трафикті (немесе көрсетілген бір ғана) тіркей алады. Брандмауэрлер пайдаланушыларға тиісті оқиғалар жөнінде ескерту жасай алады

Кемшіліктері

– Брандмауэрлер рұқсат етілген мазмұннан қорғай алмайды.

– Брандмауэрлер қосымшаларды қорғайды және осы қосымшалармен әдеттегі ақпарат алмасуға мүмкіндік береді (әйтпесе брандмауэрлер жақсыдан гөрі көп зиян келтіретін еді). Бірақ егер қосымшаларда ақаулар болса, онда брандмауэрлер оларды түзетпейді және шабуылды болдырмауға мүмкіндік бермейді, себебі брандмауэрге жіберілген барлық ақпарат толығымен қабылданады.

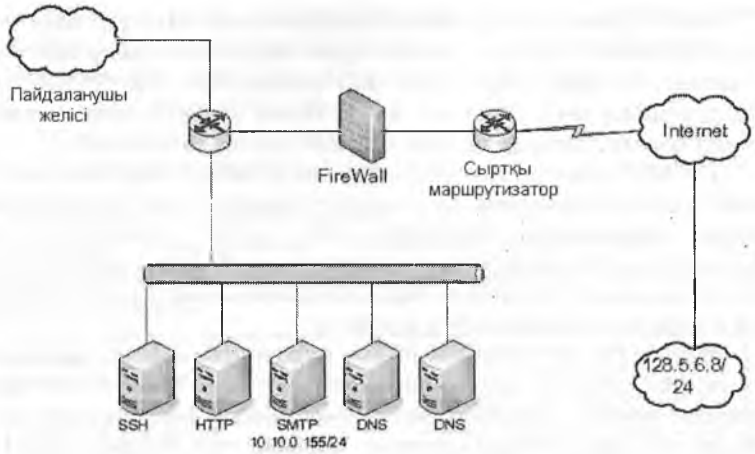
– Орындауға арналған ережелері қаншалықты тиімді болса, брандмауэрлер де соншалықты тиімді болып табылады.

– Тегін ережелердің жиынтығы брандмауэрдің тиімділігін төмендетеді.

– Зиянды мақсаттарда өз құқықтарын әдейі пайдаланатын уәкілетті пайдаланушы сияқты брандмауэрлер адам факторы алдында әлсіз.

– Брандмауэрлер әкімшілік қателіктерін жоя алмайды немесе нашар дайындалған қауіпсіздік саясатын өзгерте алмайды.

– Брандмауэрлер трафиктері өзі арқылы өтпеген шабуылдарға қарсы тұра алмайды.



Сурет 17. Қауіпсіз және қауіпті желілердің брандмауэрге қатысты өзара орналасуы

Пакеттерді сүзу мысалын қарастыру үшін, біз мынадай критерийлер бойынша бірқатар ережелерді орнатамыз:

– хаттаманың түрі;
– жіберушінің мекен-жайы;
– алушының мекен-жайы;
– жіберушінің порты;
– алушының порты;
– критерийге сәйкестікті анықтаған кезде брандмауэрдің жасау қажет әрекеті

8.2 Интернет қызметтерінің кемшіліктері

FTP-(File Transfer Protocol) файлдарды жіберу протоколы. Тексттік және екілік файлдарды жіберуде қолданылады. FTP-серверлерде құжаттар, бағдарламалар, графика және тағы басқа ақпараттар сақталады.

SMTP - (Simple Mail Transfer Protocol) протоколы интернетте почта тасмалдау қызметін атқарады. Бұл протоколды қолдану проблемаларының бірі почтаны қабылдаушы почта жіберішінің адресін тексере алмайды. Хакер ішкі желіге өте көп почталық хабарлар жіберіп, сервер жұмысын істен шығаруы мүмкін.

Интернетте кең тараған Send-Mail электеронды бағдарламасы өзінің жұмысында ақпарат жіберушінің IP адресін қолданады. Крекер Send-Mail арқылы жіберіліп жатқан хабарларды алып, адрестерді ауыстыру арқылы шабуылға шығуы мүмкін.

DNS – (Domain Name Server) желідегі аттар қызметі. DNS-те желі туралы мәліметтер мысалы, әрбір IP-адресі бар компьютерлер саны туралы мәліметтер болады. DNS проблемаларының бірі бұл базаны бөгде пайдаланушылардан жасыру өте қиын. Нәтижеде DNS арқылы локальды желідегі компьютерлер саны және олардың аттарын біліп алады.

TELNET (алыс терминалды эмуляциялау қызметтері) алыс желілерге қосылу үшін қолданылады. Бұл қызметті қолдану үшін пайдаланушылар тіркеліп, парольдерін ендірулері керек. Алыс терминалдан тұрып пайдаланушы файл және бағдарламалармен жұмыс істеуі мүмкін. TELNET жүйесіне қосылып, бағдарлама пайдаланушыларының барлығының аттары және парольдері жазылып алынуы мүмкін.

WWW (World Wide Web) – интернетте әртүрлі серверлердің мазмұнымен танысуға мүмкіндік беретін жүйе. WWW-тің ең маңызды қасиетінің бірі бұл гиперсілтемелерді қолданады. Бірақ, мұның ең әлсіз жері де сол гиперсілтемені қолдану. Өйткені гиперсілтемеде бір беттен екінші бетке қалай өтетіндігі туралы мәліметтер бар. Крекерлер осы мәліметтерді біліп алып, жүйені бұзу мүмкін.

8.3 Желілік қауіпсіздік саясаты

Желілік қауіпсіздік саясаты екі бөліктен тұрады:

1. Желілік қызметтерге рұқсат алу саясаты;
2. Брандмауэрлердің қолдану саясаты.

Желілік қызметтерге рұқсат алу саясатына сәйкес интернеттегі кейбір қызметтерді пайдалануға және интернетке қосылу жолдарына шектеу қойылған.

Мысалы, SLIP (Serial Line Internet Protocol) және PPP (Point to Point Protocol) интернетке шектеу қоятын (қосылу жолдарына) протоколдар. Интернеттегі пайдалануға тыйым салынған қызметтерді басқа жолмен пайдаланбауды көздейді. Желілік қызметтерге рұқсат алу саясаты келесі принциптердің біреуін пайдалана алады:

- интернеттен ішкі желіге рұқсатты болдырмау, ал ішкі желіден интернетке тығуға рұқсат жоқ;
- интернеттен ішкі желіге шектелген қызметтерге рұқсат беру, мысалы, почталық серверлерге.

Брандмауэрлердің қолдану саясаты бойынша ішкі желі ресурстарына рұқсат алу әдістері анықталады. Ең алдымен қорғау жүйесі қаншалықты сенімді екенін анықтап алу керек. Басқаша айтқанда ішкі ресурстарға рұқсат алу мына принциптердің біреуіне негізделген болуы керек:

- ашық түрде рұқсат берілмеген барлығына тыйым салу;
- ашық түрде тыйым салынбаған барлығына рұқсат.

Брандмауэрлердің бірінші принцип бойынша қолдану жоғары дәрежедегі қауіпсіздікті қамтамасыз етеді. Бірақ, бұл принципті қолдану пайдаланушыларға қиындықтар тудырып, орындалу қиынға түседі.

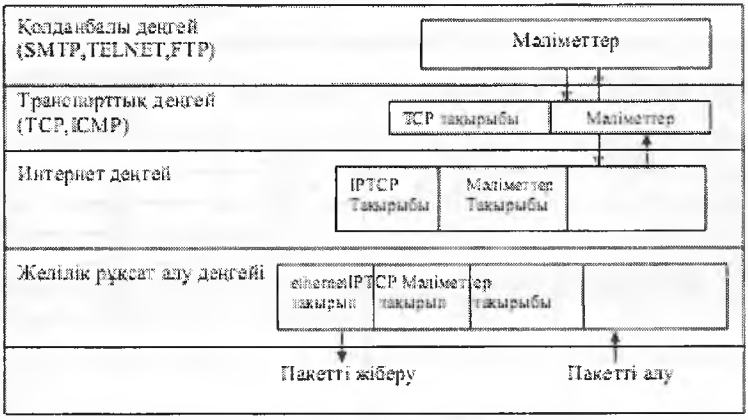
Брандмауэрлерді екінші принцип бойынша қолдану ыңғайлы және аз шығынды болғанымен ішкі желі қауіпсіздігі өз деңгейінде болмайды.

Брандмауэрлердің компоненттері үш топқа бөлінеді:

1) Желілік деңгейдегі шлюздар;
2) Фильтрлеуші маршрутизаторлар;
3) Қолданбалы деңгейдегі шлюздар.

Фильтрлеуші маршрутизаторлар

Серверде орындалатын бағдарлама енуші және шығушы пакеттерді фильтрлеу пакеттердің IP-тақырыптарында орналасқан ақпарат бойынша орындалады.



Сурет 18. TCP/IP протоколына мәліметтерді жіберу және мәліметтерді қабылдау схемасы.

Фильтрлеуші маршрутизатор IP-пакеттерді пакет тақырыбындағы мына өрістердің мазмұны бойынша фильтрлеуі мүмкін:

1) жіберуші IP-адресі, яғни пакетті жіберген жүйе адресі;
2) қабылдаушы IP-адресі, яғни пакетті қабылдаушы адрес;
3) жіберуші порты, яғни жіберуші жүйесіндегі байланыс порты;
4) қабылдаушы порты.

Порт – клиент және сервер қолданатын бағдарламалық анықтама. Порт 16 биттік сан арқылы идентификацияланады. Фильтрлеу әртүрлі жолмен хост компьютерлер және порттармен байланыстарды болдырмау үшін қолданылуы мүмкін. Мысалы, сенімсіз деген компьютерлермен байланыстарды үзуге болады. Егер брандмауэр TCP немесе UDP протоколымен байланысты болдырмайтын болса,онда брандмауэр белгілі бір хост компьютерлермен байланысын өз қауіпсіздік саясаты бойынша жүргізуі мүмкін. Мысалы, ішкі желі белгілі бір жүйелерден басқа барлық жүйелерден енуші байланыстарды болдырмауы мүмкін.

Бұл жүйелер үшін кейбір қызметтер ғана рұқсат етілуі мүмкін (SMTP 1 – жүйе үшін, TELNET және FTP басқа жүйе үшін). Фильтрлеуші маршрутизаторға мысал ретінде ішкі желімен 123.4.*.* адресі бойынша байланыс орнатушы қауіпсіздік саясатының орындалуын қарастырайық.

TELNET – байланыстар бір ғана 123.4.5.6 адресті хост компьютермен орнатылуы мүмкін.

SMTP – байланыстар 2 хост компьютермен 123.4.5.7 және 123.4.5.8 рұқсат етілген.

NNTP – (NetWork News Transfer Protocol) протоколы бойынша байланыс жаңалық сервері, адресі 129.6.48.254 болған сервер және ішкі желідегі 123.4.5.9 адресті компьютерге ғана рұқсат етілген.

8.4 Фильтрлеу әдістері

Түрі	Жіберушінің адрес	Қабылдаушының Адрес	Жіберушінің порты	Қабылдаушының порты	Әрекет
TCP	*	123.4.5.6	>1023	23	Рұқсат
TCP	*	123.4.5.7	>1023	25	Рұқсат
TCP	*	123.4.5.8	>1023	25	Рұқсат
TCP	129.6.48.254	123.4.5.9	>1023	119	Рұқсат
UDP	*	123.4.*.*	>1023	>123	Рұқсат
*	*	*	*	*	Рұқсат жоқ

1-ші әдіс бойынша порт номері >1023 болған барлық инетернеттегі компьютерлерден пакеттерді 123.4.5.6 компьютерінің алуына рұқсат.

2-ші, 3-ші әдістер бойынша адрестері 123.4.5.7 және 123.4.5.8 компьютерлеріне SMTP пакеттерін 25-ші порт арқылы қабылдауға рұқсат.

4-ші әдіс бойынша 129.6.48.254 компьютерден 123.4.5.9 компьютерге пакеттерді қабылдауға рұқсат.

5-ші әдіс бойынша UDP протоколы бойынша байланысқа рұқсат бар.

6-шы басқа барлық әдістерге рұқсат жоқ.

Пакеттерді фильтрлеу әдістерінің құрылуы өте күрделі. Фильтрленген пакеттерді тестілеу құралдары жоқ. Кейбір фильтрлеуші маршрутизаторлардың протоколдау құралдары жоқ. Сондықтан, қауіпті пакеттер маршрутизатордан өтіп кетсе, олар өздерін танытқанға дейін танып-білуге болмайды.

Егер желі администраторы фильтрлеудің тиімді әдістерін қолдансада оның мүмкіндіктері шектеулі болып қала береді. Мысалы, администратор белгісіз болған адрестерден келуші пакеттерді ішкі желіге енуіне рұқсат бермейтін әдісті қолданады. Бірақ, хакерлер пакеттерді жіберу кезінде

сенімді (авторизацияланған) клиенттердің адрестерін қолдануы мүмкін. Бұл жагдайда фильтрлеуші маршрутизатор жалған пакетті ажырата алмай өткізіп жіберуі мүмкін. Шабуылдың бұл түрі адрестерді өзгерту деп аталады.

Өзін-өзі бақылау сұрақтары:

1. Брандмауэр –
a) екі немесе бірнеше желілер арасында қорғаныс барьерін құрушы жүйелер комбинациясы
b) үш немесе бірнеше желілер арасында қорғаныс барьерін құрушы жүйелер комбинациясы
c) жауабы жоқ;
d) шифрланатын мәтіннің бөлігіне қолданылатын түрлендірудің негізгі әдістерінің тізбегі
e) үш немесе төрт желінің арасында қорғаныс барьерін құрушы жүйелер комбинациясы

2. Брандмауэр жүйесі төмендегідей болуы мүмкін: 1)Репититор 2)жол көрсету 3)ПК 4)Хаост 5)ресивер
a) 1, 2, 3
b) 2, 3, 4
c) 1, 4, 5
d) 3, 4, 5
e) 2, 4, 5

3. Брандмауэрлердің алғашқы ұрпағы қандай көрсеткіштерге ие болған?
a) пакеттердің фильтрациялы маршрутизаторларына
b) пакетті фильтрациялы хостарға
c) қол жетпейтін серверлер
d) бағынышты серверлер
e) дұрыс жауап жоқ

4. Брандмауэрлер көбіне қандай платформада функционалдайды?.
a) Windows NT
b) UNIX
c) OS/2
d) MS DOS
e) ешқандай

5. Сигнатуралар-
a) қорғаныс үшін пайдадланылатын және бағдарламалық тәсілмен тексерілетін электронды есептеуіш машинаның бесаспап сипаттамасы
b) ақпаратты оның кілтін білмей-ақ кері шифрлау мәселесімен айналысады
c) акпаратты заңсыз пайдаланушылардан корғау мақсатымен оны турлендіру әдістері жайындағы ғылым
d) ақпаратты шифрлау арқылы түрлендіреді
e) қорғаныс үшін пайдадланылатын электронды есептеуіш машинаның бесаспап сипаттамасы

6. Хакерлер категориясы:
a) хакер-дилетанттар және хакер-мамандар
b) саяси хакерлер және тыңшы хакерлер
c) пайдакүнем хакерлер және маманданған хакерлер
d) өндірістік хакерлер және хакер-дилетанттар
e) хакер-ойшылдаржәне хакер-мамандар

7. Сандық берілу-
a) бұл дәстүрлік қолжазбалық сигнатураның электрондық эквиваленті
b) бұл дәстүрлік қолжазбалық көшірменің электрондық эквиваленті
c) бұл дәстүрлік қолжазбалық сигнатураның электрондық көшірмесі
d) бұл математикалық қолжазбалық сигнатураның электрондық эквиваленті
e) бұл аралас қолжазбалық сигнатураның электрондық эквиваленті

8. Қолжазбалық сигнатуралар-
a) қауіпсіздік қызметін қамтамасыз етеді
b) саяси қызметін қамтамасыз етеді
c) қорғаудың қызметін қамтамасыз етеді
d) ақпарат кошірмесін сақтауды қамтамасыз етеді
e) ақпараттың тұтас жетуін қамтамасыз етеді

9. Компьютер желісіндегі ақпараттың қауіпсіздігін жабдықтау үшін келесі қасиеттерді сақтау керек:
a) қажеттілігі, тұтастылығы, құпиялылығы
b) қажеттілігі, құпиялылығы
c) арнаулылығы, тұтастығы, айқындылығы
d) пайдалылығы, құндылығы, бағалылығы.
e) пайдалылығы, тұтастылығы, құпиялылығы

10. Интернеттегі қорғаныс хаттамасының басқа трансакциясы
a) SET
b) GET
c) NT
d) IP
e) TP

11. SET цифрлық сертификаттың стандарты қандай?
a) X.509
b) X.100
c) ГОСТ 28147-89
d) 21-36N
e) ГОСТ 34

12. Брандмауэр бұл .....
a) желі аралық экран
b) интернет
c) желі
d) шифр
e) дұрыс жауап жоқ

13. Хаттамалар талдауышы немесе дестелердің сниффері-
a) тыңдау режимінде жұмыс істейтін тораптық бейімдеуішті пайдаланатын қолданбалы программа
b) көру режимінде жұмыс істейтін тораптық бейімдеуішті пайдаланатын қолданбалы программа
c) есту режимінде жұмыс істейтін тораптық бейімдеуішті пайдаланатын қолданбалы программа
d) тыңдау режимінде жұмыс істейтін тораптық бейімдеуішті пайдаланатын қолданбалы құрылғы
e) көру режимінде жұмыс істейтін тораптық бейімдеуішті пайдаланатын қолданбалы құрылғы

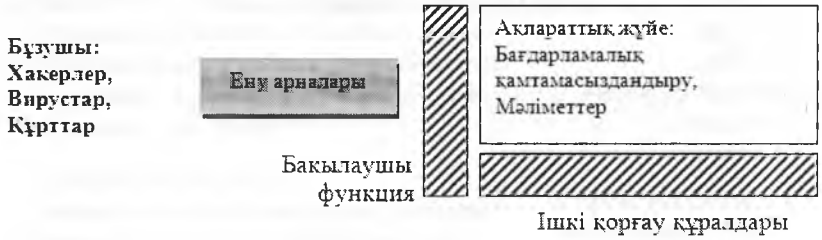
14. Ethernet желісі мәліметті жіберудің қандай әдісімен орындалады
a) манченстерлік кодтау
b) потенциалдар
c) скрэмблерлеу
d) қысу
e) аналогты кодтау

15. ArcNet желісі мәліметті жіберудің қандай әдісімен орындалады
a) скрэмблерлеу
b) потенциалдар
c) манченстерлік кодтау
d) қысу
e) аналогты кодтау

9 АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІҢ ҚАУІПСІЗДІК МОДЕЛЬДЕРІ

9.1 Ақпараттық жүйенің қауіпсіздік моделі

Ақпараттық жүйенің қауіпсіздігінің жалпы моделін төмендегідей суреттеуге болады (19-сурет):



Сурет 19. Ақпараттық жүйенің қауіпсіздік моделі

Берілген модель ақпараттық жүйе қауіпсіздігінің концепциясын суреттейді, оның көмегімен рұқсатсыз енуді алдын алады. Желідегі қолжетімді жүйелерге заңсыз енуге тырысатын хакердің желіні бұзу барысында жай ғана ләззат алуы мүмкін, сонымен қатар ол ақпараттық жүйені зақымдауы және/немесе өз мақсаттары үшін бір-нәрселерді енгізуі мүмкін. Мысалы, хакердің мақсаты жүйеде сақталған несие карталарының нөмірлерін алу болып табылады.

Қаламайтын қолжетімділіктің тағы бір түрі есептеуіш жүйеге қолданбалы бағдарламалар мен бағдарламалық қамтамасыз етуге редарторлар, компиляторлар және т.с.с. бір-нәрсені енгізу болып табылады. Осылайша, шабуылдардың екі түрі бар:

1. Жүйеде сақталған мәліметтерді алу немесе өзгерту үшін ақпаратқа қол жеткізу.

2. Пайдалануға жол бермеу үшін сервиске шабуыл жасау.

Вирустар мен құрттар - осындай шабуылдардың мысалдары. Мұндай шабуылдар дискеталар арқылы, сондай-ақ желі арқылы жүзеге асырылуы мүмкін.

Қажетсіз енуді болдырмайтын қауіпсіздік қызметтерін екі санатқа бөлуге болады:

1. Бірінші категория күзету функциясы бойынша анықталады. Бұл механизмдер кіру процедураларына негізделген, мысалы, рұқсатты пайдаланушыларға ғана рұқсат беретін құпия сөзді пайдалану. Сонымен қатар бұл механизмдерге әртүрлі қорғаушы экрандар (firewalls) жатады, олар хаттамалар ағынының TCP/IP әртүрлі деңгейлерінде шабуылдарды болдырмайды, және де, атап айтқанда, құрттардың, вирустардың енуі жөнінде ескертеді және басқа да ұқсас шабуылдарға жол бермейді.

2. Қорғаныстың екінші желісі пайдаланушыларға қол жеткізуді бақылауды және олардың қызметін талдауды жүзеге асыратын түрлі ішкі мониторлардан тұрады.

Ақпараттық жүйенің қауіпсіздігін қамтамасыз етудегі негізгі ұғымдардың бірі – авторландыру тұжырымдамасы болып табылады - белгілі бір ресурстарға және/немесе объектілерге кіру құқығын анықтау және беру.

Ақпараттық жүйенің қауіпсіздігінің негізін келесі негізгі қағидаттар құрауы керек:

3. Ақпараттық жүйенің қауіпсіздігі жүйе орнатылған ұйымның рөлі мен мақсаттарына сәйкес келуі керек.

4. Ақпараттық қауіпсіздікті қамтамасыз ету кешенді және тұтастық тәсілді қажет етеді.

5. Ақпараттық қауіпсіздік осы ұйымдағы басқару жүйесінің ажырамас бөлігі болуы тиіс.

6. Ақпараттық қауіпсіздік экономикалық негізделген болуы қажет.

7. Қауіпсіздікті қамтамасыз ету үшін жауапкершілік айқын болуы керек.

8. Ақпараттық жүйенің қауіпсіздігі кезең-кезеңімен қайта бағалануы керек.

9. Әлеуметтік факторлар, сондай-ақ әкімшілік, ұйымдық және физикалық қауіпсіздік шаралары ақпараттық жүйенің қауіпсіздігін қамтамасыз ету үшін өте маңызды.

9.2 Формальды модельдер

Қолжетімділікті басқаратын механизм ресурстарды қорғаудың негізі болып табылады, ол қорғалатын ақпараттық және техникалық ресурстарға-объекттерге субъекттердің (пайдаланушылар мен процесстер) қолжетімділігін шектеу шараларымен қамтамасыз етеді. Қолжетімділікті басқаратын механизм тәжірибе кезінде қорғалатын ресурстарға қолжетімділікті шектеу ережелерін және қорғалатын ресурсқа қолжетімділікті талап ету ережелерін анықтайтын абстрактті немесе формальды модельді іске асырады.

Әдебиетте мәліметтерге қол жеткізудің келесі формальды модельдері көрсетілген: Биба моделі, Гоген-Мезигер моделі, сазерлендская моделі, Кларк-Вильсон моделі, дискрециялық (матрицалық) модель, көп деңгейлі (мандаттық) моделі.

Тәжірибеде ең көп таралған – дискрециялық модель. Ол келесі ережелерге негізделген:

– барлық субъектілер мен объектілер анықталуы тиіс;

– субъектінің объектіге қол жеткізу құқығы кейбір сыртқы ережелер негізінде анықталады.

«Субъект-объект» қарым-қатынастарын қолжетімділік матрицасы ретінде қарастыруға болады, ондағы бағандарда АЖ субъектілері, жолдарда объектілер тізбектелген, ал жолдар мен бағандардың қиылысқан торларында қолжетімділіктің қосымша шарттары мен рұқсат етілген түрлері берілген. Осылайша, қол жеткізуді бақылауды жүзеге асыру объектіге сәйкес келетін матрица жолдарын тексеруден тұрады және

Үлгінің артықшылығы – сәйкес қорғау механизмдерін қарапайым жүзеге асыру. Кемшіліктері – модельдің статистикалық сипаты және субъектілер мен объектілер арасындағы қарым-қатынастың бөлшектік кезеңде сипаттау, соның салдарынан әкімшілік етудің күрделіленуі және қателердің пайда болуы.

Матрицалық модельдердің кемшіліктерін жою үшін көп деңгейлі модельдер (Белл және Ла-Падула, Деннингтің торлы моделі) әзірленді.

Бэлл және Ла-Пудал қауіпсіздік моделі

Бұл модель бойынша ақпараттық қауіпсіздікті қамтамасыз ету үшін төменгі деңгейдегі субъектілерге жоғарғы деңгейдегі субъектілердің ақпараттарын оқуға тыйым салынады.

Қауіпсіздік моделінің бірінші қасиеті: «Жоғарыға оқу жоқ»

Х-қауіпсіздік деңгейіндегі субъект, У-қауіпсіздік деңгейіндегі субъекттің ақпараттарын оқи алады, егер ол У-қауіпсіздік деңгейінен жоғары тұрса.

Қауіпсіздік моделінің екінші қасиеті: «Төменге қарай жазу жоқ»

Х-қауіпсіздік деңгейіндегі субъект, У-қауіпсіздік деңгейіндегі субъектке жаза алады, тек қана егер Х-қауіпсіздік деңгейіндегі субъект У-қауіпсіздік деңгейінен жоғары тұрса.

Көп деңгейлі қорғау модельдері матрицалыққа қарағанда нақты өмір мұқтаждықтарына анағұрлым жақынырақ, қолжетімділікті шектеудің автоматтандырылған жүйелерін құру үшін ең жақсы негіз болып табылады.

Қолжетімділіктің бақылаудың мандатты түрі келесі талаптарды қамтиды:

– барлық субъектілер мен АЖ объектілері бірегейлендірілуі тиіс;

– Құпиялылық белгілерінің желілік реттелген жиынтығы көрсетіледі;

– әрбір жүйе объектісіне ондағы ақпараттың құндылығын анықтайтын құпиялылық белгісі берілген - құпиялылық деңгейі;

– жүйенің әрбір субъектіне оған қол жеткізу деңгейін анықтайтын құпиялылық белгісі беріледі; субъектінің құпиялылық белгісі оның қолжетімділік деңгейі деп аталады.

Мандатты саясаттың басты мақсаты - төмен қолжетімділігі бар объектілерге жоғары қолжетімділігі бар объектілерден ақпараттардың ағылуын болдырмау болып табылады. Мандатты модельдің маңызды артықшылығы – бұл тұжырымның формалды дәлелі: егер жүйенің

бастапқы жағдайы қауіпсіз болса және жүйенің бір күйден екінші күйге көшуі қауіпсіздік саясатымен тұжырымдалған шектеулерді бұзбайтын болса, онда жүйенің кез-келген жағдайы қауіпсіз.

Мандатты модельдің кемшілігі - оны жүзеге асырудың күрделілігі. Көптеген операциялар оқу (мәліметтер ағыны объектіден субъектке бағытталған) және жазу (ағын субъектіден объектіге бағытталған) әрекеттерімен шектеледі.

Көбінесе, құпия ақпаратты өңдеуде ресурстарға қол жеткізуді шектеу саясатын жүзеге асырудың негізі дискрециялық үлгі, ал құпия ақпаратты - мандатты болып табылады.

9.3 Қауіпсіздік саясаты және негізгі элементтері

Қауіпсіздік саясаты – берілген қауіптер жиынынан КЖ қорғау құралдарының жұмысының реттемеленген нормалар, ережелер мен практикалық ұсыныстар жиынтығы.

Ұйымның қауіпсіздік саясаты ретінде ақпаратты және онымен байланысатын ресурстарды қорғауға бағытталған құжатталған басқару шешімдерінің жиынтығын түсінеді. Қауіпсіздік саясаттың көмегі арқылы ұйымның компьютерлік жүйесінің қызметі жүзеге асырылады. Жалпы қауіпсіздік саясаты қолданылатын компьютерлік ортамен анықталып, ұйымның арнайы талаптарын бейнелеп көрсетеді.

Әдетте КЖ түрлі, кейде өзара нашар келісетін аппараттық және бағдарламалық: компьютерлер, ОЖ, желілік құралдар, МББЖ, түрлі қосымшалар қамтамасыз ету күрделі кешені болып табылады. Әдетте бұл компоненттердің барлығы өзара келістіруге болатын меншікті қорғау құралдарына ие болады. Сондықтан корпоративтік жүйенің қауіпсіздігін қамтамасыз ету бойынша келіскен тұғырнама сапасында тиімді қауіпсіздік саясаты өте маңызды. Компьютерлік жүйенің өсуі және оның ғаламдық желіге ықпалдасу барысында жүйеде әлсіз орындарының жоқтығын қаматамыз ету керек, себебі ақпаратты қорғау бойынша барлық талпыныстар тек бір қателікпен құнсыздап қалуы мүмкін.

Қауіпсіздік саясатын нақты активтер мен қосымшаларға кімнің қатынауы бар екенін, нақты тұлғалардың қандай мақсаттары мен міндеттері бар екенін анықтайтындай, сонымен қатар нақты қауіпсіздік міндеттері қалай орындалу керектігін айқын бұйыратын қауіпсіздік үрдістерін ескеретіндей етіп құру керек. Нақты қызметкердің жұмысының ерекшелігі басқа жұмыскерлер қол жеткізбейтін ақпаратқа қатынауды талап етуі мүмкін. Мысалы, қызметкерлер бойынша менеджер кез келген қызметкердің жеке ақпапаратына қол жеткізе алады, сол кезде есептілік бойынша маман тек қызметкерлердің қаржылық мәліметтеріне қатынай алады, ал қатардағы қызметкер тек өзінің жеке ақпаратына қатынай алады.

Қауіпсіздік саясаты ұйымның компьютерлер мен желіні ұтымды пайдалану бойынша козқарасын, сонымен қатар қауіпсіздіктің

қақтығыстарына алдын алу және жауап қайтару бойынша рәсімдерді анықтайды. Үлкен корпоративтік жүйеде түрлі саясатардың кең ауқымы қолданыла алады: бизнес-саясаттардан мәліметтер жиынына қатынау арнайы ережелерге дейін. Бұл саясаттар ұйымның нақты талаптарымен анықталады.

Өзін-өзі бақылау сұрақтары:

1. Ақпараттың қауіпсіздігі – бұл:
a) ақпаратты енгізудің, сақтаудың, өңдеудің және таратудың оның ағылып кетуі, бұзылуы болмайтын жағдайларды жасау;
b) ақпаратты қорғаудың әлсіз бөлімін аса беріктісіне алмастыру;
c) ақпаратты қорғаудың әлсіз бөлімін бір немесе одан да көп бөгеттермен қайталау;
d) оның сейфте сақталынуы;
e) міндетті түрде шифрлау.

2. Қауіпсіздік саясаты-
a) мекеменің ақпаратты қалайша өңдейтінін, қорғайтынын және тарататынын анықтайтын заңдар, ережелер және тәртіп нормаларының жиыны
b) жүйенің жүзеге асырылуына көрсетілетін сенім өлшемі
c) заңсыз қол жеткізуден немесе оқудан қорғау
d) ақпаратты өз мақсаттарында қолдануға мүмкіндік береді
e) заңсыз қол жеткізуден немесе түрлендіруден қорғайды

3. Кепілділік-
a) жүйенің жүзеге асырылуына көрсетілетін сенім өлшемі
b) мекеменің ақпаратты қалайша өңдейтінін, қорғайтынын және тарататынын анықтайтын заңдар, ережелер және тәртіп нормаларының жиыны
c) заңсыз қол жеткізуден немесе оқудан қорғау
d) ақпаратты өз мақсаттарында қолдануға мүмкіндік береді
e) жүйенің жүзеге асырылуына шаралар тізімі

4. Кепілділіктің түрлері:
a) операциялық және технологиялық
b) кездейсоқ және ойластырылған
c) әкімшілік, ұйымдық
d) кездейсоқ және техникалық
e) оптикалық және талшықты

5. Активті қорғау құралдарының түрлері:
a) ішкі және сыртқы активті қорғау
b) активті және пассивті

c) оң және теріс
d) кездейсоқ және арнайы
e) оптикалық және талшықты

6. Тарихи дәстүрлі жеке меншік құқығы объектісі -
a) материалды объекті болып саналады
b) ақпаратты ұстаушылар немесе иеленушілер болып саналады
c) ақпарат көзі немесе жеткізушілер болып саналады
d) ақпарат қорғаудың түрі болып саналады
e) құқықтық объекті болып саналады

7. Жеке меншік құқығы неше түрлі жеке меншік құқығы элементтерінен тұрады:
a) 3
b) 2
c) 1
d) 4
e) 5

8. Басқару құқығы арқылы –
a) ақпараттың қолданылу аймағын басқарады
b) ақпаратты өзгертілмеген күйде иемденуге құқық береді
c) ақпаратты өз мақсаттарында қолдануға болады
d) ақпаратты кім иемденетінін немесе қолдануын анықтауға болады
e) ақпаратты кім басқаратынын анықтауға болады

9. Иемдену құқығы -
a) ақпаратты кім иемденетінін немесе қолдануын анықтауға мүмкіндік береді
b) ақпаратты өзгертілмеген күйде иемденуге құқық береді
c) ақпаратты өз мақсаттарында қолдануға мүмкіндік береді
d) ақпаратты өзінің жеке мақсатында қолдану үшін иемдену
e) ақпаратты кім иемдену құқығын анықтауға мүмкіндік береді

10. Қолдану құқығы –
a) ақпаратты өз мақсаттарында қолдануға мүмкіндік береді
b) ақпаратты кім иемденетінін немесе қолдануын анықтауға мүмкіндік береді
c) ақпаратты өзгертілмеген күйде иемденуге құқық береді
d) ақпаратты кез-келген мақсатта қолдануға мүмкіндік береді
e) ақпаратты арнайы жұмыстар мақсаттарында қолдануға мүмкіндік береді

11. Ақпаратты құқықтық қорғау-
a) құқықтық негізде ақпарат қорғауды жасақтайтын арнаулы құқықтық актілер, ережелер, процедуралар және шаралар

b) ақпарат өңдейтін техникалық құралдарда жалған ақпарат құруға бағытталған әрекеттер
c) ақпаратпен танысу, оны өңдеу
d) ақпарат қорғаудың мазмұны мен оны ұйымдастыру қимылдарының тәртібі
e) ақпаратқа қатынас құру тәртіптерін өзгерте отырып қатынас құру

12. Қол жеткізуді басқару саясаты -
a) таратылған және рұқсат етілген ақпараттарды пайдалану ережесін ескеруі тиіс
b) таратылған және рұқсат етілген ақпараттарды тарату ережесін ескеруі тиіс
c) таратылған және сақталған ақпараттарды тарату ережесін ескеруі тиіс
d) шифрланған және рұқсат етілген ақпараттарды пайдалану ережесін ескеруі тиіс
e) таратылмаған және рұқсат етілген ақпараттарды пайдалану ережесін ескеруі тиіс

13. ICO стандартына сәйкес келетін қорғау жүйенің жобалануының кезеңдері:
a) жүйедегі өзгерістерді тексеру, тіркеу
b) қол жеткізулік оңтайлығын және жасырындылығын қолдау
c) жүйенің қауіпсіздігін бұзу, жүйедегі өзгерістерді тексеру, тіркеу, жүйедегі қатені анықтау, қателіктерді түзету
d) қауіпсіздікке шабуыл жасауға мүмкіндік тудыратын жағдайды талдау, қорғау жүйесін жоспарлау, қорғау жүйесін жүзеге асыру, қорғау жүйесіне сүйемелдеу
e) қажетті қорғау жүйесін іздеу, жинастыру, пайдасын индентификациялау, аутентификациялау және авторизациялау

14. Қауіпсіздік саясатының дискретті моделінің ерекшелігі
a) сандық ықтималдылықтың бағалау сенімділігі
b) динамикалығы
c) жоғарғы дәрежелі сенімділік
d) реализацияның қарапайым механизмі
e) дұрыс жауап жоқ

15. Компьютерлік қауіпсіздік облысындағы стандарттар системасы жазылған:
a) «Қызыл кітапта»;
b) «Қызғылт кітапта»;
c) «Сары беттерде»;
d) «Жасыл кітапта»;
e) МЕСТ.

10 КОМПЬЮТЕРЛІК ЖЕЛІЛЕРДІҢ ҚАУІПСІЗДІГІ

10.1 Жергілікті желілерді қорғау

Ғимарат ішіндегі мекеменің бөлімдері арасында сенімді ақпарат алмасуды ұйымдастыру және мәліметтер базасын ортақтасып пайдалануға мүмкіндік беретін компьютерлік желіні жергілікті деп атайды:

– локальды желісі зерделеніп, оның функциялары анықталады

– ақпараттың қауіпсіздігін қамтамасыз ету құралдары зерттеледі, таңдалады және әдістері өңделеді

Дербес компьютердегі жұмыстан желідегі жұмысқа көшу келесі себептермен ақпаратты қорғау күрделендіреді:

– желіде пайдаланушылардың үлкен саны және олардың өзгергіш құрамы болады. Пайдаланушының аты және паролі деңгейінде қорғау бөтен адамдардың желіге кіруден қорғамайды;

– желінің маңызды ұзындығы және желіге ену көптеген потенциалды каналдарының бар болауы;

– аппараттық және бағдарламалық қамтамасыз етудегі белгіленген жетіспеушіліктері пайдалану барысында анықталады.

Әрбір желілік жүйенің ерекшелігі, оның компоненттері кеңістікте орналасады, ал олардың арасындағы байланыс физикалық түрде болады және бағдарламалық түрде хабарландыру механизмі көмегімен жүзеге асырылады. Есептеуіш жүйенің объектілерінің арасындағы байланыс желілік байланыс бойынша ауыстыру пакеті ретінде жіберіледі. Желілік жүйелерге жергілікті шабуылдан басқа желілік шабуылдар да жасалады. Олардың ерекшелігі біріншіден, қарақшы шабуыл жасалатын объектіден мыңдаған километр жерде орналасуы мүмкін, екіншіден шабуыл жеке компьютерге емес, желімен берілетін ақпаратқа жасала алады. Жергілікті және ауқымды желілердің дамуына байланысты алыстан шабуыл жасау қолданылуына қарай ең жоғарғы көрсеткіштер көрсетуде.

Қашықтықтан шабуыл деп есептеуіш жүйеге байланыс арнасы бойынша бағдарламалық түрде жүзеге асатын ақпараттық зақым келтіретін әсерді айтады.

Мәліметтерге қауіп техникалық жағынан да келетін болғандықтан, келесі жағдайларды ескеру қажет: сервер сенімділігі, винчестер жұмысының кемшіліктері, қолданылған бағдарламалық жабдықтың кемшіліктері және т.б.

Компьютермен жұмыстан желідегі жұмысқа өту ақпараттық қорғанысты келесі себептер бойынша қиындатады:

1. желінің созылымы және желіге енудің потенциалды арналарының көп болуы;

2. желідегі пайдаланушылардың саны және олардың ауысуы. Құпия сөз және ат қою желіні бөгде адамның кіруінен қорғай алмайды;

3. ақпараттық және бағдарламалық жабдықтардың кемшіліктері, олар қолдану кезінде анықталады.

Үлкен қашықтықты қамтитын желінің коаксикальды кабельді бір сегментінде проблеманың тереңдігін байқау. Желіде ақпаратқа енуге мүмкіндік беретін арналарының көптігі көрінеді. Желідегі барлық құрылғы электромагниттік сәулеленудің көзі болып табылады, себебі сәйкес алаңдар нашар экрандалған. Кабельдік желінің жерде болуы желідегі ақпаратқа енуге рұқсат береді.

Коаксикальды немесе витая пара кабельдерін пайдалану, кабельдік жүйеге физикалық түрде қосылуға мүмкіндік береді. Желіге енетін құпия сөз белгілі болып немесе табылған болса, желіге ену файл-серверден немесе жұмыс станциясынан мүмкін болады. Сонымен қатар, желіден тыс арналардан ақпарат ағып кетуі мүмкін:

1. Ақпарат тасымалдаушылардың қоймасы,

2. Телефон, радио және басқа да сымды және сымсыз арналар (соның ішінде ұялы байланыс арналары).

3. Компьютерлік желідегі ақпаратқа рұқсатсыз енудің арналары мен орындары

Интернет арқылы таралатын желілік шабуылдардың классификациясы:

1. Сниффер пакеттері.

2. IP-спуфинг.

3. Парольді шабуылдар.

4. Қосымшалар деңгейіндегі шабуылдар.

5. Вирустар.

Internet желісінің бірегейлігі қандайда бір физикалық тұлғаның немесе жекеменшік компанияның, мемлекеттің немесе жеке елдің меншігінде еместігі. Сондықтанда іс – тәжірибе жүзінде оның барлық сегменттерінде орталықтан басқару және де басқа ақпараттарға бақылау жасау тәсілдері жоқ. Осының нәтижесінде тәжірибе жүзінде қылмыскерлер қолданатын кез-келген ақпаратқа кіру мүмкіндігі шектелмейді. Internet желісін тек компьютерлік қылмыстың орындалу құралы ретінде қарамай, сонымен қатар әр түрлі қылмыстық іс-әрекеттің енгізілу ортасы деп те айтуға болады.

Internet желісін қолдану қылмыстық іс-әрекетте заң бұзушылар үшін қылмыстық ақпаратты алмасуға шақырады. Бұрын бүкіл әлеммен байланысу барлық державаның тек қана арнайы қызметкерлерінің мүмкіндіктері болды, олар қажетті ғарыштық технология болды. Internet желісінің қылмыскерлер үшін тағыда бір ерекшелігі ауқымды масштабта адамдарға ақпаратты-психологиялық әсер ету. қылмыстық қоғам өзінің доктриндерінің және білімдерінің таралуына көңіл бөледі және қоғамдық ойларды тыңдайды, қылмыстық әлем өкілінің позициясының бекуіне және құқық қорғау органдарының беделін түсіруге жұмыс жасайды.

Бірақ та Internet желісі қылмыстық орындалу құралы ретінде айтарлықтай қызығушылық көрсетті. Ең қарапайым нұсқауы бұл авторлық

құқықты бұзумен байланысты қылмыс. Осындай қылмыс түрлеріне бірінші кезекте иемденуші компанияның серверінде орналасқан бағдарламаны заңсыз көшіру және сату жатады. Қылмыстың екінші тобына тауарды және қызметті ресми емес түрде алу, яғни әртүрлі телефон компаниялары төлейтін қызметті ақысыз пайдалану. Қызметтерді заңсыз пайдаланудың басқа тәсілдерінің негізіне, осы қызметті көрсететін компаниялардың мәліметтер қорынан осы қызмет туралы мәліметтерді модификациялау жатады. Мұндай қылмыстар түріне несиеге алынған зат туралы ақпаратты заңсыз пайдалану немесе оны жойып жіберу, не басқа төленген қызметтің орнына жіберу болып табылады.

Internet желісінде қылмыскерлердің көптеп пайда болуының алғы шарты компьютерлік желінің өсуімен ақпараттың бағалы тауарға айналуы. Әсіресе бұл банк сферасында ақша салу мен ақша салушы мәліметінде, банк пен клиенттің қаржылық жағдайы, банк саясаты аумақтарында кездеседі. Несиелік-қаржылық субъекттің қазіргі кездегі шарттарына байланысты ақпарат алмасудың болуы, және сонымен қатар банктік алшақталған филиалдарымен байланысып отыру үшін Internet желісі қолданылады. Бұл қылмыскерлерге құпия ақпараттарға енуге нақты шанс беріп отыр. қылмыскерлердің бұндай ақпараттарды жойып жіберуі мекememен бәсекелестіктен туындайды. Internet ағымы арқылы орындалатын компьютерлік қылмыстардың қосымша сферасында электронды банктік есептердің шығуымен қылмыста күшейді. Электронды түрдегі ақпаратты алудың әр түрлі тәсілдері бар.

Соңғы кездерде кеш болса да барлық мекемелер өз компьютерлерінің бүкіл әлемдік Internet желісіне шығуға мүмкіндік алғанда қандай тәуекелге баратынын түсінді. Олар қаскүнемдердің барлық ұсталары (мамандандырылған бұзушылар және ұрылар, кекті бағынушылар немесе бәсекелестер) алдында тәуекелге барады және де оларды төмендегідей метериалдық шығынға ұшыратады. Нәтижесіде компьютерлік желілердегі ақпаратты қорғауда, нақты құралдарды таңдау негізгі рөл ойнайды.

– Компьютерлік жүйеде сақталған ақпараттың бағалылығын анықтау;

– Қаскүнем компьютерлік жүйенің қорғанысын жеңу үшін қолданылатын уақыттың және қаржылық шығын базасы;

– Компьютерлік жүйеге шабуылдаған кездегі қаскүнем қылығының ықтималдық моделі;

– Ұйым үшін компьютерлік жүйені адекватты қорғауға қажетті уақыттың және қаржылық шығын базасы.

Бүтіндей ақпаратты қорғауды қамтамасыз ету құралдарын орындау тәсілі бойынша қасақана әрекеттерді қақпайлау мына топтарға бөлуге болады:

1) техникалық (аппараттық) құралдар.

Техникалық құралдардың артықшылығы олардың сенімділігі, субъективті факторлардан туәелсіз, модификацияға биік тұрақтылығы.

Әлсіз жақтары – иілгіштігі төмен, салыстырмалы көлемі және салмағы үлкен, құны жоғары.

2) бағдарламалық құралдар – пайдаланушыларды сәйкестендіру, қол жеткізуді бақылау, ақпаратты шифрлау, қалған (жұмысшы) уақытша файлдан ақпаратты өшіру, қорғау жүйелерін тестілік бақылау бағдарламаларынан құралады.

Бағдарламалық құралдардың негізгі артықшылықтары:

- әмбебаптық, иілгіштік, сенімділік,
- құруы қарапайым,
- модификацияға және дамуға қабілеттіліктері.

Кемшіліктері:

- желінің функционалдылық шектелуі,
- файл-сервер және жұмысшы станциялардың ресурстарының бір бөлімін қолдану,
- кездейсоқ немесе қасақана өзгертуге биік сезгіштік, компьютерлердің үлгісіне тәуелділігі

Ұйымдық құралдар

3) ұйымдық құралдар: ұйымдық - техникалық (компьютерлер орналастыру, кабелдік жүйе салу) ұйымдық-құқықтық құралдардан тұрады.

Олардың артықшылықтары: әр текті проблемалардың жиынын шешуге мүмкіндік етеді, орындауы қарапайым, желідегі жағымсыз әрекеттерге жылдам сезінеді, модификация және даму мүмкіншіліктері шектелмеген.

Кемшіліктері: жалпы ұйымдардағы субъективті факторларға биік тәуелділігі.

10.2 Корпоративтік желілерді қорғау

Корпоративтік желілерде өңделетін ақпарат өте осал болып табылады. Қазіргі уақытта мәліметтерді рұқсатсыз пайдалану немесе өзгерту, айналымға жалған ақпаратты енгізу мүмкіндіктерін елеулі түрде жүзеге асыруға:

– Компьютердегі өңделетін, жіберілетін және сақталатын ақпарат көлемінің көбеюі;

– Маңыздылығы мен құпиялылығы әртүрлі деңгейдегі ақпараттық мәліметтер базасында шоғырлануы;

– Мәліметтер базасында сақталатын ақпаратқа және есептеу желісінің қорларына қатынайтын пайдалануышлар аясының кеңеюі;

– Қашықтағы жұмыс орындары санының көбеюі;

– Байланыс үшін пайдаланушылардың Интернет жаһандық желісін және әртүрлі байланыс арналарын кеңінен пайдалануы;

– Пайдаланушылардың компьютерлері арасында ақпарат алмасудың автоматталуы мүмкіндік туғызады.

Ең алдымен, нені қорғау және кіммен немесе неден қорғау керектігін анықтауға, содан кейін қорғауды қалай қамтамасыз етуге болатынын шешуге ұмтылып көреміз.

Кез келген корпоративтік желінің негізгі міндеті қажет ақпаратты пайдаланушыға қай жерде болса да және барынша өте қысқа мерзімде жеткізу болып табылады. Ақпаратты қорғау жүйесі корпоративтік желінің негізгі қызметін – қызметтік ақпаратты уақытында айырбастауды тиімді орындауға мүмкіндік туғызады. Кез келген корпоративтік желінің базисі жалпы жүйелік бағдарламалық қамтамасыздандыру болып табылады, оның құрамында әртүрлі амалдық жүйелер, бағдарламалық қабықтар, жалпы жүйелік бағдарламалар, мәтіндік процессорлар, редакторлар және интеграланған бағдарлама дестелері, мәліметтер базасын басқару жүйелері болады.

Ақпаратты өңдеу үдерісінде мәліметтерді өңдеу, сақтау және жіберу әртүрлі техникалық құралдары жұмыс істейді. Ақпарат автоматтандырылған жұмыс орнынан ішкі және сыртқы байланыс арналары арқылы түсуі мүмкін, мұнда ол пернетақта арқылы да, сыртқы ақпарат тасымалдаушысынан да енгізіледі. Сонымен қатар желіде кейде басқа мекемелер мен ұйымдардың және жаһандық телекоммуникациялық желілердің ақпараттық қорлары пайдаланылады. Жаһандық телекоммуникациялық желілер тұтынушыларға ақпаратты жіберу үшін қатынас ортасы ретінде қолданылады.

Корпоративтік желінің пайдаланушысы деп белгіленген тәртіппен тіркелген адамдарды (ұйымдарды) түсінуге болады, оларға желіде нақты қатынау өкілдері үлестіріліп беріледі. Пайдаланушы өз өкілдіктері шеңберінде жалпыжүйелік және қолданбалы бағдарламалық қамтамасыздандыруды пайдаланы, тек рұқсат етілген іс-қимылдарды жүзеге асыра алады.

Желіде ақпаратты өңдеу жүйе әкімшісінің бақылауымен орындалады, ал оны қорғау өз қызметін арнайы жұмыс орнында орындайтын қауіпсіздік әкімшісінің басқаруында болады. Бұл орындар өңделетін ақпаратқа әрқашан қатынауға мүмкіндік бермейді, бірақ әрдайым оны өңдеу үдерісіне ықпал жасауға мүмкіндік туғызады.

Корпоративтік желіні әртүрлі аппараттық – бағдарламалық ішкі жүйелерден тұратын жүйе түрінде көрсетуге болады, мұнда басқарушының жұмыс орны, қашықта орналасқан жұмыс орыны, жүйе қауіпсіздігі әкімшісінің жұмыс орны кіреді, бұлардың әрбіреуі біршама тәуелсіз болады. Мұндай ішкі жүйеге жалпы жүйенің белгілері өзіне тән келеді. Сондықтан мұнда ақпаратты қорғау тұрғысынан декомпозиция

принципін қолданылады. Осы принципке негізделген ақпарат қауіпсіздігі қатеріне ықпал жасау тетігі жүйеге толық, сондай-ақ жекелеген ішкі жүйеге де қолданылады.

Жасалған талдау негізінде корпоративтік желіде таралған ақпаратқа қауіп төндіретін барлық көздерді:

– Субъекті іс-қимылына негізделген қауіптер (антропогендік);
– Техникалық құралдарға негізделген қауіптер (техногендік);
– Стихиялық көздерге негізделген қауіптер деп үш негізгі топқа бөлуге болады. Компьютерлік қылмыстар аясында әртүрлі мамандардың жүргізген талдауы негізінде қауіпсіздік қатерінің біліну жиілігіне байланысты:
– Бағдарламалық қамтамасыздандыруды ұрлау;
– Ақпаратты әдейі ауыстыру;
– Ақпарат тасымалдаушыларынан мәліметтерді жою;
– Вирустық щабуыл нәтижесінде қалыпты жұмысты бұзу;
– Ақпарат тасымалдаушыларындағы мәліметтерді өзгерту;
– Ақпаратты ұстап қалу;
– Қорларды ұрлау;
– Байланыс арналарының қалыпты жұмысын бұзу;
– Алдын ала болжанбаған жоғалулар деп орналастырамыз.

Ақпарат қауіпсіздігінің қатерлерін білудің салдары ең ақырында:

1. Бағдарламалық, аппараттық немесе бағдарламалық-аппараттық ақпаратты өңдеу құралдары немесе қорғау жүйелерінің бұзылуынан, сонымен қатар форс-мажорлық жағдайлардан, бәсекелестердің, мекеменің немесе оның филиалдарының қызметшілерінің, қылмыстық элементтер немесе үшінші адамдардың мүдделері үшін ақпаратты өңдеу құралдарымен жабдықтаушылардың әсерін тигізетін арнайы техникалық, бағдарламалық құралдарды қолдануынан ақпараттың жойылуы;

2. Бағдарламалық, аппараттық немесе бағдарламалық-аппараттық ақпаратты өңдеу құралдары немесе қорғау жүйелерінің бұзылуының, сонымен қатар форс-мажорлық жағдайлардың, бәсекелестердің, мекеменің немесе оның филиалдарының қызметшілерінің, қылмыстық элементтер немесе үшінші адамдардың мүдделері үшін ақпаратты өңдеу құралдары мен жабдықтаушылардың әсерін тигізетін арнайы бағдарламалық құралдарды қолдануының салдарынан ақпараттың өзгеруі немесе бұрмалануы;

3. Байланыс тораптарына немесе техникалық құралдарға қосылу жолымен, қосымша электромагниттік сәулелердің сигналдарын алу немесе мағынасын ашу, суретке түсіру, ақпарат тасымалдаушыларына ұрлық жасау, мекеменің немесе оның филиалдарының қызметшілерін параға сатып алу немесе бопаслау, бәсекелестердің мекеме қызметшілерінің немесе қылмыстық элементтердің құпия сөйлесулерді тыңдау, рұқсатсыз

ақпарат көшірмесін жасау, басқа пайдаланушылардың мәліметтерін оқу, автоматтандырылған жүйеге қызмет етуші қызметшілердің тіркелген пайдаланушысы түрінде алдауы, жасырынуы, бағдарламалық тұзақ көмегімен ақпарат алу есебінен ақпаратты ұрлау;

4. Үшінші адамдардың мүдделлері үшін ақпаратты өңдеу құралдарымен жабдықтаушылардың жүзеге асыратын немесе мекеме қызметшілерінің жүргізетін ақпаратпен айла - шарғысы нәтижесінде ақпарат иесінің құқығына қысым жасатуы немесе материалдық шығынға ұшыратуы мүмкін. Сонымен қатар электрондық қолды жалған жасауы немесе қабыл алмауы мүмкін.

Аппараттық–бағдарламалық құралдар көбінесе, тікелей ақпаратты өңдеу және жіберу үдерісімен байланысты қауіптерді жоюға бағытталған. Бұл құралдарсыз ақпараттық қауіпсіздік толық кешенді жүйесін құру мүмкін болмайды.

Ақпаратты қорғаудың кешенді жүйесін жасаудың негізгі принциптерінің бірі ең жоғары *достық принципі* болуы керек. Басқаша айтқанда, өтіп кетуге мүмкіндік болса, тыйымды енгізбеу керек, ал егер шек қою қажет болса, онда қалай пайдаланушыға өте аз ыңғайсыздық жасауға болатындығын басынан ойлану қажет. Сонымен қоса корпоративтік желінің амалдық және бағдарламалық - аппараттық құрылымын және фирманың қалыптасқан дәстүрлерін пайдаланып құрастыратын қорғаудың кешенді жүйесінің үйлесімді болуын ескерту керек.

Бұл мәселе өте жақын *ашықтық принципі* тұр. Корпоративтік желіні тек қана жоғары сыныпты бағдарламалаушылар пайдаланбайды. Сонымен қатар корпоративтік желінің негізгі міндеті пайдаланушылардың өндірістік қажеттілігін, яғни ақпаратпен жұмыс істеуін қамтамасыз ету болып табылады. Сондықтан, ақпараттық қорғау жүйесі «фондық» режимде жұмыс істеуі қажет, «байқалмайтын» және пайдаланушының негізгі жұмысына кедергі жасамайтын, бірақ оған жүктелген барлық қызметті мүлтіксіз атқаруы керек.

Ескерту принципі. Ақпарат қауіпсіздігіне қауіп төндіру салдары ақпаратты қорғаудың кешенді жүйесін жасауға кеткен шығындармен салыстырғанда қаржылық, уақыттық және материалдық анағұрлым көп шығындарды қажет ететіндігі әрқашан есте болуы керек.

Оңтайлылық принципі. Ақпарат қауіпсіздігіне қауіпті амалдаудың әртүрлі әдістері мен тәсілдерінің арақатынасын оңтайлы таңдау, шешім қабылдағанда ақпаратты қорғау жүйесін жасау шығындарын едәуір дәрежеде азайтуға мүмкіндік береді.

Жүйелік принципі. Қорғау жүйесін қарастыруда бұл принцип ақпарат қауіпсіздігіне қауіпті амалдау бойынша шаралар кешенін желіні жобалау кезеңінде қарастырылады, бұл ақпаратты қорғаудың ұйымдық және инженерлік-техникалық шаралардың оңтайлы қиылысуына мүмкіндік

береді. Бұл принциптік жүзеге асуының маңыздылығы мынады: жұмыс істеуші қорғалмаған корпоративтік желіні ақпараттық қорғау құралдарымен жабдықтауды бастапқы жобалау және қорғалған нұсқада тұрғызудан күрделі және қымбат болады.

Бейімділік принципі. Ақпаратты қорғау жүйесі желінің пішін үйлесімі, пайдаланушылар саны, құпиялық дәрежесі және ақпарат құндылығының өзгеру мүмкіндігін есепке алып құрылуы қажет. Мұнда желіге жаңа элементті енгізу немесе іс-әрекеттегі жағдайларды өзгерту корпоративтік желінің тұтас алғанда, қол жеткен қорғау деңгейін төмендетпеуі керек.

Дәлелдік принципі. Ақпаратты қорғау жүйесін жасауда корпоративтік жүйенің ішінде ұйымдастыру шараларын логикалық және физикалық жұмыс орындарын бір біріне байланыстыра орындау, сонымен қатар арнайы аппараттық – бағдарламалық сәйкестендіру, бірегейлендіру құралдарын қолдану және ақпараттық түпнұсқалығын растау қажет. Бұл принципті жүзеге асыру жүйені күрделендіру шығындарын азайтуға мүмкіндік береді, мысалы, цифрлық электрондық қол қоюды тек корпоративті желімен байланыс арнасы арқылы қосылған қашықтағы, сыртқы жұмыс орындары мен терминалдармен жұмыс істегенде ғана қолдау. Бұл принцип корпоративтік желі қауіпсіздігін қамтамасыз ету бағытын, ақпаратты қорғау функциялары мен шараларын таңдау кезінде негізге алынуы қажет.

Ақпараттық қауіпсіздік ішкі жүйесін құрудың негізгі кезеңдерін қарастырайық. Бірінші кезеңде бар немесе жүзеге асыру жоспарланған корпоративтік жүйенің қорғалуына сараптау жүргізеді, мұнда әуелі құпиялылық дәрежесі бойынша қолдануда компанияның ақпараттыө қорларына айқын сыныптау жүргізу ұсынылады. Бұл мәселені, әдетте, ұйымдастыру әдістерімен де, техникалық құралдармен де шешуге болады, бірақ ең тиімді тәсіл кейбір тұжырымдалған шешімді қолдану болып табылады.

Бұл кезде ұйымды интернетке қосуда мүмкін болатын КЖ қауіптер мен тәуекелділікке талдау жасалады. Ұйымды Интернетке қосу тәуекелділігін талдау осал жерлерді анықтау, қауіп төну ықтималдығын бағалау, оның жүзеге асуынан болған материалдық шығын, қауіптен пайда болған тәуекелділікті қауіптен пайда болу ықтималдығы мен оны болдырмауға қажет және жеткілікті қорғау шараларының шығынына көбейтіп есептеуді қамтиды. Тәуекелділікті талдау үдерісін автоматтау үшін арнайы бағдарламалық десте бар. Талдау нәтижесі келесі кезеңнің орындалуының негізі болып табылады.

Екінші кезеңде КЖ ақпараттық қауіпсіздігінің тұжырымдамасы мен саясаты әзірленеді. КЖ-де көптеген қорғау құралдарының аймақтарда орналасуы, орталықтан басқаруды қажет етеді. Қауіпсіздік құралдарымен

орталықтан басқару қауіпсіздіктің бірыңғай жаһандық саясаты болуын жобалайды.

Қауіпсіздік саясаты КЖ ақпараттық қорларын қорғау үдерісінің ерекшелігін анықтайды және қауіпсіздік ережелерінің екі түрінің көмегімен нақтылайды:

– серверлер, жұмыс станциялары, байланыс арналары, мәліметтер базасы, жекелеген файлдар, амалдық жүйе қорлары сияқты ақпараттық нысандарға қатынау процедураларын бағындыру ережелері. Бұл ережелер әдетте, жадқа жүктелетін желілік құрылғыларға - маршруттаушылар, жұмыс станциялары, коммутаторлар, серверлер, мамандандырылған қорғау кешендері және т.б. қатынау тізімі түрінде дайындалады. Бұл түрдегі қауіпсіздік ережелерін жүзеге асыру үшін өте жеткілікті аспаптық құралдар әзірленген, олар пайдаланушылық деңгейде қауіпсіздік ережелерінің сақталу үдерісін бақылайды;

– желілік дестелердің мазмұнын талдауға байланысты ережелер, сәйкес желілік мониторинг құралдарын және қаскүнемнің басып кіруін білу құралдарын баптау. Техниалық жағынан бұл мәселе күрделі, сондықтан жеткілікті түрде жетілдірілген аппараттық және бағдарламалық қорғау құралдарын пайдалануды қажет етеді.

Үшінші кезеңде ақпараттық қауіпсіздіктің ішкі жүйесіне қойылған мәселелерді ойдағыдай шешуге мүмкіндік беретін ұйымдастыру шараларымен бірге тікелей техникалық құралдарды таңдауға кірісу қажет.

Ең басты фактор - негізгі принципке сәйкес қауіпсіздік мен күрделілік арасында баланс орнату: жүйе күрделі болған сайын ол осал және жасауға қиын. Күрделі жүйелерді лайықты түрде көрсету қиын, ал әртүрлі дәлсіздік қауіпсіздік мәселелерінің тууына әкеліп соғады.

Нақтылы өндірушінің нақтылы ақпаратты қорғау жүйесін (АҚЖ) ақтық таңдауда өнімге қойылатын базалық талаптардан басқа:

– осы АҚЖ жылдамдығы;

– сәйкестік сертификатының болуы сияқты екі критерийге көңіл бөлу қажет.

АҚЖ жылдамдығы туралы талап көбінесе, желіаралық әрекеттесуді қорғау құралдарына қойылады, өйткені осы жерде, қағида бойынша, ақпаратты өңдеу жылдамдығына қатаң талап пайда болады. Ең алдымен, бұл ақпаратты криптографикалық түрлендіру әдісін қолданатын АҚЖ-ға қатысты, өйткені уақыттың нақты масштабында трафикті мұндай өңдеу алдын ала бағалауға қажет байыпты есептеу қорларын талап етеді.

Ақпараттық қауіпсіздіктің ішкі жүйесін тиімді жобалауда ақпараттық қауіпсіздікті қамтамасыз етудің бірнеше жалпы принциптерін ескеру қажет. Бұл принциптерге мыналар жатады:

– экономикалық тиімділік - мүмкін болатын зиян мөлшеріне қарағанда, қорғау құралдарының құны төмен болуы керек;

– артықшылық минимумы - әрбір пайдаланушы жұмыска қажет ең төмен артықшылық жиынына ие болуы керек;

– қарапайымдылық - қорғау тиімді болады, егер онымен пайдаланушының жұмыс істеуі жеңіл болса;

– қорғаудың ағытылуы - қорғау қалыпты жұмыс істегенде ағытылмау керек, тек ерекше жағдайларда арнайы өкілеттігі бар қызметкер қорғау жүйесін ағыта алады;

– қорғау тетігін жобалау және қызметінің ашықтығы - қорғау жүйесіне қатысы бар мамандар оның өызмет істеу принциптерін толық меңгеруі керек және қиын жағдайлар туындаған кезде оларға барабар әрекет етуі қажет;

– жалпы бақылау - қорғалатын субьектілер мен объектілердің бақылану жиынынан кез келгенін алып тастау, ақпаратты өңдеуді автоматтау кешенінің қорғалымдылығын төмендетеді;

– қорғау субъектілерінен қорғау жүйесінің тәуелсіздігі - қорғау жүйесін әзірлеумен шұғылданатын адамдар, бұл жүйені бақылайтындардың ішінде болмауы керек;

– есеп беруші және бақылауда болу - қорғау жүйесі өз жұмысының дұрыстығына дәлелдеу беруі керек;

– жауапкершілік - ақпарат қауіпсіздігін қамтамасыз етумен шұғылданатын адамдардың дербес жауапты болуы;

– оқшаулау және бөлектеу - қорғау нысандарын топтарға бөлу лайықты болады, мұнда бір топтағы қорғаудың бұзылуы басқасының қауіпсіздігіне ықпал жасамау керек;

– толық және келісімділік - сенімді қорғау жүйесінің толық өзгешеліктері анықталған, тестіден өткізілетін және келісілген болуы керек;

– параметрлеу - қорғау өте тиімді және икемді болады, егер әкімші жағынан оның параметрлерін өзгертуге мүмкіндік болса;

– шабуылшы қоршау принципі - қорғау жүйесін жобалауда шабуылшы қоршауы болады деп есептеу керек. Құраушылар пайдаланушылардың ниеті өте нашар болатын, маңызды қателер жасайды, қорғау тетігін елемеу жолдарын іздейді деген ұйғарымды негізге алуы қажет.

– адамды қатыстыру - ең маңызды және өте қиын шешімдерді адам қабылдауы керек;

– қорғау тетіктерінің болуы туралы артық ақпарат болмауы - ол туралы мүмкіндігінше пайдаланушылардан жасыру қажет, өйткені олардың жұмысы бақылауда болуы керек.

Кәсіпорын масштабының желілік қауіпсіздік жүйесін басқарудың негізгі міндеттерін тұжырымдайық. Кәсіпорын масштабының бөлінген

желілерінде ақпараттарды қорғаудың басқару жүйесі функционалдық тұрғыдан мына міндеттерді шешуі тиіс:

– кәсіпорын желілерінің шеңберінде ауқымды қауіпсіздік саясатын басқару, жекелеген құрылғылардың жергілікті қауіпсіздік саясатын ақпараттарды қорғаудың бүкіл құрылғыларына дейін жеткізу;

– қатынау объектілері мен субъектілерін конфигурациялауды басқару; құрылғылар құраушыларын, версияларды, құрамды басқару, қорғауды бағдарламалық қамтамасыздандыру, сондай-ақ пэтчаларды (patch) басқару кіреді.

– бөлінген қолданбалы жүйелерге қорғау сервистерін беру, сондай-ақ қорғалған қосымшалар мен олардың қорларын (ресурстарын) тіркеу. Осы топ қосымшалары, ең алдымен, қолданбалы жүйелер тарапынан қорғау сервистерімен басқаруды қамтамасыз ету үшін интерфейсті (API) қамтамасыз етуі тиіс.

– криптоқұралдармен басқару, жекелей алғанда, кілтпен басқару (кілттік инфрақұрылым). Кілттік инфрақұрылым инфрақұрылымдық (өзін-өзі құратын) қызметтердің құрамында жұмыс істеуі тиіс;

– оқиғаны хаттамалау; әртүрлі құрылғыларға логтар беруді баптау, логтардың егжей - тегжейлік деңгейін басқару, хаттамалау жүргізетін, оқиғалар құрамын басқару;

– ақпараттық жүйелердің қауіпсіздік аудиті; ақпараттық жүйелердің қорғаушыларының ағымдағы жай күйі туралы объективті мәліметтер алу мен оны бағалауды қамтамасыз етеді, кейбір уақытта, логтарды талдау, жұмыс істеп тұрған жүйедегі бұзушылар мен жыртықтарды іздеу қауіпсіздік аудиті болып түсіндіріледі;

– жүйенің қауіпсіздік мониторингі, құрылғылардың жай-күйі, белсенділігі туралы және құрылғыларда болып жатқан қауіпсіздік контексімен, мысалы, әлеуетті шабуылдар туралы, нақты уақыттағы ақпараттарды алуды қамтамасыз етеді;

– арнайы қорғалған қосымшалар жұмысын қамтамасыз ету, мысалы, операцияларды нотариалдық қадағалау, күнтәртібіндегі іс-шараларды қолдау (кілттерді, парольдерді, қорғау құрылғыларын ауыстыру, смарт-карталар шығару және т.б.);

– қосымшалардың жобалау - түгендеу топтарының жұмысын қамтамасыз ету; қосымшалардың осы тобы:

– кәсіпорын желілерінде қорғау құралдарын орнатудың нүктелерін анықтауды;

– қолданылатын қорғау құралдарын есепке алуды;

– қорғау құралының модульдік құрамын бақылауды;

– қорғау құралдарының жай-күйін бақылауды жүзеге асыруы тиіс.

Желілерде ақпараттарды қорғау құралдарының басқару жүйелері мен желілерін басқарудың дәстүрлі жүйелерінің өзара әрекеттерін

ұйымдастыруда проблемалар бар. Осы проблемаларды шешу үшін екі негізгі тәсілдеме қолданылады.

Ұйымдастырушы құралдары ұйымдастырушы-техникалық (бөлімдерді компьютермен жабдықтау, кабельді жүйелерді дайындау т.б.) және ұйымдастырушы-құқықтық (ұлттық заңнама және белгілі бір кәсіпорын басшысы бекіткен жұмыс жасау ережелері) құралады.

Ұйымдастырушы құралдардың артықшылығы – олар көптеген әр типтегі проблемаларды шешуге мүмкіндік береді, жүзеге асыруда қарапайым, желідегі қажетсіз әрекеттерге тез жауап береді, даму мен түрлендіру мүмкіндігі шектеусіз.

Кемшілігі – субъектілі факторға тәуелділігі жоғары, соның ішінде нақты бөлімшелердегі жалпы ұйымдастыру жұмысы.

Ал қалған құралдар ақпаратты қорғаудың қосымша деңгейін қамтамасыз ету қажет болған кезде ғана қолданылады.

Өзін-өзі бақылау сұрақтары:

1. Қызмет көрсетуге қатысты – OSI моделінің көрсеткіші
a) қолданбалы
b) транспортты
c) сеанс
d) физикалық
e) дұрыс жауап жоқ

2. OSI моделінің төменгі деңгейі:
a) сеанстық
b) физикалық
c) қолданбалы
d) желілік
e) арналық

3. Дәл осы уақытта қай жақ активті екенін тіркейтін және өзара байланысты басқаратын деңгей
a) физикалық
b) қолданбалы
c) көліктік
d) желілік
e) сеанстық

4. Маршрутизаторлар жұмыс жасайтын OSI моделінің деңгейі
a) көліктік
b) арналық
c) қолданбалы
d) бірігу
e) желілік

5. Желілік адаптермен желілік топсымның жалғану тәсілін анықтайтын деңгей
a) бірігу
b) желілік
c) көліктік
d) физикалық
e) арналық

6. OSI моделінің деңгейлері
a) көліктік, желілік, физикалық, қолданбалы, арнайы
b) арналық, көліктік, желілік, физикалық, желілік
c) желілік, физикалық, қолданбалы, жалпы,
d) физикалық, желілік,маршруттық, арналық,сеанстық, ұсынылатын, қолданбалы
e) физикалық, арналық, желілік, көліктік, сеанстық, ұсыныс, қолданбалы

7. OSI моделінде кадрлар құрылатын деңгей
a) көліктік
b) физикалық
c) қолданбалы
d) желілік
e) арналық

8. Физикалық деңгейдегі өңделмеген биттерді берілгендер кадрына топтайтын деңгей
a) көліктік
b) желілік
c) сеанстық
d) қолданбалы
e) арналық

9. Берілгендер ағымында бақылау нүктелер қою арқылы пайдаланушының тапсырмаларының синхрондалуын қамтамасыз ететін деңгей
a) желілік
b) сеанстық
c) қолданбалы
d) көліктік
e) арналық

10. Қауіпсіздік саясаты – бұл:
a) ақпаратты тарату және қорғау тәсілдерін анықтайтын заңдардың, жүріс- тұрыс ережелері мен нормалардың жиынтығы;
b) жүріс-тұрыс нормасы;

c) ақпаратты жасыру;
d) енуге рұқсатпен мәжбүрлі басқару;
e) енуге рұқсатпен еркін басқару.

11. Ақпараттың жойылуына әкеп соқтыратын қатерлер -
a) кездейсоқ және ойластырылған
b) техникалық және тораптық
c) әкімшілік, ұйымдық
d) кездейсоқ және техникалық
e) мақсаттық және техникалық

12. Тәсіл - бұл
a) белгілі бір мақсатқа жетудің әрекеттерінің реті және әдістері
b) бір нәрсе жасауға арналған ережелер жиынтығы
c) белгілі бір есеп шешудің тәсілі
d) белгілі жұмысты шешу үшін қолданылатын әдіс
e) белгілі бір мақсатқа жетудің әрекетерінің тізімі

13. Хаттама-
a) бірнеше жақпен орындалатын іс-әрекет тізбегі
b) ашық мәтін символдары алдыңғы n символға байланысты шифрлайды
c) кездейсоқ екілік тізбек болып табылатын кілт қолданады
d) мәтіндерді блоктарға бөліп оларды бір бірден ретімен шифрлайды
e) ақпарат алмасушы құрал

14. Криптографиялық хаттама-
a) құрамында криптография қолданылған хаттама
b) құрамында математикалық символдар қолданылған хаттама
c) ақпараттарды түрлендіріп екінші жаққа жеткізу жұмысын атқарады
d) идентификациялық нөмірлерді қамтиды
e) кездейсоқ екілік тізбек болып табылатын кілт қолданады

15. «Қызғылт кітапта» сенімділіктің (қауіпсіздіктің) қанша деңгейі анықталады?
a) 4
b) 2
c) 10
d) 5
e) 7

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

АА – ақпараттық ағындар

АЖ – ақпараттық жүйе

АҚ – ақпараттық қауіпсіздік

АҚЖ – ақпараттық қауіпсіздік жүйесі

МББЖ – мәліметтер базасын басқару жүйесі

ҚА – құпия ақпарат

ОЖ – операциялық жүйе

СО – сертификаттау орталығы

ЭЦҚ – электронды цифрлық қолтаңба

ГЛОССАРИЙ

Авторизация – ақпараттық өзара байланыстың белгілі бір қатысушысы үшін құқықтық профилін қалыптастыру.

Ақпаратты қорғау – ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені.

Ақпараттық қауіпсіздік – мемлекеттік ақпараттық ресурстардың, сондай-ақ ақпарат саласында жеке адамның құқықтары мен қоғам мүдделері қорғалуының жай күйі.

Асимметриялық жүйе – ашық кілтті криптожүйелер деп те аталады. Бұл жүйеде мәліметтерді шифрлау үшін бір кілт, шифрды ашу үшін басқа кілт қолданылады.

Аутентификация - ақпараттық өзара байланыс қатысушысының дұрыс анықталуына сенімділікті қамтамасыз ету.

Блоктық шифрлар – шифрланатын мәтіннің бөлігіне қолданылатын түрлендірудің негізгі әдістерінің тізбегі.

Гаммалау (gamma xoring) – белгілі бір заңға сәйкес шифрдың гаммасын ашық мәліметтердің үстіне салу (беттестіру) үрдісі.

Гаммалау арқылы шифрлау – шифрланатын мәтіннің символдары шифр гаммасы деп аталатын кейбір кездейсоқ тізбек символдарымен қосылады.

Әліпби – ақпаратты кодтау үшін пайдаланылатын таңбалардың шектеулі жиынтығы

Жасырындылық – заңсыз қол жеткізуден немесе оқудан қорғау.

Идентификатор - берілген жүйеде объектіге немесе субъектіге сәйкес келетін символдар жиынтығы.

Идентификация - ақпараттық өзара байланыс үрдісінің қатысушысын, оған қандай да бір ақпараттық қауіпсіздік аспектілерін қолданбай тұрып тану.

Кілт – ақпаратты шифрлау және кері шифрлау, сондай-ақ оған қол қою үшін арналған цифрлық код.

Криптоанализ – ақпаратты оның кілтін білмей-ақ қалайша кері шифрлау мәселесімен айналысады.

Криптография – құпияжазу, ақпаратты заңсыз пайдаланушылардан қорғау мақсатымен оны түрлендіру әдістері жайындағы ғылым.

Криптографиялық алгоритм – шифрлау және кері шифрлау үшін қолданылатын математикалық функция.

Криптожүйе – шифрлау алгоритмі, сондай-ақ алуан түрлі кілттердің, ашық және шифрланған мәтіндердің жиынтығы.

Криптология – ақпаратты оны түрлендіру арқылы қорғаумен шұғылданатын ғылым.

Пароль – ұсынылатын идентификаторға субъектінің сәйкестігін растауға мүмкіндік беретін құпия символдар жиынтығы.

Профиль - берілген объект пен субъект үшін параметрлер мен конфиғурациялар жиынтығы және оның АЖ-дегі жұмысын анықтау.

Тұтастылық – хабарды алушы алынған хабарда оны жіберу кезінде жолай қандайда болмасын өзгеріс енгізілдіме, жоқпа соны тексере алады.

DES стандарты – АҚШ-тың Ұлттық стандарттар бюросы жариялаған шифрлау стандарты.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Баранова Е.К. Информационная безопасность и защита информации / Е.К. Баранова, А.В. Бабаш. – М. : Инфра-М, 2017. – 324 с.
2. Нестеров С. Основы информационной безопасности. Учебное пособие / С. Нестеров. – СПб. : Лань- Петербург, 2009. – 324 с.
3. Нестеренко А. Криптографические методы защиты информации : учебник / А. Нестеренко, М. Рожков. – М. : КноРус, 2016. – 192 с.
4. Фомичёв В. Криптографические методы защиты информации. Часть 1 и 2. / В. Фомичёв, Д. Мельников. – М. : Издательство Юрайт, 2017. – 454 с.
5. Партыка Т.Л. Защита информации в персональном компьютере / Т.Л. Партыка, И.И. Попов, Н.З. Емельянова. – М. : ФОРУМ, 2010. – 368 с.
6. Платонов В.В. Программно-аппаратные средства защиты информации / В.В. Платонов. – М. : Издательский центр «Академия», 2013. – 336 с.
7. Мельников В.П. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М. : Издательский центр «Академия», 2012. – 336 с.
8. Зайцев А. Технические средства и методы защиты информации. 7-е издание. / А. Зайцев, Р. Мещеряков. – М. : Горячая линия-Телеком, 2012. – 442 с.
9. Аяжанов Қ.С. Ақпараттық қауіпсіздік және ақпаратты қорғау : оқулық. / Қ.С. Аяжанов, А.С. Есенова. – Алматы : ЖШС РПБК «Дәуір», 2011. – 376 б.
10. Ярочкин В.И. Информационная безопасиость : учебник для студентов вузов / В.И. Ярочкин. – М. : Академический Проект, 2010. – 544 с.
11. Адаменко М. Основы классической криптологии. Секреты шифров и кодов / М. Адаменко. – М. : ДМК-Пресс, 2012. – 256 с.
12. Климентьев К. Компьютерные вирусы и антивирусы: взгляд программиста / К. Климентьев. – М. : ДМК-Пресс, 2013. – 656 с.
13. Левин М. PGP: Кодирование и шифрование информации с открытым ключом / М. Левин. – М. : Бук-пресс, 2010. – 166 с.
14. Шаньгин В. Информационная безопасность компьютерных систем и сетей / М. : Инфра-М, 2011. – 416 с.