Оқу-әдістемелік үдерісте және киберкеңістіктегі жұмыста ақпараттық қауіпсіздікті қамтамасыз ету бойынша ұсыныстар

Ақпараттық қауіпсіздікті қамтамасыз ету, тұтастай алғанда, заңмен қорғалатын жеке және іскерлік сипаттағы ақпаратты қорғау, осы бағытта әкімшілік, ұйымдастырушылық, тәрбиелік және құқықтық сипаттағы тиісті шаралар жүйесін іске асыруды көздейтін кешенді міндет болып табылады. Ақпараттық қауіпсіздік мәселелері қоғамның барлық салаларына деректерді өңдеу мен берудің техникалық құралдарының, ең алдымен есептеу жүйелерінің ену процестерімен үнемі күрделене түсуде.

Ақпараттық қауіпсіздікке төнетін қауіптер ақпараттық жүйеге әртүрлі әсер етуі мүмкін, олар пассивті (ақпараттың құрылымы мен мазмұнын өзгертпейтіндер) және белсенді (жүйенің құрылымы мен мазмұнын өзгертетіндер, мысалы, арнайы бағдарламаларды қолдану) болып бөлінеді.

Көбінесе жаңа түрлермен толықтырылатындары ең қауіпті болып саналады, бұл ең алдымен, экономиканы компьютерлендірумен және электронды транзакциялардың таралуымен байланысты. Зиянкестер құпия деректерді алудың және компанияға шығын келтірудің жаңа жолдарын іздейді.

Мекемені ақша мен зияткерлік меншікті жоғалтудан қорғау үшін ақпараттық қауіпсіздікке көбірек көңіл бөлу керек. Бұл алдыңғы қатарлы технологиялар арқылы ақпаратты қорғау құралдарының арқасында мүмкін болады.

Ақпараттық қауіпсіздікті қамтамасыз ету бойынша ұсынымдар:

барлық бағдарламалық жасақтамаңызға – антивирустық және антишпиондық бағдарламаларға, операциялық жүйелерге, мәтіндерді өңдеу бағдарламаларына және басқа бағдарламаларға үнемі жаңартулар орнатыңыз;

қолжетімді болған кезде бағдарламалық жасақтаманы автоматты түрде жаңарту мүмкіндіктерін қосыңыз;

пайдаланбайтын бағдарламалық жасақтаманы жойыңыз;

әріптер, сандар мен белгілердің тіркесімін қамтитын күшті құпия сөздерді қолданыңыз;

барлық сайттарда бірдей құпия сөздерді қолданбаңыз;

құпия сөздерді жұмыс үстелінде электронды түрде сақтамаңыз, жазылған құпия сөздерді қоғамдық орындарда сақтамаңыз, құпия сөздерді үшінші тұлғаларға айтпаңыз;

ЭЦҚ компьютерде сақталмауы керек;

бағдарламалық жасақтаманы тек сенетін сайттарға жүктеңіз;

электрондық пошта хабарламаларындағы сілтемелерге өтпеңіз және тегін бағдарламалық жасақтама ұсынылатын веб-сайттардан, әсіресе, тегін антивирустық бағдарламалық жасақтамалардан аулақ болыңыз;

музыканы, ойындарды, бейнелерді және басқаларын “тегін” жүктеуден сақ болыңыз. Олар жүктеуде зиянды бағдарламаны қамтуы мүмкін;

бейтаныс адамдардан электрондық пошталар мен күдікті тіркемелерді ашпаңыз, әсіресе, егер бұл мұрағат немесе орындалатын файлдар болса (exe – файл кеңейтімі). Егер сіз хатты маңызды деп ойласаңыз, онда жіберушімен телефон арқылы хабарласып, хаттың тақырыбын және жіберудің себебін нақтылауыңыз керек.

лицензияланған вирусқа қарсы бағдарламалық жасақтаманы пайдаланыңыз. Компьютерге қосылған кезде кез-келген тасымалдаушыны вирустарға тексеруді ұмытпаңыз;

автоматты тексеруді орнату арқылы кіріс электрондық поштадан барлық файлдарды вирустарға тексеріңіз;

Интернет желісіне қосылуды Интернетке қол жеткізудің бірыңғай шлюзі арқылы ғана жүргізу қажет;

үшінші тұлғаларға IP мекенжайын және логин мен пароль тіркесімін айтпаңыз;

платформаларда (Zoom, Webex Meetings, Team Link және т. б.) көпшілік іс-шараларды ұйымдастыруда жеке конференция идентификаторын (PMI) пайдаланбауға тырысыңыз;

іс-шараны жоспарлау кезінде кездейсоқ конференция идентификаторын жасаңыз және құпия сөзді қорғауды қосыңыз;

бұқаралық іс-шараларға сілтемелерді бөгде адамдарға таратпаңыз;

компьютерлік жүйедегі өте маңызды деректердің үнемі қосалқы көшірмесін жасап және қашықтан сақтаңыз.

**Ақпаратты қорғау**

**Ақпаратты қорғау — ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені. Тәжірибе жүзінде ақпаратты қорғау деп деректерді 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, программалық және техникалық әдістер мен құралдардан тұрады.**

**Ақпараттық қауіпсіздік**

**Ақпаратты өңдеудің автоматтандырылған жүйесі (АЖ) ретінде келесі объектер жиынтығын түсіну керек:**

**есептеуіш техника құралдарын;**

**программалық жасауды;**

**байланыс арналарын;**

**түрлі тасушылардағы ақпараттарды;**

**қызметшілер мен жүйені пайдаланушыларды.**

**АЖ-нің ақпараттық қауіпсіздігі жүйенің мына күйлерінде:**

**жүйенің сыртқы және ішкі қауіп-қатерлердің тұрақсыздандыру әсеріне қарсы тұра алу қабілеті бар кезіндегісі;**

**жүйенің жұмыс істеуі және жүйенің бар болуы сыртқы ортаға және оның өзінің элементтеріне қауіп келтірмеуі кезіндегісі қарастырылады.**

**Тәжірибе жүзінде ақпараттық қауіпсіздік қорғалатын ақпараттың келесі негізгі қасиеттерінің жиынтығы ретінде қарастырылады:**

**конфиденциалдылық (құпияланғандық), яғни ақпаратқа тек заңды пайдаланушылар қатынай алатындығы;**

**тұтастық, біріншіден, тек заңды және сәйкесті өкілдігі бар пайдаланушылар ғана өзгерте алатын ақпараттың қорғалуын, ал екіншіден ақпараттың ішкі қайшылықсыздығын және (егер берілген қасиет қолданыла алатын болса) заттардың нақты жағдайын бейнелеуін қамтамасыз ететіндігі;**

**қатынау қолайлығы, қорғалатын ақпаратқа заңды пайдаланушыларға бөгетсіз қатынаудың кепілі болуы.**

**Желілік қауіпсіздік сервистері есептеуіш жүйелерде және желілерде өңделетін ақпараттың қорғау механизмдерін береді.**

**Инженерлік-техникалық әдістер өзінің мақсаты ретінде техникалық арналар арқылы ақпараттың жайылып кетуінен ақпараттың қорғалуын қамтасыз етуді қарастырады.**

**Ақпаратты қорғаудың құқықтық және ұйымдастырушылық әдістері нормалар үлгілерін жетілдіру үшін ақпараттық қауіпсіздікті қамтамасыз етуге байланысты әр түрлі қызметтерді ұйымдастырады.**

**Ақпараттық қауіпсіздікті қамтамасыз етудің теориялық әдістері өз кезегінде екі негізгі мәселені шешеді. Біріншіден, ақпараттық қауіпсіздікті қамтамасыз етуге байланысты әр түрлі процесстерді формализациялау.Осыдан екінші мәселе туындайды – ол, қорғалу деңгейін талдағанда ақпараттық қауіпсіздікті қамтамасыз етудегі жүйелер қызметінің қисындылығы мен адекваттығының қатаң негізделуі.**

**Ақпараттық қауіпсіздіктің қауіптері**

**Автоматтандырылған жүйенің ақпаратық қауіпсіздігіне қауіп дегеніміз – бұл АЖ өңдейтін ақпараттың конфиденциалдығы, тұтастығы мен қатынау қолайлығының бұзылуына әкеліп соғатын әсерлердің жүзеге асырылуы және де АЖ құраушыларының жоғалуына, жойылуы мен қызмет етуін тоқтатуына келтіретін мүмкіндігі. Қауіптердің жіктелуі:**

**Пайда болу табиғатына қарай табиғи және жасанды болып бөлінеді. Табиғи –бұл адамға байланыссыз АЖ-ге физикалық процесстер мен табиғи апаттардың әсер ету нәтижесінде пайда болған қауіп. Өз кезегінде жасанды қауіп адамның әрекетінен туындайды. Табиғи қауіптің мысалы ретінде өрт, тасқын, цунами, жер сілкінісі және т.б. айтса болады. Мұндай қауіптің жағымсыз жағы – оны болжаудың қиындығы және мүмкін еместігі.**

**Ниеттілік дәрежесіне сәйкес кездейсоқ және қасақана болып бөлінеді. Кездейсоқ қауіп қызметшілердің немқұрайдылығынан немесе әдейілеп жасалмаған қателіктерінен пайда болады. Қасақана қауіп әдетте бағытталып жасалған әрекет нәтижесінде пайда болады.Кездейсоқ қауіптің мысалы ретінде байқаусыз деректердің қате енгізілуін, абайсыз жабдықтың бүлдірілуін келтіруге болады. Ал қаскүнемнің физикалық қатынаудың белгіленген ережелерін бұзып қорғалатын аймаққа рұқсатсыз кіру қасақана қауіптің мысалы болып табылады.**

**Қауіп көзіне тәуелді келесідей бөледі:**

**қауіп көзі – табиғи орта. Мысалы: өрт, тасқын және басқа да табиғи апаттар;**

**қауіп көзі – адам. Мысалы, бәсекелес ұйымның АЖ қызметкерлері қатарына өз агенттерін енгізу;**

**қауіп көзі – рұқсатты программалық-аппараттық құралдар. Мысалы, жүйелік утилиттерді пайдалануды жете білмеушілік;**

**қауіп көзі – рұқсатсыз программалық-аппараттық құралдар. Мысалы, жүйеге кейлоггерлерді енгізу;**

**Қауіп көзінің орналасуына байланысты былай бөлінеді:**

**қауіп көзінің бақылау аумағынан тыс орналасуынан пайда болатын қауіп.Мысалы, жанама электромагнит сәулеленулерін (ЖЭМС) немесе байланыс арналарымен беріліп жатқан деректерді ұстап алу; қашықтан фото және бейне түсіру; бағытталған микрофон көмегімен акустикалық ақпаратты ұстап қалу;**

**қауіп көзінің бақылау аумағының шекарасында орналасуы. Мысалы,білдірмей тыңдау құрылғыларын қолдану немесе конфиденциялды ақпараты бар деректерді тасушыларын ұрлау.**

**АЖ-ге әсер ету дәрежесі бойынша пассивті және активті қауіптер деп бөледі.**

**Пассивті қауіп іске асырылғанда АЖ құрамына және құрылымына ешқандай өзгеріс енбейді, ал активті қауіп, керісінше, АЖ құрылымын бұзады. Пассивті қауіптің мысалы ретінде деректер файлдарын рұқсатсыз көшіруді келтіруге болады.**

**АЖ ресурстарына қатынау тәсілі бойынша былай бөлінеді:**

**стандартты қатынауды қолданатын қауіп. Мысалы, заңды иеге қатысты пара беру, шантаж, физикалық қауіп төндіру арқылы рұқсатсыз парольді алу;**

**стандартты емес қатынауды қолданатын қауіп. Мысалы, қорғау құралдарының ресми мәлімделмеген мүмкіндіктерін пайдалану.**

**Қауіптердің негізгі жіктелуі:**

**Ақпараттың конфиденциялдығын (құпияланғандығын) бұзатын қауіптердің орындалу нәтижесінде құпия ақпаратпен танысу үшін өкілдігі жоқ субъектіге ақпаратқа қатынау мүмкіндігі туады.**

**Ақпараттың тұтастығын бұзатын қауіптерге, АЖ көмегімен өңделініп жатқан ақпаратты кез келген қаскүнемділікпен бұрмалау немесе құрту жатады.**

**Ақпараттың қатынау қолайлығын бұзатын қауіптерге, АЖ ресурсына рұқсаты бар пайдаланушының қатынауы бұғатталғанда туындайтын жағдайлар жатады.**

**Ақпарат қорғанысының негізгі қауіптеріне және ақпараттық жүйенің қарапайым функциялануына келесілер жатады:**

**құпия ақпараттың ағып кетуі;**

**ақпаратты компрометациялау;**

**ақпараттық ресурстарды бекітілмеген жолмен қолдану;**

**ақпараттық ресурстарды қателесіп қолдану;**

**абоненттердің арасында бекітілмеген ақпарат алмасу;**

**ақпараттан бас тарту;**

**Идентификация**

**Идентификация – қатынасатын субъектке арнайы идентификатор (қайталанбайтын) тағайындау және оны мүмкін болатын идентификатор тізімімен салыстыру операциясы.**

**Аутентификация**

**Аутентификация – қатынасатын субъект пен оның идентификаторының сәйкестігін тексеру әрі растау операциясы. Аутентификацияның әдістерін үлкен 4 топқа бөлуге болады:**

**Белгілі бір құпия ақпаратты білуге негізделген әдістер. Бұл әдістің бәрімізге таныс мысалы – парольдік қорғаныс. Қолданушы жүйеге кірер кезде пароль, яғни таңбалардың құпия тізбегін, енгізу керек болады. Аутентификацияның бұл әдісі ең кең таралған болып табылады.**

**Қайталанбайтын зат (нәрсе) қолдануға негізделген әдістер. Қайталанбайтын зат ретінде түрлі смарт карталар, токен, электрондық кілттерді айтуға болады.**

**Адамның биометриялық белгісіне негізделген әдістер. Іс жүзінде биометриялық белгілердің келесідей түрлері қолданылады: Саусақтың ізі, Көздің торлы қабықшасы не мөлдір қабықшасының суреті, Қолдың жылулық суреті, Беттің фотосуреті не жылулық суреті, Жазу (қолтаңба), Дауыс**

**Қолданушымен байланысты ақпаратқа негізделген әдістер. Мұндай әдістердің мысалы ретінде қолданушының GPS арқылы алынған координаттарын айтуға болады.**

**Аутентификацияның парольдік жүйелерінің ерекшеліктері:**

**Жүзеге асырудың салыстырмалы түрдегі жеңілдігі. Шынымен-ақ, парольдік қорғаныс механизмін ұйымдастыруға, көп жағдайда, ешқандай артық аппараттық құралдар керек емес.**

**Дәстүрлік. Парольдік қорғаныс механизмі қолданушылардың көпшілігіне таныс, сондықтан басқа құралдарға қарағанда (м: көздің мөлдір қабықшасының сканерлеу) психологиялық жатсыну тудырмайды.**

**Қауіпсіздіктің парольдік жүйелерінің негізгі қауіптеріне:**

**Адами факторлардың әлсіздігін пайдалану жолы. Бұл жерде пароль алу әдістері әр түрлі: пароль енгізу кезінде көріп алу, тыңдап алу, шантаж немесе біреудің тіркелгісін рұқсатпен пайдалану.**

**Теріп тауып алу. Бұл жерде келесідей әдістер пайдаланылады:**

**Барлық вариантты теріп, тауып алу. Бұл әдіс бойынша парольді енгізіп көру кезінде барлық мүмкін комбинация тексеріледі. Қаскүнемнің жүйеге кіру уақыты көп болу керек екендігі өз-өзінен-ақ түсінікті. Бұл әдіспен шыдамдығы кез-келген парольдер табылады.**

**Сөздік бойынша теріп, тауып алу. Іс жүзінде пайдаланылатын парольдер мағыналы сөз не сөз тіркесі болып табылады. Осындай көп пайдаланылатын парольдер тізімделіп, сөздік жасалады. Осы сөздіктің көмегімен парольді тез тауып алуға болады.**

**Қолданушы туралы мәлімет бойынша теріп, тауып алу. Бұл әдістің негізінде әр қолданушы өз паролін өздері ойлап табу фактісі жатыр. Көп жағдайда, адамдар пароль ойлап тапқан кезде, өздеріне байланысты мәлімет енгізеді.**

**Қауіпсіз жүйе**

**Қауіпсіз жүйе - белгілі бір тұлғалар немесе олардың атынан әрекет жасайтын үрдістер ғана ақпаратты оқу, жазу, құрастыру және жою құқығына ие бола алатындай етіп ақпаратқа қол жеткізуді тиісті құралдар арқылы басқаратын жүйе.**

**Сенімді жүйе**

**Сенімді жүйе - әр түрлі құпиялық дәрежелі ақпаратты қатынас құру құқығын бұзбай пайдаланушылар тобының бір уақытта өңдеуін қамтамасыз ету үшін жеткілікті ақпараттық және программалық құралдарды қолданатын жүйе.**

**Жүйенің сенімділігі (немесе сенім дәрежесі) екі негізгі өлшемі бойынша бағаланады: қауіпсіздік саясаты және кепілділік.**

**1983 жылы АҚШ Қазақстан Республикасының Қорғаныс министрлігі қызғылт сары мұқабасы бар «Сенімді компьютерлік жүйелерді бағалау өлшемдері» деп аталатын кітап шығарды.**

**«Қызғылт сары кітапта» сенімділіктің төрт деңгейі анықталған: D, С, В және А. D деңгейі қанағаттандырылмаған жүйеге арналған С деңгейіне А деңгеіне өту кезінде жүйелерге қатаң талаптар қойыла бастайды. С және В деңгейінің бөлімдері сенімділік деңгейінің өсуі бойынша кластарға (С1,C2.B1,B2,B3) бөлінеді.**

**Қауіпсіздіктің барлық алты класы бар (C1,C2,B1,B2,B3,A1). Сертификация кезінде жүйені белгілі бір кластарға жатқызу үшін, оның қауіпсіздік саясаты мен кепілдеме деңгейі маңызды талаптарды қанағаттандыру қажет.**

**«Қызғылт кітапқа» қойылатын талаптар келесідей:**

**Қауіпсіздік политикасы**

**Жүйе дәл анықталған қауіпсіздік политикасын ұстануы тиіс.**

**Субъекттің объектке қолжетушілік мүмкіндігі олардың ұқсастығы және қолжетушілікпен басқару ережелерінің жиынтығы негізінде анықталуы керек.**

**Объектімен қолжетушілікті бақылау процедуралары үшін бастапқы информация есебінде қолданылатын қауіпсіздік белгілері бір-біріне ұйқасуы керек.**

**Есеп беру**

**Барлық субьекттерде ерекше идентификаторлар болуы тиіс.**

**Қолжетушілік бақылауы қолжетушіліктің объектісінің және субъектісінің ұқсастығы, айырмашылығы және қолжетушілікті бөлу ережелері негізінде жүзеге асуы қажет.**

**Тіркелу жүйесі оқиғаның жалпы ағынының анализін жүзеге асыруы және одан тек қауіпсіздікке әсер ететін оқиғаларды бөліп алу қажет.**

**Оқиға хаттамасы рұқсатсыз қолжетушіліктен, түрлендіру және жоюдан сенімді қорғалған болуы тиіс.**

**Кепілдік**

**Қорғау құралдары қорғау функцияларының жұмысқа қабілеттілігін қамтамасыз ететін тәуелсіз аппараттық немесе программалық компоненттерден құралуы тиіс.**

**Бақылау құралдары қорғау құралдарынан түгелдей тәуелсіз болуы керек.**

**Барлық қорғау құралдары рұқсатсыз бөгеулер мен ажыратулардан қорғалуы тиіс, сонымен қатар бұл қорғау қорғау жүйесінің жұмысының кез-келген режимінде және барлық автоматтандырылған жүйелерде тұрақты және үзіліссіз болуы керек.**

**Ақпараттық қауіпсіздік саясаты**

**Қауіпсіздік саясаты**

**Қауіпсіздік саясаты - мекеменің ақпаратты қалайша өңдейтінін, қорғайтынын және тарататынын анықтайтын заңдар, ережелер және тәртіп нормаларының жиыны. Бұл ережелер пайдаланушының қайсы кезде белгілі бір деректер жинағымен жұмыс істей алатынын көрсетеді. Қауіпсіздік саясатын құрамына мүмкін болатын қауіптерге талдау жасайтын және оларға қарсы әрекет шаралары кіретін қорғаныштың белсенді сыңары деп санауға болады.**

**Кепілдік**

**Кепілдік - жүйенің сәлетіне және жүзеге асырылуына көрсетілетін сенім өлшемі. Ол қауіпсіздік саясатын іске асыруға жауапты тетіктердің дұрыстығын көрсетеді. Оны қорғаныштың, қорғаушылар жұмысын қадағалауға арналған, белсенсіз сынары деп сипаттауға болады.**

**Қауіпсіздік кластары**

**С1 - Дискретті қорғау**

**Кластың талабы: пайдаланушы ұсынылған қорғау құралдарын қолдану мүмкіншілігі бар. Қорғау бірнеше үзінді «нүктелі» элементтерден ұйымдастырылады.**

**Тиісті критерийлары:**

**Авторизациялау сервері болу керек**

**Аппараттық және программалық құралдары болуы керек**

**Қауіпсіздік ережелерін сақтау талабы қойылады**

**Қорғаныс механизмдері тестіленіп отыруы керек**

**Идентификация және аутентификация**

**С2 - Қатынаумен таңдамалы басқару**

**Қатынауды тиімділеу бағытта, ұсыныстар, кеңестер беріледі. Жүйеге қадағалау енгізіле басталады.**

**Тиісті критерийлары:**

**объектілердің қайта қолдануы**

**жүйеде орындалған әр іс-әрекет нақты пайдаланушымен байланысты**

**тіркелетін ақпарат қорғалуға тиісті**

**В1 - Мандатты басқару**

**Мандатты басқару – (ағылш. Mandatory access control, MAC) — субъектілердің объектілерге қолжетімділігін берілген құқыққа немесе (мандатқа, рұқсатқа) сәйкес ұйымдастыру. Кейбір жерлерде оны Еріксіз басқару деп аударады.**

**Тиісті критерийлары:**

**Қауіпсіздік саясат**

**Архитектураны верификациялау**

**Қауіпсіздік белгілері**

**Пайдаланушыны жүйемен жұмыс жасауда құжаттандыру керек**

**В2 - Құрылымдық қорғаныс**

**Ақпаратты жіберетін жасырын арналарға бақылау жүргізе отырып,барлық субъектілерге қолданылатын дискрециялық және мандатты қатынауды басқаруды ескеретін формалды анықталған және нақты құжатталған қауіпсіздік моделі**

**Тиісті критерийлары:**

**Сенімді есептеу базасы, өзіне тиесілі жобалардың енуі мен тұрақтылығын қамтамасыз етуі**

**Алғашқы идентификациялық,аудентификациялық операцияларды орындағанда есептеуіш базасына сенімді байланысу жолын қамтамасыз ету**

**Жады мен алмасу құпия арналарын тіркеу**

**Тестілер құпия ақпарат алмасу арналарының қатынау қабілеттілігінің шектеуін құптайды**

**Есептеу базасы жақсы құрылымданған және тәуелсіз модульдерден тұрады**

**В3 - Қауіпсіздік домендері**

**Барлық қорғау механизмдері қауіпсіздік ядросында шоғырлануы керек.Аудит құралдарының жұмыс істеу жауапкершілігіне және жүйені қалпына келтіруге администратор жауапты.**

**Тиісті критерийлары:**

**Анықталған қауіпсіздік саясатты ұстануы**

**Аудит құралдарына хабарландырулар енуі тиіс**

**Қауіпсіздік мониторын қолдау**

**Қауіпсіздік ядросы ықшамды болып келеді**

**Есептеуіш базаға сырттан келген шабуылға қарсылық көрсету**

**Жүйенің жұмыс істеу қабілетін қалпына келтіру құралдарының бар болуы қажетті.**

**А - Верификацияланған (тексерілетін) қауіпсіздік**

**Тестілеу сенімді есептеу базасының формалдық спецификациясының жоғары деңгейін қадағалап, өндіруі қажет**

**Формальды спецификациялық жоғары деңгейлі болуы тиіс. Заманауи әдіс формалды спецификация мен верификациялық жүйені қолданады.**

**Конфигурациялық механизм басқару жүйесі бүкіл өмір циклін және барлық жүйе компаненттерін, оған тиесілі қауіпсіздік әрекеттерін қамтамасыз етеді.**

**Кепілдік түрлері**

**Кепілдіктің екі түрі болады: операциялық және технологиялық. Біріншісі жүйенің сәулеті және жүзеге асырылу жағына, ал екіншісі - құрастыру және сүйемелдеу әдістеріне қатысты.**

**Есепберушілік**

**Есепберушілік (немесе хаттамалау тетігі) қауіпсіздікті қамтамасыз етудің маңызды құралы болып табылады. Сенімді жүйе қауіпсіздікке байланысты барлық оқиғаларды тіркеп отыруы керек, ал хаттаманы жазу-жүргізу тексерумен (аудитпен – тіркелу ақпаратына талдау жасаумен) толықтырылады.**

**Сенімді есептеу базасы**

**Сенімді есептеу базасы (СЕБ) - компьютерлік жүйенің қауіпсіздік саясаты жүзеге асыруға жауапты қорғаныш тектерінің жиынтығы. Компьтерлік жүйенің сенімділігіне баға беру үшін тек оның есептеу базасын қарастырып шықса жеткілікті болады. СЕБ негізгі міндеті - қатынасым мониторының міндетін орындау, яғни, объектілермен белгілі бір операциялар орындау болатындығын бақылау.**

**Қатынасым мониторы**

**Қатынасым мониторы – пайдалынушының программаларға немесе деректерге әрбір қатынасының мүмкін болатын іс - әрекеттер тізімімен келісімдігі екендігін тексеретін монитор.**

**Қатынасым мониторынан үш қасиеттің орындалуы талап етіледі:**

**Оңашаландық**

**Монитор өзінің жұмысы кезінде аңдудан қорғалуға тиісті;**

**Толықтық**

**Монитор әрбір қатынасу кезінде шақырылады. Бұл кезде оны орай өтуге мүмкіндік болмау керек;**

**Иландырылатындық**

**Мониторды талдауға және тестілеуге мүмкін болу үшін ол жинақы болуы керек.**

**Қауіпсіздік өзегі**

**Қауіпсіздік өзегі - қатынасым мониторының жүзеге асырылуы. Қауіпсіздік өзегі барлық қорғаныш тетіктерінің құрылу негізі болып табылады. Қатынасым мониторының аталған қасиеттерінен басқа қауіпсіздік өзегі өзінің өзгерместігіне кепілдік беруі керек.**

**Қауіпсіздік периметрі**

**Қауіпсіздік периметрі - сенімді есептеу базасының шекарасы. Оның ішіндегі сенімді, ал сыртындағы сенімсіз деп саналады. Сыртқы және ішкі әлемдер арасындағы байланыс ретқақпа арқылы жүзеге асырылады. Бұл ретқақпа сенімсіз немесе дұшпандық қоршауға қарсы тұра алуға қабілетті бар деп саналады.**

**Объектінің ақпараттық қауіпсіздігін қамтаммасыз етуге арналған жұмыстар бірнеше кезеңге бөлінеді:**

**даярлық кезеңі,**

**ақпараттық қорларды түгендеу,**

**қатерді талдау,**

**қорғаныш жоспарын жүзеге асыру.**

**Осы аталған кезеңдер аяқталған соң эксплуатациялау кезеңі басталады.**

**Даярлық кезең**

**Бұл кезең барлық келесі шаралардың ұйымдастырушылық негізін құру, түпқазық құжаттарды әзірлеу және бекіту, сондай-ақ, үрдіске қатысушылардың өзара қарым - қатынастарын анықтау үшін қажет. Даярлық кезеңде ақпарат қорғау жүйесінің ақпараттың міндеттері анықталады.**

**Ақпараттық қорларды түгендеу**

**Бұл кезеңде, әдетте, объект, ақпараттық ағындар автоматтандырылған жүйелердің құрылымы серверлер, хабар тасышулар, деректер өңдеу және сақтау тәсілдері жайында мәлімет жиналады. Түгендеу анықталған соң олардың осалдылығына талдау жасалынады.**

**Қатерді талдау**

**Келесі шаралардың нәтижелерді ақпараттық қорлардың қорғанылу күй - жағдайның қаншалықты толық және дұрыс талдануына тәуелді болады.**

**Қатерді талдау мыналардан тұрады:**

**талданатын объектілерді және оларды қарастырудың нақтылану дәрежесін таңдау;**

**қатерді бағалау әдіснамасын таңдау;**

**қауіптерді және олардың салдарын талдау;**

**қатерлерді бағалау;**

**қорғаныш шараларын талдау;**

**таңдап алынған шараларды жүзеге асыру және тексеру;**

**қалдық қатерді бағалау.**

**Қауіп бар жерде қатер пайда болады. Қауіптерді талдау кезеңі қатерді талдаудың орталық элементі болып табылады. Қауіптердің алдын алу үшін қорғаныш шаралары мен қүралдары қажет. Қауіптерді талдау, біріншіден, мүмкін болатын қауіптерді анықтаудан (оларды идентификациялаудан) және, екіншіден, келтірілетін болашақ зиянды болжау - бағалаудан тұрады.**

**Бұл кезеңнің орындалу нәтижесінде объектідегі қауіп - қатерлер тізбесі және олардың қауіптік дәрежесі бойынша жіктемесі құрастырылады. Бұлар бәрі ақпарат қорғау жүйесіне қойылатын талаптарды айқындауға, қорғаныштың ең әсерлі шаралары мен құралдарын таңдап алуға, сондай - ақ, оларды жүзеге асыруға қажетті шығындарды анықтауға мүмкіндік береді.**

**Қорғаныш жоспарын құрастыру**

**Бұл кезеңде осының алдында жүргізілген талдаудың нәтижесінде анықталған қатердерді бейтараптау үшін қорғаныштың тиісті ұйымдастырушылық және техникалық шаралары таңдап алынады.**

**Қорғаныш жоспарын құру ақпарат қорғау жүйесінің функционалдық сұлбасын әзірлеуден басталады. Ол үшін қорғаныш жүйесінің атқаратын міндеттері анықталады және нақты объектінің ерекшеліктерін ескере отырып жүйеге қойылатын талаптар талқыланады.**

**Жоспарға мынадай құжаттар қосылады:**

**қауіпсіздік саясаты;**

**ақпаратты қорғау құралдарының объектіде орналасуы;**

**қорғаныш жүйесін жұмысқа қосу үшін қажет шығындардың сметасы;**

**ақпарат қорғаудың ұйымдастырушылық;**

**техникалық шараларын жүзеге асырудың күнтізбелік жоспары.**

**Қорғаныш жоспарын жүзеге асыру**

**Бұл кезеңде қорғаныш жоспарында келтірілген шаралармен қоса жабдықтаушылармен келісім - шарттар жасасу жабдықтарды орнату және баптау, қажетті құжаттарды әзірлеу және т. б. осы сияқты шаралар іске асырылады.**

**Қауіпсіздік саясаты**

**Қауіпсіздік саясаты (ұйымдастыру тұрғысынан қарағанда) есептеу және қатынас қорларын пайдалану тәсілін, сондай - ақ, қауіпсіздік режимін бұзудың алдын алу және мән беру процедураларын дұрыс анықтайды. Қауіпсіздік саясатын қалыптастыру іс - әрекетін келесі кезеңдер түрінде қарастыруға болады:**

**Ұйымдастыру мәселелерін шешу**

**Бұл кезеңде ақпараттық қауіпсіздік қызметі құралады, ақпараттық қауіпсіздік тұрғысынан қарағанда пайдаланушылардың санаттары, пайдаланушылардың барлық санаттарының жауаптылық деңгейлері, құқықтары және міндеттері анықталады.**

**Қатерге талдау жасау**

**Қатерді талдау үрдісі нені қорғау керек, неден қорғау керек және қалай қорғау (істеу) керек деген сияқты сұрақтардың жауабын анықтайды. Мүмкін болатын қатерлердің бәрін қарастырып шығу керек және оларды келтіретін зиянының ықтимал мөлшеріне байланысты жіктеу керек. Қорғанышқа жұмсалатын қаржы қорғалынатын объектінің құнынан аспауға тиісті.**

**Жеңілдіктерді анықтау**

**Қорларды пайдалану құқықтары, қорларды қолдану ережелері, әкімшілік жеңілдіктер пайдаланушылардың құқықтары мен міндеттері, жүйелік әкімшілердің құқықтар мен міндеттері, жасырын ақпаратпен жұмыс істеу тіртіптері және тағы басқа анықталады.**

**Қауіпсіздік саясатының бұзылуына жауап қайтару шараларын анықтау**

**Қауіпсіздік режимін бұзушыларды табуға және жауапкершілікке тартылуға бағытталған әрекеттер, сонымен қатар, ақпаратты бұрынғы қалпына келтіру және бұзулардың зардаптарын жою шаралары анықталады.**

**Ұйымдастыру-өкімгерлік құжаттарды дайындау**

**Қауіпсіздік саясатының негізгі жайлары әр түрлі нұсқауларда, қағидаларда, ережелерде және өкімдерде келтіріледі.**

**Қауіпсіздік саясаты ақпарат қорғау жүйесінің қауіп-қатерлерге қарсы әрекет жасауға бағатталған құқықтық нормалардың, ұйымдастырушылық (құқықтық) шаралардың, программалық-техникалық құралдар және процедуралық шешімдер кешенінің жиынтығын анықтайды.**

**Ақпарат қауіпсіздігінің жоғарғы дәрежесіне қол жеткізу тек тиісті ұйымдастыру шараларын қолдану негізінде ғана мүмкін болады. Ұйымдастырушылық шаралар кешенінің құрамына ақпараттық қауіпсіздік қызметін құру, жасақтау және оның іс-әрекеттерін қолдау, ұйымдастыра-өкімгерлік құжаттар жүйесін дайындау жұмыстары, сонай-ақ, қорғаныш жүйесін құруға және оның жұмысын сүйемелдеуге арналған бірқатар ұйымдастырушылық және ұйымдастыру-техникалық шаралар кіреді.**

**Ұйымдастырушылық және ұйымдастыру - техникалық шаралар жүргізу ақпараттың сыртқа кететін жаңа арналарын дер кезінде табуға, оларды бейтараптандыру шараларын қолдануға, қорғаныш жүйелерін толық жетілдіруге және қауіпсіздік режимін бұзу әрекеттеріне жедел қарсы шара қолдануға мүмкіндік береді. Қатерге талдау жүргізу қауіпсіздік саясатын қалыптастырудың негізгі кезеңі болып табылады.**

**Ұйымдастыру мәселелерін шешілгеннен кейін программалық-техникалық проблемалардың кезегі келеді - таңдалған қауіпсіздік саясатын іске асыру үшін не істеу керек? Қазіргі уақытта құны атқаратын міндеті және сапасы жағынан әртүрлі болатын ақпарат қорғау құралдарының көптеген түрі бар. Олардың ішінен нақты объектінің ерекшелігіне сай келетінін таңдап алу күрделі мәселелердің бірі болып саналады.**

**Қауіпсіздік саясатының негізгі элементтері**

**Қауіпсіздік саясаты мынадай элементтерден тұрады:**

**қатынас құруды ерікті басқару,**

**объектілерді қайтадан пайдаланудың қауіпсіздігі,**

**қауіпсіздік тамғасы,**

**қатынас құрудың мәжбүрлі басқару.**

**Қатынас құрудың ерікті басқару**

**Қатынас құрудың ерікті басқару - жеке субъект немесе құрамына осы сцубъект кіретін топтың тұлғасын ескеру негізінде жасалған объектілерге қатынас құруды шектеу. Ерікті басқару - белгілі бір тұлға (әдетте, объектінің иесі) өзінің қарауынша басқа субъектілерге өзінің шешімі бойынша объектігі қатынас құру құқығын бере алады.**

**Қатынас құрудың ағымдағы жағдайы ерікті басқару кезінде матрица түрінде көрсетіледі. Қатарларында - субектілер, бағандарында - объектілер, ал матрицаның түйіндерінде қатынас құру құқығының (оқу, жазу, орындау және т. б. ) кодасы көрсетіледі.**

**Операциялық жүйелердің және дерекқор басқару жүйелерінің көпшілігі осы ерікті басқаруды жүзеге асырады. Оның негізгі жағымды жағы - икемділігі, ал негізгі кемшіліктері - басқарудың бытырыңқылығы және орталықтандырылған тексерудің күрделілігі, сондай-ақ, қатынас құру құқығының деректерден бөлек қарастырылуы (қаскүнемдер осыны пайдалана отырып құпия ақпараттарды жалпы қол жеткізерлік файлдарға көшіріп алуы мүмкін).**

**Объектілерді қайтадан пайдаланудың қауіпсіздігі**

**Бұл элемент құпия ақпаратты «қоқтықтан» кездейсоқ немесе әдейі шығарып алудан сақтайтын қатынас құруды басқаратын құралдардың маңызды қосымшасы болып табылады.**

**Объектілерді қайтадан пайдаланудың мүмкін болатын 3 қаупі бар:**

**жедел жадыны қолдану;**

**сыртқы сақтау құрылғыларын қайтадан пайдалану;**

**ақпарат еңгізу/шығару құрылғыларын қайтадан пайдалану.**

**Қорғаныш тәсілдерінің бірі - құпия ақпаратпен жұмыс істегеннен кейін жедел жадыда немесе аралық жадыны тазалау. Жақсы әдіс деп тегерішті нығыздау программаларын қолдануды да санауға болады.**

**Мәселен, принтерлердің аралық жадында құжаттардың бірнеше беті сақталып қалуы мүмкін. Олар басу үрдісі аяқталған соң да жадыда қалып қояды. Сондықтан оларды арашықтан шығарып тастау үшін арнаулы шаралар қолдану қажет. Әдетте кездейсоқ биттер тізбегін үш қайталап жазу жеткілікті болады.**

**«Субъектілерді қайтадан пайдаланудың» қауіпсіздігі жайында да қамдану керек. Пайдаланушы ұйымнан кеткен кезде оны жүйеге кіру мүмкіншіліктерінен айыру және барлық объектілерге оның қатынас құруына тиым салу керек.**

**Қауіпсіздік тамғасы**

**Қатынас мәжбүрлі басқарудың кезінде субъектілер және объектілер қауіпсіздік тамғасы арқылы байланысады. Субъектінің тамғасы оның шүбәсіздігін сипаттайды. Объектінің тамғасы оның ішіндегі сақталатын ақпараттың жабықтық деңгейін көрсетеді.**

**Қауіпсіздік таңбасы екі бөліктен тұрып: құпиялылық деңгейі және категориялар.**

**Құпиялылық деңгейі реттелген жиынтық құрайды және әр түрлі жүйелерде құпиялылық деңгейлер жиынтығы әр түрлі болуы мүмкін. Қазақстан Республикасының заңнамасына сәйкес мемлекеттік құпия құрайтын мәліметтердің үш құпиялық дәрежесі тағайындалған және осы дәрежелерге сәйкес аталған мәліметтердің тасушыларына мынадай құпиялылық белгілері берілген: «аса маңызды», «өте құпия», «құпия», ал қызметтік құпия құрайтын мәліметтірге «құпия» деген құпиялылық белгісі беріледі.**

**Санаттар реттелмеген жиынтық құрайды. Олардың міндеті - деректер жататын аймақтың тақырыбын сипаттау.**

**Қауіпсіздік таңбалардың тұтастығын қамтамасыз ету оларға байланысты негізгі проблемелардың біреуі болып табылады. Біріншіден, тамғаланбаған субъектілер мен объектілер болмау керек. Әйтпесе тамғалық қауіпсіздікте (қолдануға ыңғайлы) саңылаулар пайда болады және қаскүнем осы жағдайды пайдаланып қорғанылатын ақпаратқа заңсыз қол жеткізуі мүмкін. Екіншіден, қорғалынатын деректермен қандайда болмасын операциялар орындалмасын, қауіпсіздік тамғалары өзгермей қалуы керек.**

**Қауіпсіздік тамғаларының тұтастығын қамтамасыз етуші құралдардың біреуі - құрылғыларды көп деңгейлік және бір деңгейлік деп бөлу. Көп деңгейлік құрылғыларда әр түрлі құпиялық деңгейлі ақпарат, ал бір деңгейлік құрылғыларда тек бір құпиялық деңгейі бар ақпарат сақталады.**

**Қатынас құрудың мәжбүрлі басқару**

**Қатынас құруды басқару мәжбүрлі деп атаудың себебі - қатынас құру мүмкіндігі субъектінің ерігіне тәуелді емес. Мұндай басқару субъектінің және объектінің қауіпсіздік тамғаларын салыстыру негізінде жүргізіледі.**

**Ерге субъектінің құпиялылық деңгейіобъектінің құпиялылық деңгейінен кем болмаса, ал объектінің қауіпсіздік тамғасында көрсетілген барлық санаттар субъектінің тамғасында болса (яғни, осындай екі шарт орындалса), онда субект объектіден кез келген ақпаратты оқи алады. Мысалы, «өте құпия» субъект «өте құпия» және «құпия» файлдарын оқи алады. Бұл жағдайда «субъектінің қауіпсіздік тамғасы объектінің қауіпсіздік тамғасынан басым» деп атайды.**

**Тарихы**

**Ең ерте байланыс құралдарынның пайда болысымен, дипломаттар мен әскери қайраткер құпиялық хабарлар мен оның тәсілдерін анықтау, бұрмалау әрекеттерін кауіпсіздікке алу қажеттілігін түсінді. Мысалы, Юлий Цезарьдың шамамен б.з.б 50-жылдардағы өнертабысы, яғни Цезарь шифры, оның құпия хабарламаларын, жіберушіден басқа адамдардың окмауының алдын алу үшін ойлап табылған.[1] Дегенмен, бұл қауіпсіздіктің көп бөлігі құпия хабарламаның жету процедурасын қамтамасыз етті. Құпия хабарлар сенімді тұлғалар арқылы немесе сенімді күзетпен, қауіпсіз жерлерде қорғалып, жіберілген.**