№8 Лекция тақырыбы: Ақпараттық қауіпсіздіктің қатерлері және олардың жіктелуі. Зиянды бағдарламалар. Ақпаратты қорғаудың шаралары мен құралдары. Ақпараттық қауіпсіздік саласындағы стандарттар мен спецификациялар. ҚР ақпараттық қауіпсіздік саласындағы реттеуші құқықтық қатынастар заңнамасы. Электрондық цифрлы қолтаңба. Шифрлау.

Лекцияның оқыту нәтижелері: Ақпараттық қауіпсіздіктің қатерлері және олардың жіктелуі, Киберқауіпсіздік және Интернетті басқару

Лекция мазмұны:

8.1. Ақпараттық қауіпсіздіктің қатерлері және олардың жіктелуі

Ақпараттық қауіпсіздікті қамтамасыз етудің ең маңызды құраушысы қауіпті анықтау және оның жіктелуі болып табылады. Ақпараттық қауіпсіздікке қауіп төндіруші – қорғалған ақпаратқа қауіпті тудыратын қандай да бір факторлар мен жағдайлардың жиынтығы.

Ақпараттық қауіпсіздік (Information Security) – ақпаратқа рұқсатсыз қол жеткізуді, пайдалануды, ашуды, бұрмалауды, өзгертуді, зерттеуді, жазуды немесе жоюды болдырмау тәжірибесі.

Ақпараттық қауіпсіздік-жеке тұлғаның, қоғамның, мемлекеттің (ұлттық мүдделердің) мүдделеріне нұқсан келтіруі мүмкін ішкі және сыртқы қауіптерден формациялық ресурстардың (ақпараттық ортаның) қорғалу жағдайы.

Ақпараттың қауіпсіздігі – ақпараттың қажетсіз (ақпараттық қатынастардың тиісті субъектілері үшін) жария етілуінен (құпиялылықтың бұзылуынан), бұрмаланудан (тұтастықтың бұзылуынан), ақпараттың қолжетімділік дәрежесінің жоғалуынан немесе төмендеуінен, сондай-ақ оның заңсыз таралуынан қорғалуы.

Ақпараттық қауіпсіздік режимін қалыптастыру кешендік мәселе болып табылады. Оны шешу үшін заңнамалық, ұйымдастырушылық, программалық, техникалық шаралар қажет [12].

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

Ақпараттық қауіп – ақпаратты жоғалтуға не жария етуге әкеліп соқтыратын қорғаныс объектісіне заңсыз немесе кездейсоқ әсер ету мүмкіндігі. Ақпараттық қауіпсіздік, ақпаратты қорғау секілді кешенді мәселе, ол қауіпсіздікті қамтамасыз етеді, қауіпсіздік жүйесін енгізу арқылы іске асырылады. Ақпаратты қорғау мәселесі жан-жақты кешенді және бірқатар маңызды міндеттерді қамтиды.

Ақпараттық қауіпсіздік үшін қауіп төндірушіні, қорғау объектісін анықтау қажет. Себебі ақпарат – бұл қандай да бір дерек. Мысалы, құпия ақпаратты тасымалдаушылар – құжаттар, ақпаратты өндеу мен сақтаудың техникалық құралдары немесе адамдар болуы мүмкін.

Қауіптің үш түрі бар:

1. Құпиялылықты бұзу қаупі – бұл ақпарат оған қол жеткізуге құқығы жоқ адамға белгілі болады. Бұл есептеу жүйесінде сақталған немесе бір жүйеден екіншісіне берілетін кейбір құпия ақпаратқа қол жеткізілген кезде орын алады. Кейде құпиялылықты бұзу қаупіне байланысты «тарап кету» термині қолданылады.

Құпиялылық – ол тіркелген пайдаланушыға ғана ақпараттық ресурспен қолжетімді. Ақпараттың құпиялығы онымен өзінің иесі белгілеген қатаң шектелген адамдар тобы ғана таныса алады дегенді білдіреді.

2. Тұтастықты бұзу қаупі – кез келген есептеу жүйесінде сақталған немесе бір жүйеден екінші жүйеге берілетін ақпараттың қасақана өзгеруін қамтиды. Қаскүнемдер қасақана алдаған кезде ақпараттың тұтастығы бұзылған деп айтылады. Бағдарламалық қамтамасыздандыру немесе аппараттық құралдың кездейсоқ қателігі рұқсат етілмеген өзгеріске әкелсе, тұтастық бұзылады. Санкцияланған өзгерістер – бұл уәкілетті тұлғалар негізделген мақсатпен жасайтындар (мысалы, санкцияланған өзгеріс – кейбір мәліметтер базасын мерзімді жоспарланған түзету).

Ақпараттың тұтастығы - ақпараттың бұрмаланбаған түрде болуы (оның кейбір бекітілген күйіне қатысты өзгеріссіз болуы). Көбінесе субъектілер тақырыптық аймақтың жай-күйін көрсетудің сәйкестігінен (толықтығы мен дәлдігінен) және ақпараттың тікелей

тұтастығынан, яғни оның бұрмаланбауынан тұратын ақпараттың неғұрлым кең қасиетін – сенімділігін қамтамасыз етуге мүдделі. Тұтастылық – ол ақпаратты жіберу немесе сақтау үрдісінде өзгермеуі.

3. Қызметтердің істен шығу қаупі басқа пайдаланушы немесе шабуылдаушы жасаған қасақана әрекеттердің нәтижесінде есептеу жүйесінің кейбір ресурсына кіруге тыйым салынған кезде пайда болады. Шын мәнінде, бұғаттау тұрақты болуы мүмкін – сұралған ресурс ешқашан алынбайды немесе ол сұралған ресурстың пайдасыз болуы үшін жеткілікті ұзақ кідіріс тудыруы мүмкін. Бұл жағдайларда ресурс таусылды деп айтылады.

Ақпараттың қолжетімділігі – субъектілердің өздерін қызықтыратын ақпаратқа уақтылы кедергісіз қол жеткізуін қамтамасыз ету қабілетімен және субъектілерден келіп түсетін сұрау салуларға қызмет көрсетуге тиісті автоматтандырылған қызметтердің дайындығымен сипатталатын ақпарат айналымда болатын жүйенің (ортаның, құралдардың және өңдеу технологиясының) қасиеті.

Қолжетімділік – ол уақыттың әрбір сәтінде тіркелген пайдаланушыға ақпараттық деректерді алу және пайдалану мүмкіндігін анықтайтын ақпараттық ресурстардың қасиеті. Егер ақпаратқа қолжетімділікті уәкілеттілігі жоқ адам алатын болса, құпиялықтың бұзылуына немесе рұқсат етілмеген қолжетімділікке жол беріледі. Ақпараттық қауіпсіздік – ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қорғау [13].

8.2. Зиянды бағдарламалар. Ақпаратты қорғаудың шаралары мен құралдары

«Зиянды бағдарлама» термині компьютердегі немесе мобильді құрылғыдағы кез келген зиянды бағдарламаны сипаттау үшін қолданылады. Бұл бағдарламалар пайдаланушылардың келісімінсіз орнатылады және компьютердің жұмысының төмендеуі, пайдаланушының жеке деректерін жүйеден жою, деректерді жою немесе тіпті компьютер аппараттық құралдарының жұмысына әсер ету сияқты бірқатар жағымсыз салдарға әкелуі мүмкін. Киберқылмыскерлер пайдаланушы жүйелеріне енудің барған сайын күрделі жолдарын ойлап тапқандықтан, зиянды бағдарламалар нарығы айтарлықтай кеңейді. Интернеттен табуға болатын зиянды бағдарламалардың ең көп тараған түрлерін қарастырайық.

1. Вирустар. Компьютерлік вирустар өз атауын компьютердегі көптеген файлдарды «жұқтыру» қабілеті үшін алды. Вирус жұққан файлдар электрондық пошта арқылы жіберілгенде немесе пайдаланушылар USB дискілері сияқты физикалық медиада тасымалдағанда, олар басқа машиналарға да таралады. Ұлттық стандарттар және технологиялар институтының (NIST) мәліметтері бойынша, «Brain» деп аталатын алғашқы компьютерлік вирусты 1986 жылы екі ағайынды компаниядан Бағдарламалық жасақтама (БЖ) ұрлап жатқан қарақшыларды жазалау мақсатында жазған. Вирус иілгіш дискілердің жүктеу секторын жұқтырды және көшірілген вирус жұқтырған иілгіш дискілер арқылы басқа компьютерлерге берілді.

2. Құрттар. Вирустардан айырмашылығы, құрттар таралу үшін адамның араласуын қажет етпейді: олар бір компьютерді жұқтырады, содан кейін компьютерлік желілер арқылы иелерінің қатысуынсыз басқа машиналарға таралады. Электрондық пошта бағдарламаларындағы кемшіліктер сияқты желінің осалдықтарын пайдалана отырып, құрттар мыңдаған көшірмелерін жіберіп, барлық жаңа жүйелерді жұқтыруы мүмкін, содан кейін процесс қайтадан басталады. Көптеген құрттар жүйелік ресурстарды жай ғана «жеп», осылайша компьютердің жұмысын төмендетеді, олардың көпшілігінде қазір файлдарды ұрлауға немесе жоюға арналған зиянды компоненттер бар.

3. Жарнамалық бағдарлама. Зиянды бағдарламалардың ең көп таралған түрлерінің бірі – жарнамалық бағдарлама. Бағдарламалар хост компьютерлеріне жарнамаларды автоматты түрде жеткізеді. Adware сорттарының арасында веб-беттердегі қалқымалы жарнамалар және «тегін» бағдарламалық жасақтаманың бөлігі болып табылатын жарнамалар бар. Кейбір жарнамалық бағдарламалар салыстырмалы түрде зиянсыз, басқалары сіздің орналасқан жеріңіз немесе сайтқа кіру тарихы туралы ақпарат жинау және мақсатты жарнамаларды компьютер экранына шығару үшін бақылау құралдарын пайдаланады. BetaNews антивирустық қорғауды өшіре алатын жарнамалық бағдарламаның жаңа түрі табылғанын хабарлады. Adware пайдаланушының келісімімен орнатылғандықтан, мұндай бағдарламаларды зиянды деп атауға болмайды: олар әдетте «ықтимал қалаусыз бағдарламалар» ретінде анықталады.

4. Шпиондық бағдарлама. Шпиондық бағдарлама – компьютердегі әрекеттеріңізді бақылайды. Ол ақпаратты жинайды (мысалы, компьютердің пернетақтасындағы пернелерді тіркейді, қай сайттарға кіргеніңізді бақылайды және тіпті тіркеу деректерін ұстайды), содан кейін ол үшінші тұлғаларға, әдетте киберқылмыскерлерге жіберіледі. Сондай-ақ, ол компьютердегі белгілі бір қорғаныс параметрлерін өзгерте алады немесе желілік байланыстарға кедергі келтіруі мүмкін.

5. Төлем бағдарламалары. Төлем бағдарламалары сіздің компьютеріңізді жұқтырады, содан кейін жеке құжаттар немесе фотосуреттер сияқты құпия деректерді шифрлайды және оларды декодтау үшін төлем талап етеді. Егер сіз төлеуден бас тартсаңыз, деректер жойылады. Төлем бағдарламаларының кейбір түрлері компьютерге кіруді толығымен блоктауы мүмкін. Олар өз әрекеттерін құқық қорғау органдарының жұмысы үшін бере алады және сізді кез келген заңсыз әрекеттеріңіз үшін айыптай алады. 2015 жылдың маусымында Cryptowallet төлемдік вирусының нәтижесінде жалпы сомасы 18000000 АҚШ долларын құрайтын қаржылық шығын туралы хабарлаған пайдаланушылар ФБР-дегі онлайн алаяқтық шағымдарын қабылдау орталығына жүгінді.

6. Боттар. Боттар – бұл белгілі бір операцияларды автоматты түрде орындауға арналған бағдарламалар. Оларды заңды мақсаттар үшін пайдалануға болады, бірақ шабуылдаушылар оларды зиянды мақсаттарына бейімдеді. Компьютерге ену арқылы боттар оны белгілі бір командаларды қолданушының рұқсатынсыз немесе мүлдем білместен орындай алады. Хакерлер сонымен қатар бұзылған машиналарды қашықтан басқару үшін пайдаланылатын бот желісін құру үшін бірнеше компьютерді бір ботпен жұқтыруға тырысуы мүмкін, құпия деректерді ұрлау, жәбірленушінің әрекеттерін бақылау, спамды автоматты түрде тарату немесе компьютерлік желілерде жойқын DDoS шабуылдарын бастау.

7. Руткиттер. Руткиттер үшінші тарапқа компьютерге қашықтан қол жеткізуге және басқаруға мүмкіндік береді. Бұл бағдарламаларды IT мамандары желі ақауларын қашықтан жою үшін пайдаланады. Бірақ шабуылдаушылардың қолында олар алаяқтық құралына айналады: сіздің компьютеріңізге ену арқылы руткиттер киберқылмыскерлерге оны басқаруға және деректеріңізді ұрлауға немесе басқа зиянды бағдарламаларды орнатуға мүмкіндік береді. Руткиттер мүмкіндігінше ұзақ уақыт бойы байқалмай қалу үшін жүйеде өз қатысуын сапалы түрде жасыра алады. Мұндай зиянды кодты табу әдеттен тыс мінез-құлықты қолмен бақылауды, сондай-ақ ықтимал инфекция маршруттарын болдырмау үшін бағдарламалық жасақтама мен операциялық жүйеге үнемі түзетулер енгізуді талап етеді.

8. Трояндық бағдарламалар. Трояндықтар ретінде танымал бұл бағдарламалар заңды файлдар немесе бағдарламалық қамтамасыздандыру ретінде жасырылады. Жүктеп алып, орнатқаннан кейін олар жүйеге өзгерістер енгізеді және зиянды әрекеттерді жәбірленушінің білімінсіз немесе келісімінсіз жүзеге асырады.

9. Пернетақта тыңшысы. Пернетақта тыңшысы ең қауіпті зиянды қолданбаларға жатады. Ол арқылы хакерлер кез-келген құпия ақпаратты, соның ішінде пайдаланушының төлем деректерін ала алады [3, 208 б.].

Қазіргі заманғы зиянды бағдарламалар, әдетте, бірнеше компоненттерден тұрады, олардың әрқайсысының өз міндеті бар. Мұндай бағдарламалық қамтамасыздандыру жеке құралдар жиынтығынан гөрі Швейцария армиясының пышағын еске түсіреді, бұл шабуылдаушыға шабуылдаушы жүйеде көптеген түрлі әрекеттерді орындауға мүмкіндік береді. Мұндай шабуылда жиі кездесетін компоненттердің бірі – барлық пернелерді басуды жазатын жоғары мамандандырылған құрал – Keylogger. Дәл осы құралдың көмегімен шабуылдаушы байқалмай, көптеген құпия ақпаратты байқамай ұстай алады. Клавиатура – бұл компьютердің пернетақтасындағы барлық манипуляцияларды ұстап, жаза алатын бағдарламалық қамтамасыздандырудың немесе жабдықтың кез-келген компоненті. Көбінесе клавиатура пернетақта мен операциялық жүйенің арасында орналасады және пайдаланушының барлық әрекеттерін ұстайды. Бұл құрал ұрланған ақпаратты вирус жұққан компьютерде сақтайды немесе егер ол үлкен шабуылдың бөлігі болса, барлық деректер дереу шабуыл ұйымдастырушыларының қашықтағы компьютеріне жіберіледі.

Кейлоггерлердің көптеген нұсқалары болғанымен, негізгі бөлу бағдарламалық қамтамасыздандыру мен аппараттық құралдарға бөлінеді. Көбінесе троян немесе руткит сияқты зиянды бағдарламаның бөлігі болып табылатын бағдарламалық қамтамасыздандыру кілті

қолданылады. Әдетте, бұл физикалық араласусыз қызығушылық жүйесіне қол жеткізудің қарапайым нұсқасы. Бағдарламалық қамтамасыздандыру кілттерінің ең көп таралған түрлерінің бірі мақсатты машинада әр пернені басуды жазатын дайын API-ді қолдана алады.

Пайдаланушылардың қауіпсіздігін қамтамасыз ету үшін қазіргі заманғы қорғаныс өнімдерінің көпшілігінде бірнеше технологиялар енгізілген, бұл шабуылдаушылардың тыңшылық, кейлоггинг, тіркелген деректерін ұрлау, рұқсат етілмеген криптовалюта өндірісі, қажетсіз файлдарды шифрлау (төлем бағдарламалары арқылы), ақпарат алу (банктік трояндар арқылы), спам және алаяқтық сияқты көптеген әрекеттеріне, сондай-ақ кибершабуылдардың басқа түрлеріне қарсы тұруға мүмкіндік береді.

Антивирус

Антивирус – бағдарламалық жасақтамасы бар жабдықты зиянды кодтан (вирустардан) қорғау құралы, ол файлдарды Операциялық жүйе мен қосымшалардың штаттық жұмысын барынша тарату және бұзу мақсатында өзгертеді. Антивирус бағдарламалық құрал немесе бағдарламалық құрал кешені ретінде операциялық жүйесі бар құрылғыға жүктеледі және файлдық жүйеге зиянды кодтың араласуын сырттан анықтайды, содан кейін өзгертілген файлдарды блоктайды (карантинге қояды) және оларды жояды немесе белгілі қауіптер үшін интернет арқылы жаңартылатын профильдер дерекқорына сәйкес түзетеді. Антивирустың функционалдығы мен мүмкіндіктері оның техникалық жетілдірілуіне байланысты, сондықтан жабдықты қорғаудың сенімділігі көбінесе ең тиімді өнімді таңдауға байланысты.

Қорғау әдістерінің түрлері:

- *Сканерлеу*. Көбінесе бұл вирустарды анықтау үшін жедел жадты, қатты дискіні, SSD және сыртқы медианы сканерлейтін резидент емес құралдар (пайдаланушы қолмен іске қосады). Табылған код белгілі қауіптер базасындағы профильдермен салыстырылады, бұл оны үнемі жаңартып отыруды маңызды етеді.
- *Емдеу.* Көптеген антивирустарда қолданылады. Ақпараттыө технологиялар саласында әдіс «Фаг» немесе «Полифаг» деп аталады және вирус жұққан файлды табуға, содан кейін жоюдың орнына емдеуге (бастапқы күйін қалпына келтіруге) мүмкіндік береді. Код сканерлеу сияқты қауіп- қатер базасында сақталған профильдермен салыстырылады.
- *Иммундау*. Антивирус үшінші тарап бағдарламаларымен өзгерту үшін белгілі бір жүйелік каталогтарды, тізілімдегі жазбаларды және операциялық жүйенің өмірлік ресурстарын блоктайды. Әдіс әрекеттерді қолмен растауды немесе модификацияның сенімді көздерінің тізімін жасауды талап етеді.
- *Салыстыру.* Басқаша айтқанда, бар файлдарды қайта қарау. Антивирус жүйенің күйін түсіреді (жүйелік каталогтардағы файлдардың бастапқы кодын есте сақтау арқылы) және күдікті операциялар кезінде салыстыруды орындайды.
- *Мониторинг.* Әдіс зиянды кодтың пассивті қаупінен тұрақты қорғанысы бар антивирустың фондық жұмысымен және оны файлдық жүйені үздіксіз сканерлеу арқылы анықтаумен сипатталады.
- *Сүзу.* Көп жағдайда бұл антивирустағы резиденттік құрал, ол өзінің белсенділігі мен таралуын бастамас бұрын зиянды кодты анықтау үшін операциялық жүйемен бір уақытта іске қосылады.

Қауіптің түріне байланысты (белгілі немесе белгілі бір бағдарламалық жасақтамаға белгісіз) антивирус белсенді немесе реактивті қорғауды жүзеге асыра алады:

- *Проактивті қорғаныс (эвристика).* Зиянды бағдарламаларға тән бағдарламалардың коды мен мінез-құлқын зерттеуге негізделген белгісіз вирустардан қорғау. Қорғаудың бұл түрі өзгертілген вирустармен күресу кезінде жақсы нәтиже көрсетеді. Қазірдің өзінде бар қауіптер туралы деректер негіз ретінде қабылданады. Антивирустық контекстегі Эвристика - белгілі бір қауіпті анықтамай-ақ зиянды бағдарламалардың әрекеттерін анықтау үшін қолданылатын ережелер жиынтығы.
- *Реактивті қорғаныс (вирустық қолтаңба).* Код туралы ақпаратқа және зиянды бағдарламаның қалған ерекшеліктеріне негізделген бұрыннан белгілі вирустардан қорғау. Тиімді жұмыс істеу үшін мұндай антивирустар өздерінің вирустық қолтаңбаларының дерекқорларын үнемі жаңартып отыруы керек. Вирустық қолтаңбаларға негізделген қорғаныс антивирустық бағдарламаны жасаушылар жасаған бұрыннан белгілі вирустармен сөздікке жүгінуді білдіреді.

Проактивті қорғаудың басты кемшілігі – «жалған позитивтер» деп аталатын, инфекцияланбаған бағдарламалық жасақтаманы жиі бұғаттау.

Реактивті қорғаудың кемшілігі – жаңа қауіптерден қорғану мүмкін еместігі. Қазіргі антивирустық бағдарламада проактивті және реактивті қорғаныс қолданылады [14].

8.3. Ақпараттық қауіпсіздік саласындағы стандарттар мен спецификациялар. Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы реттеуші құқықтық қатынастар заңнамасы

Өзінің ақпараттық кеңістігін қорғау қазіргі қоғам үшін негізгі болып табылады, оның дамуы ақпараттық технологияларға байланысты. Алайда, жағымсыз ақпаратқа қарсы тұру өте қиын, өйткені ақпараттық технологиялардың қарқынды дамуы күн сайын қоғамда қалыптасқан стандарттар мен нормаларға жаңа қауіп төндіреді.

Ақпараттық қауіпсіздікті қамтамасыз ету проблемасының өзектілігі, ең алдымен, қазіргі әлемде ақпараттың стратегиялық ұлттық ресурсқа айналуына байланысты. Соңғы жылдары Қазақстан Республикасында мемлекеттің ақпараттық қауіпсіздігін қамтамасыз ету жүйесін жетілдіру бойынша бірқатар шаралар іске асырылды. Ақпараттық қауіпсіздікті дамытудың қағидаттары мен негізгі бағыттарын айқындайтын негізгі саяси- құқықтық акт Қазақстан Республикасының 2016 жылға дейінгі Ақпараттық қауіпсіздік тұжырымдамасы болып табылады, №174 тұжырымдама Қазақстан Республикасы Президентінің 2011 жылғы 14 қарашадағы Жарлығымен бекітілген. Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы қоғам мен мемлекеттің ақпараттық саладағы мүдделерін қамтамасыз ету, сондай-ақ азаматтың конституциялық құқықтарын қорғау мақсатында әзірленген. Тұжырымдама Қазақстан Республикасының 2030 жылға дейінгі «Барлық қазақстандықтардың өркендеуі, қауіпсіздігі және әл- ауқатын жақсарту» даму стратегиясының негізгі ережелеріне жауап береді, оның ішінде ұлттық қауіпсіздіктің құрамдас бөлігі ретінде ақпараттық қауіпсіздікті қамтамасыз ету негізгі ұзақ мерзімді басымдықтардың бірі болып айқындалған. Тұжырымдама ағымдағы жағдайды бағалауға негізделген және мемлекеттік саясатты, ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мемлекеттік органдар қызметінің перспективаларын айқындайды.

Тұжырымдама Қазақстан Республикасының Конституциясына және «Қазақстан Республикасының Ұлттық қауіпсіздігі туралы», «Мемлекеттік құпиялар туралы», «Терроризмге қарсы іс-қимыл туралы», «Электрондық құжат және электрондық цифрлық қолтаңба туралы», «Ақпараттандыру туралы», «Техникалық реттеу туралы», «Лицензиялау туралы», «Құралдар туралы», «Байланыс туралы» Қазақстан Республикасының заңдарына сәйкес әзірленді [15].

Тұжырымдаманы әзірлеу кезінде ақпараттық қауіпсіздікті қамтамасыз ету саласындағы халықаралық тәжірибе ескерілді, атап айтқанда АҚШ, Ұлыбритания, Канада, Ресей Федерациясы, Үндістан, Эстония. Тұжырымдамада заңнамалық, нормативтік-әдістемелік, ұйымдастырушылық, технологиялық және кадрлық қамтамасыз етуді қамтитын ақпараттық қауіпсіздікті қамтамасыз ету мәселелерін іске асыруға халықаралық тәжірибеге сәйкес кешенді тәсіл қолданылды.

Тұжырымдама ережелеріне 2008 жылғы 10 қазанда Бішкек қаласында қол қойылған ақпараттық қауіпсіздікті қамтамасыз ету саласындағы Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің ынтымақтастық тұжырымдамасының, 2010 жылғы 1 маусымдағы Қазақстан Республикасының Заңымен ратификацияланған Шанхай Ынтымақтастық Ұйымына мүше мемлекеттердің үкіметтері арасындағы Халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімнің негізгі бағыттары енгізілген. «Шанхай Ынтымақтастық Ұйымына мүше мемлекеттердің үкіметтері арасындағы Халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімді ратификациялау туралы».

Тұжырымдама мемлекет пен қоғамның ақпараттық қауіпсіздігін қамтамасыз ету, оларды ішкі және сыртқы қатерлерден қорғау жөніндегі Қазақстан Республикасы қызметінің мәні мен мазмұнына ресми көзқарастардың жиынтығын білдіреді. Тұжырымдама жеке тұлғаның, қоғамның және мемлекеттің ақпараттық қауіпсіздігін қамтамасыз ету саласындағы міндеттерді, басымдықтарды, бағыттарды және күтілетін нәтижелерді айқындайды. Ол Қазақстан Республикасының ақпараттық саладағы ұлттық мүдделерін қорғау үшін мемлекеттік билік органдарының, бизнес пен қоғамдық бірлестіктердің сындарлы өзара іс-қимылы үшін негіз

болып табылады. Тұжырымдама ақпараттық қауіпсіздікті қамтамасыз етудің мемлекеттік саясатын қалыптастыру мен іске асырудағы тәсілдердің бірлігін, сондай-ақ осы саланы реттейтін нормативтік құқықтық актілерді жетілдірудің әдіснамалық негізін қамтамасыз етуге арналған.

Экономикалардың ашықтығының, тауарлардың, капиталдардың және еңбек ресурстарының еркін қозғалысының, тұлғааралық өзара іс-қимылдың өсіп келе жатқан дәрежесі ішкі және сыртқы саяси, экономикалық және ақпараттық процестер арасындағы шекараны бұлдыратады. Технологиялық эволюция жеке адамға, қоғамға және мемлекетке теріс әсер етудің бұрын қол жетімді емес мүмкіндіктерін ұсына отырып, түбегейлі жаңа қауіптердің қайнар көзіне айналады. Бұқаралық ақпарат құралдары мен жаһандық коммуникациялық тетіктердің рөлі мен ықпалы күшейе түсуде. Ақпараттық технологиялар өмірді қолдаудың маңызды объектілерін басқаруда кең қолданысқа ие болды, олар кездейсоқ және қасақана әсерлерге осал бола бастады. Қазақстан Республикасының 2016 жылға дейінгі Ақпараттық қауіпсіздік тұжырымдамасы оның ақпараттық қауіпсіздігін қамтамасыз ету мақсатында елдің алдында тұрған негізгі стратегиялық мақсаттарды, міндеттер мен бағыттарды айқындайды. Тиісінше, ақпараттық қауіпсіздікті дамытудың саяси-құқықтық аспектілерінің тұжырымдамалық көрінісі қазіргі заманғы қатерлерді жан-жақты талдаудың, сондай-ақ оларды қазіргі әлемдік қоғамдастықтың жетекші мемлекеттерін жою жөніндегі шаралардың нәтижесі болып табылады.

Қазақстандағы қауіпсіздікті қамтамасыз ету саласындағы қатынастарды реттейтін негізгі нормативтік-құқықтық акт Қазақстан Республикасының Ұлттық қауіпсіздік саласындағы құқықтық қатынастарды реттейтін және адам мен азаматтың, қоғам мен мемлекеттің қауіпсіздігін қамтамасыз етудің мазмұны мен қағидаттарын, Қазақстан Республикасының ұлттық қауіпсіздігін қамтамасыз етудің жүйесін, мақсаттары мен бағыттарын айқындайтын «Ұлттық қауіпсіздік туралы» Қазақстан Республикасының Заңы болып табылады. Ұлттық қауіпсіздік түрлерінің ішінде ақпараттық қауіпсіздік жеке түр ретінде ерекшеленеді. Ақпараттық қауіпсіздік – Қазақстан Республикасының ақпараттық кеңістігінің, сондай-ақ ақпараттық саладағы адам мен азаматтың, қоғам мен мемлекеттің құқықтары мен мүдделерінің елдің орнықты дамуы мен ақпараттық тәуелсіздігі қамтамасыз етілетін нақты және әлеуетті қатерлерден қорғалу жағдайы. Осы Заңның 6- бабында ұлттық қауіпсіздікке төнетін негізгі қатерлер арасында мыналар айқындалады: елдің ақпараттық кеңістігінің, сондай-ақ ұлттық ақпараттық ресурстардың рұқсатсыз қол жеткізуден қорғалу деңгейінің төмендеуі; ұлттық қауіпсіздікке нұқсан келтіретін жалған ақпаратты қасақана бұрмалаумен және таратумен байланысты қоғамдық және жеке санаға ақпараттық әсер ету. Тиісінше, қауіпсіздік деңгейі ұлттық қауіпсіздіктің сапасын анықтайды, бұл қазіргі заманғы қауіптердің алдын алу шаралары мен олардың алдын алу және жою шараларының тиімділігін бағалауға мүмкіндік береді. Ақпараттық кеңістік саласында бұл қауіптер әсіресе қауіпті, өйткені адамда ақпарат арқылы қоршаған әлем туралы түсінік, оның дүниетанымы және белгілі бір әрекеттерге ынталандырушы мотивтер қалыптасады.

«Ақпараттық коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 12.12.2016 № 832 Қаулысында ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар (БТ) белгіленген. БТ ережелері ақпараттық қауіпсіздікті қамтамасыз ету саласына жатады, Мемлекеттік органдардың, жергілікті атқарушы органдардың, мемлекеттік заңды тұлғалардың, квазимемлекеттік сектор субъектілерінің, мемлекеттік органдардың ақпараттық жүйелерімен интеграцияланатын немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік емес ақпараттық жүйелердің меншік иелері мен иелерінің, сондай-ақ ақпараттық қауіпсіздіктің аса маңызды объектілерінің меншік иелері мен иелерінің қолдануы үшін міндетті.

Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі тәсілдері, осы саладағы қауіптер туралы хабардар болу мемлекеттерді тұтастай алғанда ұлттық қауіпсіздікті қамтамасыз етуге деген ұмтылыстарында жақындастыратынын атап өткен жөн. Бұл ұлттық қауіпсіздіктің негізгі тәсілдерінің және оны Ресей мен Қазақстанда жүзеге асыру қағидаттарының бірегейлігіне байланысты. Кеден одағына бірігу Ресей мен Қазақстанды барған сайын жақындастырып,

олардың даму жолдарына мемлекетаралық ынтымақтастық арқылы ғана жоюға болатын жаңа қауіптер қояды.

8.4. Электрондық цифрлық қолтаңба. Шифрлау. Киберқауіпсіздік индустриясы

Ақпараттық технологиялардың арқасында қазір әртүрлі қызметтерді электронды түрде алуға болады. Электрондық қызметтерді алудағы маңызды сәттердің бірі – электрондық цифрлық қолтаңба (ЭЦҚ) болып табылады. Ол электрондық түрде алынған құжаттардың заңды маңыздылығын анықтау және растау құралы ретінде қолданылады.

Электрондық цифрлық қолтаңба – бұл қолтаңбаның аналогы. ЭЦҚ электрондық құжатқа заңды тұлғаның өз қолымен қол қойған және мөрмен бекітілген қағаз жеткізгіштегі құжаттың заңды күшіне тең заңды күш беру үшін пайдаланылады.

ЭЦҚ – электрондық тіркеу куәлігін (сертификатын) және ЭЦҚ жабық кілтін пайдаланатын, ақпаратты криптографиялық түрлендіру нәтижесінде алынатын электрондық құжат. ЭЦҚ сертификаты мен жабық кілті SMART- картада шығарылады, ЭЦҚ жабық кілтін көшіруді және осы ақпараттың тұтастығын бұзуды болдырмайды. SMART картасы PIN кодымен қорғалған, оны тек ЭЦҚ иесі пайдалана алады. Сертификат иесін анықтай отырып, ЭЦҚ электрондық құжатты қолдан жасаудан қорғауға, ондағы ақпараттың бұрмаланбауын анықтауға мүмкіндік береді.

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 дәлелдейтін 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. ЭЦҚ

артықшылықтары:

1) облыстың ғана емес, республиканың да мемлекеттік органдарының Виртуалды қабылдау бөлмелеріне өтініштерді жүзеге асыруға (бұл сервис Қазақстан Республикасы азаматтарының өз өтініштерін мемлекеттік органдарға беру мүмкіндігін береді және өтініштің мәртебесін қадағалау мүмкіндігін беретін мемлекеттік орган тарапынан жауапқа кепілдік береді: мемлекеттік органға жеткізілді, орындауға берілді, орындалды және басқалар);

2) мемлекеттік қызметтерді үйден шықпай-ақ, аптасына 7 күн тәулігіне 24 сағат алуға;

3) электрондық сауда-саттықта, аукциондарда және тендерлерде, тауарлар мен көрсетілетін қызметтердің неғұрлым тиімді баға ұсынысын ұсынуға және таңдауға құқылы.

Электрондық цифрлық қолтаңбаны (ЭЦҚ) халыққа қызмет көрсету орталығының жанында орналасқан ұлттық куәландырушы орталықтың тіркеу орталықтарынан немесе Қазақстан Республикасының Ұлттық куәландырушы орталығының сайтында онлайн өтінімді ресімдеу арқылы мына мекенжай бойынша алуға болады: www.pki.gov.kz (сурет 8.1).

Электрондық цифрлық қолтаңбаны келесі сақтау түрлері бойынша алуға болады:

1) **файлдық жүйе** – осы тармақты таңдаған кезде кілттер мен тіркеу куәліктері пайдаланушының дербес компьютерінде файлдар түрінде сақталатын болады;

2) **Kaztoken** – осы жеткізгішті таңдау кезінде кілттер мен тіркеу куәліктері пин кодтың көмегімен қорғалған негізгі ақпараттың сыртқы қорғалған жеткізгішінде сақталатын болады;

3) **Sim-картадағы ЭЦҚ** – осы тасымалдағышты таңдау кезінде кілттер мен тіркеу куәліктері клиенттің телефонының sim-картасында сақталатын болады. Тиісті SIM-картаны «Азаматтарға арналған үкімет» КАҚ және Beeline сату бөлімдерінен Астана, Алматы қалаларындағы филиалдарынан сатып алуға болады.

4) **жеке куәлік** – жеке куәлік чипіне (жеке тұлғалар үшін) ЭЦҚ жазу үшін жеке куәлікті

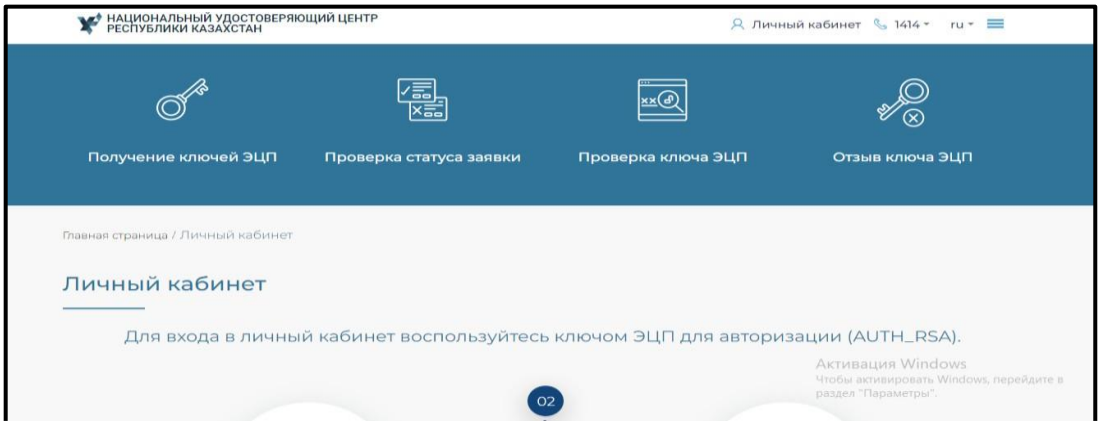
көрсете отырып, «Азаматтарға арналған үкімет» мемлекеттік корпорациясы (ХҚКО) жақын жердегі бөліміне жүгіну қажет. Жеке куәлікте жазылған ЭЦҚ-мен одан әрі жұмыс істеу үшін картридер сатып алу қажет [3, 217-220 бб.].

Шифрлау

Шифрлау – бұл деректерді шифрланған мәтінге түрлендіру үшін қолданылатын әдіс, оны тек мазмұнды транскрипциялау үшін тиісті шифрлау кілті бар пайдаланушы оқи алады. Шифрлау деректерді қорғаудың жоғары деңгейі қажет болған кезде деректерді сенімсіз көздерден сақтау немесе қорғалмаған байланыс арналары арқылы деректерді беру кезінде қолданылады.

Қолданылатын кілттердің құрылымына байланысты шифрлау әдістерінің арасында симметриялы шифрлау және асимметриялық шифрлау ерекшеленеді.

Симметриялық шифрлау – шифрлау алгоритмінің бөгде адамдарға қол жетімділігін қамтамасыз етеді, бірақ кілт (жіберуші мен алушы үшін бірдей) белгісіз болып қалады.



Сурет 8.1. Қазақстан Республикасының Ұлттық куәландырушы орталығының сайты

Деректерді шифрлау және шифрын ашу үшін симметриялық шифрлау бірдей криптографиялық кілтті пайдаланады. Бұл әдіс криптографияда кең таралған, өйткені жұмыс істеу және түсіну өте қарапайым, жабдыққа техникалық жүктеме аз, сондықтан шифрлаудың жоғары жылдамдығы мен сенімділігі қамтамасыз етіледі.

Кемшіліктерге кілттерді бөлісудің қиындығы жатады: егер кілт сәтті ұсталса, шабуылдаушы шифрланған ақпаратқа шексіз қол жеткізе алады.

Симметриялық шифрлаудың негізін 56 биттік кілттерді қолданатын DES (Data Encryption Standard) алгоритмі құрды, бұл осы алгоритмнің әртүрлі шабуылдарға қарсы тұру қабілетіне қатысты пікірталастар тудырды. Бұл стандарт 2000-шы жылдардың басына дейін, кілттің ұзындығы 128, 192 немесе 256 бит болатын жетілдірілген AES (Advanced Encryption Standard) ауыстырылғанға дейін қолданылды.

Асимметриялық шифрлау – кезінде бөгде адамдар шифрлау алгоритмі мен ашық кілтті біледі, алайда жеке кілт тек алушыға белгілі.

Асимметриялық шифрлау – бұл ашық және жабық екі кілтті қолдануды қамтитын деректерді шифрлау әдісі. Ашық (жалпыға ортақ) кілт ақпаратты шифрлау және электрондық қолтаңбаны тексеру үшін қолданылады. Жеке кілт ашық кілтпен шифрланған деректерге қол қою және шифрын ашу үшін қолданылады. Ашық және жеке кілттер – бұл белгілі бір функциямен байланысты өте Үлкен сандар, бірақ біреуін біле отырып, екіншісін есептеу өте қиын.

Ашық кілтпен шифрланған ақпарат, ашық кілттің өзі сияқты, қорғалмаған байланыс арналары арқылы берілуі мүмкін. Мұндай схемада кез-келген деректерді ұстап алудың мағынасы жоқ, өйткені бастапқы ақпаратты тек иесіне белгілі және беруді қажет етпейтін жеке кілттің көмегімен қалпына келтіруге болады.

Асимметриялық шифрлаудың ең көп таралған алгоритмі – үлкен бүтін сандарды факторизациялау мәселесінің есептеу күрделілігіне негізделген RSA алгоритмі. RSA кілтінің ұзындығы теориялық тұрғыдан шектелмейді, бірақ әдетте 1024-тен 8192 битке дейін.

Интернетке қосылған құрылғылар ұйымның тиімділігін едәуір жақсартады, бірақ Интернетке қосылған барлық заттар сияқты, олар кибершабуылдарға осал болуы мүмкін. Киберқылмыскерлер IoT экожүйесінің әртүрлі нүктелерінен жиналған ақпаратты пайдаланудың жолын таба алады. Интернет заттары технологиясының қауіпсіздігіне байыпты қарау керек.

Мобильді құрылғылар күрделі құпия сөзбен немесе биометриялық құпия сөзбен қорғалуы керек, егер ол жоғалған немесе ұрланған болса, құрылғыға ешкім кіре алмайды. Хакерлерге жүйеге және деректерге қол жеткізуге мүмкіндік беретін барлық вирустардан қорғайтын құрылғылар үшін автоматты антивирустық жаңартуды орнатыңыз, кибер құрылғыларды шабуылдан қорғау үшін автоматты антивирустық жаңартуды орнатыңыз. Әр түрлі құрылғыларда бірдей логиндер мен парольдерді қолдануға болмайды, сондықтан оларды киберқылмыскерлерге бұзу оңайырақ.

Қосылған құрылғылар бір-бірімен байланысады және олар байланыс жасаған кезде деректер бір құрылғыдан екіншісіне беріледі. Әр қиылысу нүктесінде деректерді шифрлау керек. Басқаша айтқанда, ақпаратты нүктеден нүктеге жылжыту кезінде қорғау үшін ақырғы шифрлауды (end-to-end шифрлау) пайдалану керек.

Шифрлау – бұл хабарламаларға тек жіберуші мен адресат қол жеткізе алатын ақпаратты беру тәсілі. Хабарлама шифрланған, барлық аралық кезеңдерде хабарлама түсініксіз таңбалар жиынтығы сияқты көрінеді, ал шифрлау кілті тек хат алмасуға қатысушылардың құрылғыларында болады. Егер үшінші тұлғалар ақпаратқа қол жеткізгісі келсе, онда олар оны шеше алмайды. Шифрлау WhatsApp, Viber, iMessage, Signal, Wire қосымшаларында қолданылады. Telegram, Skype және Facebook Messenger сияқты басқа танымал мессенджерлер де қосуға мүмкіндік береді (құпия чаттар деп аталатын шифрлау). Әдепкі бойынша, бұл мессенджерлерде түпкілікті шифрлау өшірілген. Instagram, VK және Twitter сияқты әлеуметтік желілердегі жазбалар шифрлауды қолдамайды.

Шифрлау – рұқсатсыз кіруді болдырмау үшін ақпаратты кодтау процесі. Ұрланған жағдайда, шифрланған деректерді тиісті кілтсіз оқу мүмкін болмайды. Шифрлауды кодтаудан ажырату қажет. Кодтау сонымен қатар ақпаратты түрлендіреді, бірақ сақтау мен тасымалдаудың қарапайымдылығы үшін құпиялылық негізгі міндет емес. Кодтаудың әдеттегі әдістері – Морзе коды және компьютерде сақтау үшін әріптерді екілік кодтау. Бүгінгі таңда компьютердегі файлдарды шифрлаудың ең ыңғайлы шешімі – жүйеде бөлек диск ретінде көрінетін «контейнер» жасау. Бұл дискіге кез-келген ақпаратты сақтауға немесе көшіруге болады, онымен кез-келген бағдарламадан жұмыс істеуге болады, ол флэш-дискіден немесе қатты дискінің бөлімінен ыңғайлы емес [3, 220-222].

8.5. Киберқауіпсіздік және Интернетті басқару

Киберқауіпсіздік желілер мен мәліметтердің, бағдарламалардың біртұтастығын кибер шабуылдардан (цифрлық шабуылдардан) қорғау технологияларының, әдістемелер мен процестердің жиынтығын білдіреді.

Киберқауіпсіздік қауіптің үш түрімен күреседі:

- Киберқылмыс – жүйеден қаржылық пайда табу, оның жұмысын бұзу немесе шабуыл жасау мақсатында бір немесе бірнеше шабуылдаушылар ұйымдастырған әрекеттер.
- Кибершабуыл – негізінен саяси сипаттағы ақпараттар жинауға бағытталған әрекеттер.
- Кибертерроризм – қорқыту немесе үрейлендіру мақсатында электрондық жүйелерді тұрақсыздандыруға бағытталған әрекеттер.

Құқық бұзушылар құпия ақпаратты заңсыз көшіріп алу немесе редакциялау (жою немесе түрін өзгерту) мақсатымен (рұқсат етілмеген) кибершабуыл жасайды. Оны негізінен, адамдардан (ақпараттық жүйелерді пайдаланушылардан) қаржыны ұрлау немесе ұйымдағы өндірістік немесе жұмыстық процестерді бұзу, тіпті мемлекеттік

құпияларды ұрлау мақсатында жүзеге асырады.

Кибертерроризмнің негізгі мақсаты – әлеуметтік, экономикалық және саяси мәселелерді шешуге әсер ету. Әлемде заттар интернетінің «ақылды» құрылғыларының саны қарқынды өсеуде. Олардың барлығы террор немесе бопсалау мақсатында мақсатты шабуылдарға жол ашады – әсіресе қазір көптеген зауыттар мен фабрикалар мұндай құрылғыларды технологиялық процесті басқарудың автоматтандырылған жүйелерінде (АБЖ III) пайдаланады. Киберқылмыскерлер халықты террор мақсатында бұзып алуы мүмкін: мысалы, цехтың істен шығуын немесе АЭС жарылысын ұйымдастыру [16].

Өз акцияларында қылмыскерлер заманауи техногиялардың барлық мүмкіндіктерін, соның ішінде заманауи гаджеттер мен бағдарламалық өнімдерді, электронды құрылғыларды, басқа салалардағы жетістіктерді (микробиология мсн гендік инженерияға дейін) белсенді қолданады. Ресми түрде, кибертерроризм-бұл бір адамның немесе бірнеше қатысушыдан тұратын тәуелсіз топтардың жасаған әрекеттері. Егер осы анықтамаға жататын іс-әрекеттерге үкіметтердің немесе өзге де 31 мемлекеттік құрылымдардың өкілдері қатысса, бұл кибер соғыс көріністері болып саналады.

Кибертеррористердің әрекеттері мыналарға бағытталған:

- компьютерлік жүйелерді бұзу, жеке және банктік ақпаратқа қол жеткізу;
- әскери және мемлекеттік деректер құпиялылығы;
- жабдықтар мен бағдарламалық қамтамасыз етуді істен шығару, кедергілер жасау, электрмен қоректендіру желілері жұмысының бұзылуы;
- компьютерлік жүйелерді бұзу, вирустық шабуылдар, бағдарламалық бетбелгілер арқылы деректерді ұрлау;
- ашық қолжетімділікке құпия ақпараттың тарауы;
- түсірілген медиа арналар арқылы жалған ақпарат тарату;
- байланыс арналары жұмысының бұзылуы және басқалар.

Қауіптер ақпаратқа зиян келтіру салдарынан заңсыз пайда алу мақсатында іске қосылады. Бірақ қауіпті фактордың жеткіліксіз қорғалуына және жаппай әрекет етуіне байланысты кездейсоқ қауіп-қатер болуы мүмкін.

Қазіргі таңда бірқатар ұйымдар мен үкіметтік мекемелерде жұмысқа қажетті ақпаратты, сондай-ақ қызметкерлердің, пайдаланушылардың және т.б. жеке мәліметтерін жинау, өңдеу және сақтау жолға қойылған. Ал бұл ақпаратты қорғауды қажет етеді, себебі жеке ақпарат құпия болуы керек. Ақпараттардың жоғалуы мен ұрлануы адамдар, ұйымдар және тіпті мемлекет үшін де кері салдарға әкелуі мүмкін.

Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны») Қазақстанның әлемнің ең дамыған 30 мемлекетінің қатарына ену бойынша «Қазақстан 2050» стратегиясының тәсілдерін ескере отырып, Қазақстан Республикасы Президентінің «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Жолдауына сәйкес әзірленді.

Әлеуметтік желілердегі қауіпсіз қарым-қатынастың ережелері. Қазіргі күнде қоғам мүшелері әлеуметтік желілерін тұрақты пайдаланауда, Вконтакте, Одноклассники, Фэйсбук, Твиттер, Тик-ток т.б. сияқты әлеуметтік желілерді пайдаланушылар күн сайын артуда. Әлеуметтік желілердің көмегімен адамдар бір-бірімен мәліметтер, фотосуреттер және т.б. қарым-қатынас жасап, мәлімет алмасады. Мұндай ресурстар танымал бола бастаған сайын, алаяқтар да оларға көбірек қызығушылық танытады. Осы орайда әлеуметтік желілерді пайдалану қауіпті бола түседі.

Әлеуметтік желілерді пайдаланудағы қауіптер:

1. Жеке ақпараттарды (оның ішінде, басқа адамдарға тиістілерін) жария ету. Бұған тіпті мәліметтердің таралуына себепші болатын дос-жаранға жіберген хабарламалар да жатады. Бұл жеке ақпаратты қорғау саласындағы құқық бұзушылықтар тізбегін құрайды.

2. Қауіпті таныстықтар. Желіде кәмілет жасына толмағандармен хат алмасу барысында азғыруды жүзеге асырса, ал кейбіреулер жеке кездесуге алдап көндіруі мүмкін.

3. Қылмыскерлердің назарын аудару. Желі қолданушыларының, жасөспірімдердің өз өміріндегі барлық оқиғаны әлеуметтік желілерде жария етуі. Статусқа жарияланған мілңметтер мен фотосуреттер бойынша бала мен оның отбасы мүшелері қай жерде болатынын, баланың жалғыз қалатынын, қай кезде үй-жайларының қараусыз қалатыны жайында мәлімет білуге болады.

4. Жұмыс іздеу, музыка, видеожазба және т.б. әртүрлі мәліметтерді көшіріп алуға мүмкіндік береді дейтін таныс емес қосымшалардың қауіпсіздігіне сенімді болмай, оларды орнатудың қажеті жоқ. Ол қосымшалар орнату кезінде жеке акаунттан логин мен пароль сұрату арқылы хакерлерге жеке ақпаратқа қолжеткізуіне мүмкіндігін береді.

5. Басқа компьютерлерден, тіпті ол танысыңның компьютері болса да, әлеуметтік желілердегі жеке аккаунттарды ашпау. Өйткені онда сенің аккаунтың туралы мәліметтерді жіберетін вирус болуы мүмкін.

6. Әлеуметтік желілерге жеке басың туралы ақпаратты орналастыру кезінде мұқият болған жөн. Алаяқтар көбіне құпия сұраққа жауап беруді өтінетін «Парольді ұмыттыңыз ба?» батырмасын пайдалану арқылы аккаунттарды бұзады.

7. Әлеуметтік желіге кіру кезінде тек браузердің мекенжай жолын немесе қосымшасын пайдалану керек. Интернеттегі күмәнді сілтеме бойынша әлеуметтік желіге өту жағдайында жеке мәліметтерді ұрлау үшін пайдаланылатын сайтқа түсу тәуекелі туындайды.

8. Жұмыс орнында әлеуметтік желілерді пайдаланбау қажет. Әлеуметтік желі тыңшылық бағдарламаларды немесе вирустарды таратуы, олар құпия мәліметтердің жоғалуына әкеліп соғуы мүмкін [16].

Бақылау сұрақтары:

1. «Ақпараттық қауіпсіздік» түсінігіне анықтама беріңіз.
2. Ақпарат қауіпсіздігіне қауіпті қалай түсінесіз?
3. Ақпарат қауіпсіздігіне қандай қауіптер мәлім?
4. Киберқауіпсіздік термині нені білдіреді?
5. Әлеуметтік желілерді пайдаланудың қандай қауіптілігі бар?
6. Әлеуметтік желілерді пайдалану кезінде алдын ала сақтанудың қандай іс-шараларын қабылдау керек?

Оқытудың техникалық құралдары: Компьютерлер мен ноутбуктер, интерактивті тақта, проектор мен экран, интернет желісі.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері: баяндау, сұрақ-жауап, түсіндіру, кіріспе лекция.

БӨЖ және ОБӨЖ тапсырмалары, олардың түрлері мен орындалуына қойылатын ұпайлардың үлестері:

1. Компьютерлік желілердің түрлерін (LAN, MAN, WAN) сипаттап, олардың айырмашылығын кесте түрінде көрсетіңіз.
2. Желі топологияларының (жұлдызша, сақина, шина, аралас) артықшылықтары мен кемшіліктерін салыстырмалы талдау жасаңыз.
3. TCP/IP және OSI модельдерінің деңгейлерін салыстыру кестесін құрастырып, әр деңгейдің функцияларын түсіндіріңіз.
4. IP-адрестеудің құрылымын және маскамен жұмыс істеу мысалын келтіріңіз.
5. DHCP хаттамасының жұмыс принципін сызба түрінде бейнелеңіз.

Интернетке қосылу технологияларын (DSL, спутниктік, Wi-Fi, LTE, 5G) зерттеп, олардың жылдамдығын және қолдану аймағын салыстырыңыз.

БӨЖ бағалау критерийлері:

- Теориялық материалды түсіну және қолдану -20 балл

- Бағдарламаны дұрыс жазу немесе есепті шешу -25 балл
- Нәтижелердің дәлдігі мен түсіндіру сапасы -15 балл

Барлығы: 60 балл

ОБӨЖ бағалау критерийлері:

- Тапсырманың толық және уақытылы орындалуы -15 балл
- Теориялық және практикалық түсіндіру сапасы -15 балл
- Топтық жұмысқа белсенді қатысу, сұрақтарға жауап беру-10 балл

Барлығы: 40 балл

Жалпы бағалау үлесі:

- **БӨЖ — 60% (60 балл)**
- **ОБӨЖ — 40% (40 балл)**

Пайдаланылған әдебиеттер тізімі:

Негізгі:

1. Болашақ мамандардың ақпараттық-коммуникативтік құзырлығын қалыптастыру: Монография. К. М. Беркимбаев, Б. Т. Керимбаева. Түркістан, 2017.
2. Information-communication technology. 2016. Urmashev B.A.
3. Information technologies for professional purposes. Laboratory works. 2016 Davletova V., Bayterekova N.

Қосымша:

1. Молдабекова Б.Қ. Ақпараттық-коммуникациялық технологиялар: Оқу құралы. - Қарағанды: Қазтұтыну одағы Қарағанды экономикал

Пайдаланылған әдебиеттер тізімі:

Негізгі:

2. Нурпеисова Т. Б., Кайдаш И. Н. Ақпараттық-коммуникациялық технологиялар. Оқу құралы. 2018.
3. Сапарходжаев Н. П., Ниязова Г.Ж., Рахмет Ү.Р. Білім берудегі ақпараттық-коммуникациялық технологиялар. Оқу құралы. Шымкент, 2020.
4. Камалова Г.А., Диярова Л.Б. Ақпараттық қауіпсіздік және ақпаратты қорғау. «Альманах» баспа үйі. Алматы, 2019
5. Камалова Г.А., А.Х. Касымова, Диярова Л.Б. Ақпараттық қауіпсіздікті басқару. «Альманах» баспа үйі. Алматы, 2020
6. Компьютерлік желілер. Бекмагамбетова Г.М. Оқу құралы. Алматы. 2021
7. Мауленов С.С., Аймешов Ж.А.. Интернет технологиялары: Оқу-әдістемелік құрал. Түркістан, 2017.
8. Ахметов О.С.. Информатика. Учебно-методический комплекс. 2022г. Алматы,
9. Болашақ мамандардың ақпараттық-коммуникативтік құзырлығын қалыптастыру: Монография. К. М. Беркимбаев, Б. Т. Керимбаева. Түркістан, 2017.
9. Information-communication technology. 2016. Urmashev B.A.
10. Information technologies for professional purposes. Laboratory works. 2016 Davletova V., Bayterekova N.

Қосымша:

2. Молдабекова Б.Қ. Ақпараттық-коммуникациялық технологиялар: Оқу құралы. - Қарағанды: Қазтұтыну одағы Қарағанды экономикалық университеті, 2018. - 158 б. rmebrk.kz
3. Жаркимбекова А.Т. т.б. Ақпараттық-коммуникациялық технологиялар: Электрондық оқулық. / А.Т. Жаркимбекова, Ж.Б. Кадирова С.Р. Жақсыбаева. - Қарағанды: ҚарМТУ, 2019. rmebrk.kz
4. Әділбекова Э.Т., Бәймішева А.Ж. Білім берудегі ақпараттық-коммуникациялық технологиялар: Оқу құралы. Шымкент, 2014. - 112 б. rmebrk.kz
5. М.Ф.Баймухамедов, А.М.Баймухамедова, С.Н.Боранбаев. Жасанды интеллект. Оқулық. 2 бөлім – Алматы: «Бастау». 2020
6. Информационно-коммуникационные технологии : Учебник: В 2-х частях. Ч. 2, - Алматы: МУИТ, 2017. - 624 с., http://rmebrk.kz

ық университеті, 2018. - 158 б. rmebrk.kz

7. Информационно-коммуникационные технологии : Учебник: В 2-х частях. Ч. 2, - Алматы: МУИТ, 2017. - 624 с., http://rmebrk.kz