**КИБЕРҚАУІПСІЗДІК**

**Ақпарат қауіпсіздігінің тәуекелдері және олардың жіктемелері. Киберқауіпсіздік индустриясы. Киберқауіпсіздік және Интернетті бақылау. Зиян келтіретін қосымшалар. Ақпаратты қорғау шаралары мен құралдары. Ақпараттық қауіпсіздік саласындағы стандарттар мен ерекшеліктер. Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы құқықтық қатынастарды реттейтін актілері. Цифрлық қолтаңба. Кодтау.**

**Киберқауіпсіздік. Ақпарат қауіпсіздігінің тәуекелдері және олардың жіктемелері.**

Бүгінде біз адамзат тарихының ең трансформациялық кезеңдерінің бірінде тұрамыз, мұнда барлығы өзара әрекеттескен. Және де бұл байланыстық ақпараттық желі біздің күнделікті өміріміздің ажыратылмас бөлігі болып табылады. Мемлекеттік, медициналық, қаржылық және білім беру мекемелері сияқты, барлық ұйымдар бұл желіні тиімді жұмыс үшін пайдаланады. Күн сайын осы барлық ұйымдар цифрлық ақпараттың көптеген санын жинайды, өңдейді, сақтайды және алмасады. Цифрлық ақпараттың бұдан да көп санын жинауы мен таратуына қарай, бұл ақпаратты қорғау біздің ұлттық қауіпсіздігіміз және экономикалық тұрақтылығымыз үшін маңыздылығы арта түседі.

Киберқауіпсіздік – бұл компьютерлерді, серверлерді, мобильді құрылғыларды, электрондық жүйелерді, желілерді және олардың ішіндегі барлық деректерді зиян келтіретін атакалардан қорғауға тырысу. Бұгінде барлық елдер өздерінің азаматтарын және инфрақұрылымды қорғауға көмектесу үшін, киберқауіпсіздік жөніндегі мамандарға мұқтаж.

Ақпараттық және коммуникациялық технологиялардың дамуы және Интернетке қолжетімділіктің кеңеюіне орай, ұйымдар қауіптердің алуан түрлері алдында осал болады. Қауіптер кибератакалар немесе қызметкерлердің қызметі сияқты әртүрлі көздерден туындайды. Өздерінің деректерін немесе активтерін қорғағысы келетін барлық адамдар немесе ұйымдар олар ұшырайтын тәуекелдерді білуі және де тиісті контршараларды таңдап, атакаларға жол бермеу үшін нені жасау керектігін анықтау үшін, олардың әсер етуін айырып тануы тиіс. Тәуекелдердің жіктемесі ұйымдар үшін маңызды, өйткені ақпараттық қауіпсіздікті қамтамасыз ету жолында маңызды қадам болып табылады. Тәуекел ішкі және сыртқы объектілермен туындауы мүмкін.

Ішкі тәуекелдер біреудің сервердегі есептік жазба арқылы немесе желіге физикалық қолжетімділік арқылы желіге қолжетімділігі болған кезде туындайды. Бұл қызметкердің әрекеттерінің немесе ұйымдастырушылық процесс іркілісінің нәтижесі болуы мүмкін.

Сыртқы тәуекелдер компаниядан тыс жерде адамдардан немесе ұйымдардан болады. Олардың компьютерлік жүйеге немесе желіге авторластырылған қолжетімділігі жоқ. Сондай-ақ жер сілкінісі, су тасқындары немесе өрт сияқты табиғи апаттар да сыртқы тәуекелдерге жатады. Сыртқы атакалар қосылған желілер, физикалық басып кіру немесе серіктестік желісі арқылы орын алады.

Ақпараттық жүйенің қауіпсіздігіне негізделген тәуекелдердің жіктемесін келесі түрлерге бөлуге болады:

1. Жаңылысулар және олқылықтар – әдетте адамдардың қателіктерінен туындайтын қауіпсіздікке қауіптің бір түрі.

2. Алаяқтық және ұрлық – алаяқтықтың және ұрлықтың әртүрлі заманауи нысандарын пайдалана отырып жүзеге асырылуы мүмкін қауіпсіздіктің бір түрі.

3. Қызметкердің саботажы – компанияда жұмыс істейтін адам ақпараттық жүйе ресурстарының тәуекеліне ұшырайтын кездегі қауіпсіздікке қауіптің бір түрі.

4. Физикалық инфрақұрылымды жоғалту – бұл электр қуатын ажыратумен, байланыстың жоғалуымен, жер сілкінісімен, өртпен, ереуілдермен және т.б, туындауы мүмкін қауіпсіздікке қауіптің бір түрі.

5. Хакерлер – адамдардың рұқсат етілмеген тәсілмен қолжетімділікті алуға және жүйелік ресурстрды пайдалануға тырысатын кездегі қауіпсіздікке қауіптің бір түрі.

6. Зиян келтіретін БЖ – бұл компьютерлік вирустардың, трояндық бағдарламалардың, құрттардың, логикалық бомбалардың алуан түрі және «жағымсыз» бағдарламалық жасақтаманың басқа да нысандары кіретін қауіпсіздікке қауіптің бір түрі.

7. Жеке құпиялылыққа қауіп төндіру – бұл жеке деректердің көпшілігі әртүрлі тәсілдермен мақсаты емес бойынша пайдаланылуы мүмкін кездегі қауіптің бір түрі.

**Киберқауіпсіздік және Интернетті бақылау**

Қазіргі таңда әлеуметтік желілер Интернеттің рөлін өзгертеді. Бірінші кезде біз Интернетте біздің жүріс-тұрысымызды бақылай алдық және де біздің кім болғымыз келеді, сол болу мүмкіндігіне ие болды. Біз басқалармен қандай ерекшеліктермен бөлісуді таңдап, шеше алдық. Бүгінгі күні, Интернеттің күн сайын өсуі салдарынан, оны бақылау қиын. Біздің оффлайн-сәйкестілік біздің онлайн-әрекеттерімізге тікелей байланысты. Біздің интернет-браузеріміздің, іздеу сұрау салуларымыздың және веб-парақшаларға, электрондық поштаға және әлеуметтік желілерге келушілер санының тарихы біздің жеке тұлғамыздың белгілі бір белгілерін айқындайды.

Сіздің онлайн-сәйкестілік – бұл сіз киберқауіпсіздікте кім боласыз, сол. Бұл сіздің Интернетте өзіңізді басқа адамға қалай таныстыруыңыз. Және де сіз Интернетте жеке ақпаратпен ұқыпты болуға тиіссіз. Сіздің пайдаланушының есімі бөтен адамдарды сіз – киберқылмыста немесе жағымсыз назар аудару үшін оңай нысана екен деп ойлауға мәжбүр етпеуі тиіс.

Сіз туралы барлық ақпаратты сіздің деректеріңіз деп санауға болады. Оған сіз отбасыңызбен, достарыңызбен немесе әріптестеріңізбен алмасатын фотосуреттер мен хабарламалар кіреді. Медициналық, білім беру, қаржылық, жұмыспен қамту бойынша ақпарат сізді Интернетте сәйкестендіру үшін пайдаланылуы мүмкін.

Біз туралы және біздің құпиялығымызды және деректерімізді қорғайтын түрлі заңдар бар, бірақ біз деректеріміздің қайда орналасқанын білмейміз.

**Зиян келтіретін бағдарламалар (вирус)**

Вирус – бұл деректерді ұрлау үшін пайдаланылуы мүмкін зиян келтіретін бағдарламалық жасақтама. Ол орындалатын кодтың, скрипттердің, белсенді контенттің немесе басқа да бағдарламалық жасақтаманың нысанын қабылдауы мүмкін. Осындай кодтар компьютерлік вирустар, құрттар, троян аттары, жарнамалық БЖ, бот*тар*, бопсалаушы-бағдарламалар және т.б. ретінде сипатталады.

*Компьютерлік вирус* - Вирус – бұл жиі заңды бағдарламаларға, басқа орындалатын файлдарға бекітілетін зиян келтіретін орындалатын код.

*Құрттар* – Құрттар желілердегі осалдылықтарды тәуелсіз пайдалана отырып, өзін көшірмелейтін зиян келтіретін код болып саналады.

*Троян аттары* – Троян аты – бұл қалаулы операцияның түрін алып, зиян келтіретін операцияларды орындайтын зиян келтіретін бағдарлама.

*Жарнамалық БЖ* – Жарнамалық БЖ – бұл онлайн-жарнаманы бағдарламалық жасақтаманың пайдаланушылық интерфейсінде генерациялайтын зиян келтіретін бағдарлама.

*Бот* - Бот – әдетте, Интернетте әрекеттерді автоматты түрде орындау үшін арналған зиян келтіретін бағдарлама.

*Бопсалаушы-бағдарлама* – Бопсалаушы-бағдарлама – бұл компьютерлік жүйені немесе оның ішіндегі деректерді төлем жүргізілгенше ұстап қалу үшін арналған зиян келтіретін бағдарлама.

*"Қызмет көрсетуден бас тарту" атакасы (DoS)* – бұл желілік атаканың түрі. Ол желіні сөндіреді және оны болжамды пайдаланушылар үшін қолжетімсіз етеді. DoS-атакалардың екі негізгі әдісі бар: "батыру" немесе "іркіліс".

"Батыру" – атака жасалатын жүйе сервердің өндіруге жағдайы жоқ трафиктің үлкен көлемімен шамадан тыс жүктелген кезде орын алады.

"Іркіліс" – Киберқылмыскерлер нысаналы жүйедегі кемшіліктерді пайдаланатын қателіктерді табыстайтын кезде орын алады.

*«Қызмет көрсетуден бас тарту» (DDoS) бөлінген атака* DoS-атакаға ұқсас, бірақ бірнеше үйлестіруші көзден нығады. Ол бірнеше жүйенің бір нысанаға синхрондалған DoS-атаканы ұйымдастырған кезде орын алады.

*Фишинг* – бұл нысанамен немесе нысанлармен электрондық пошта, телефон немесе мәтіндік хабарлама бойынша байланысатын киберқылмыс. Мысалы, бөлшек дүкеннен сыйлық алу үшін сілтеме бойынша ауысу өтініші бар электрондық хат. Сілтеме сізді жеке ақпаратты ұсыну өтінішімен жалған сайтқа аударуы немесе сайт вируты орнатуы мүмкін.

Сіз жүйеңіздің зиян келтіретін бағдарламалармен жұққанын қалай анықтай аласыз? Төменде зиян келтіретін бағдарламалардың жұғудың бірнеше белгілері келтірілген:

* Компьютер тежейді
* Файлдар өзгертілген немесе жойылған
* Іркілістер
* Жұмыс үстелінде белгісіз файлдардың, бағдарламалардың немесе белгішелердің болуы
* Белгісіз процестердің іске қосылуы
* Браузердің қателігі
* Интернет-трафикті арттыру
* Хаттар сіздің хабарынсыз жіберіледі

**Ақпаратты қорғау шаралары мен құралдары**

Ақпаратты және жеке деректерді қорғау үшін, сізге қарапайым маңызды қадамдарды ұстану қажет:

* Сіздің компьютеріңіздің брандмауэрын қосыңыз. Брандмауэр – бұл желіден сіздің компьютеріңізге қандай трафиктің кіре алатынын, ал қандай трафиктің кіре алмайтынын анықтайтын қауіпсіздік деңгейі. Әдетте, ол бұл ретте хакерлерді, зиян келтіретін БЖ және басқа да күмәнді трафикті жоққа шығарып, жақсы трафикті өткізеді.
* бұл желіде сіздің компьютеріңізге қандай трафиктің кіре алатынын, ал қандай трафиктің кіре алмайтынын анықтайтын қауіпсіздік деңгейі. Әдетте, ол хакерлерді, зиян келтіретін БЖ және басқа да күмәнді трафикті жоққа шығарып, жақсы трафикті өткізеді.
* Антивирусты пайдаланыңыз. Антивирустық бағдарламалық жасақтама сіздің компьютеріңізді сканирлеуге және вирустарды жоюға арналған. Электрондық пошта арқылы вирустарды тарату тәсіл – электрондық хатқа ашық салымдар, вирус жұққан веб-сайтқа кіру, орындалатын файлға немесе вирус жұққан жарнаманы қарауға басу.
* Өзіңіздің операциялық жүйеңізді және браузеріңізді басқарыңыз. Хакерлер әрдайым сіздің операциялық жүйелеріңізде және веб-браузерлеріңізде осал жерлерді пайдалануға тырысады. Ал сіздің деректеріңізді қорғау үшін сізге операциялық жүйелерді, оның ішінде веб-браузерді жаңарту, бағдарламалық жасақтаманың түпкілікті нұсқаларын орнатуға тырысу қажет.
* Сіздің барлық құрылғыларыңызды қорғаңыз. Сіздің компьютерлік техникаңызды, ДК, ноутбуктар, планшеттер, смартфондар болсын, рұқсат етілмеген қолжетімділікке жол бермеу үшін, құпиясөзбен қорғалуы тиіс. Сондай-ақ сіздің барлық құрылғыларыңызға бірдей құпиясөзді ешқашан пайдаланбаңыз.
* Сіздің деректеріңізді шифрлаңыз. Шифрлау – бұл ақпаратты оңай оқылатын және түсінікті форматтан рұқсат етілмеген тарап оқи алмайтын нысанға түрлендіру процесі. Нарықта файлдарды, папкаларды және тіпті тұтас драйверлерді шифрлау үшін арналған шифрлау құралдары ұсынылған.

Шифрлау құралдарын таңдау кезінде келесіні есепке алу қажет:

1. Шифрлаудың мақсаты, мысалы, файлдар, электрондқ хаттар және т.д.
2. Пайдаланушылық талаптар
3. Уақытша файлдарды өңдеу
4. Өрістету қарапайымдылығы
5. Пайдалану қарапайымдылығы
6. Кілттерді басқару және қалпына келтіру

Сіз келесі нұсқаулықтарды орындап, барлық Windows нұсқаларында өзіңіздің деректеріңізді Шифрланған файлдық жүйенің (EFS) көмегімен шифрлай аласыз:

1. Бір немесе бірнеше файлды немесе папканы таңдаңыз.
2. Таңдалған деректерде тінтуірдің оң жақ түймешігін шертіңіз>Қасиеттер.
3. Қосымша … дегенді басыңыз.
4. Деректерді қорғау үшін мазмұнды шифрлау жалаушасын орналыңыз.
5. EFS комегімен шифрланған файлдар мен
6. Папкалар суретте көрсетілгендей,жасыл түспен көрсетіледі.

Қазіргі таңда Google, Facebook, Twitter сияқты белгілі онлайн-сервистер аккаунтқа кіру үшін қауіпсіздіктің қосымша деңгейін қамтамасыз ету үшін екі факторлық түпнұсқаландыруды пайдаланады. Пайдаланушының есімінен және құпиясөзінен, дербес сәйкестендіру нөмірінен (PIN) немесе шаблоннан басқа, екі фкторлық түпнұсқаландыру үшін екінші айырып танитын белгі қажет, мысалы, мынандай:

* Физикалық объект – кредиттік карточка, АТМ карточкасы, телефон, немесе кілт-карта.
* Биометриялық сканирлеу – саусақтың ізі, алақанның ізі, сонымен қатар бетті немесе дауысты айырып тану

Брандмауэр – бұл қауіпсіздіктің алдын ала белгіленген қағидалары негізінде кіріс және шығыс желілік трафикті тексеретін және бақылайтын желілік қуіпсіздік жүйесі. Ол бұл компьютерді қорғау мақсатында компьютерге орнатылуы мүмкін (жергілікті брандмауэр), немесе бұл компьютерлердің желісін және бұл желідегі барлық хост-құрылғыларды қорғайтын желілік құрылғы болуы мүмкін.

Брандмауэрдің түрлері:

* Желілік мекенжайлар, порттар немесе хаттамалар негізінде сүзгілеуді орындайтын желілік немесе пакеттік брандмауэр
* Қосымшалардың, бағдарламаның немесе қызметердің негізінде сүзгілеуді орындайтын қосымшалар брандмауэры
* Қосылуға клиенттік сұрау салуларды сүзгілеуді орындайтын прокси-сервердің брандмауэры
* Желілік мекенжайларды түрлендіру брандмауэрына мекенжайларды жеке диапазонда пайдаланатын үлкен желілік жүйе кіреді
* Бір компьютердің операциялық жүйесінде жүйелік қызметтердің порттары мен шақыруларын сүзгілеуді орындайтын жергілікті брандмауэр.

Виртуалды жекеше желі (VPN) – бұл қосылысты сервер арқылы бағдарлай отырып және өзінің әрекеттерін интернетте жасыра отырып, желіге қолжетімділікті қауіпсіз және құпиялы түрде алуға мүмкіндік беретін қызмет. Бұл қызмет сіздің деректеріңізді шифрлайды және онлайн-адресат сіздің деректеріңізді компьютеріңізден немесе сіздің орналасқан орныңыздан емес, VPN-нен түскен ретінде көрсетеді.

**Ақпараттық қауіпсіздік саласындағы стандарттар мен ерекшеліктер**

Мәні бойынша айтқанда, стандарт, есеп берушілік стандарты, техникалық стандарт немесе ақпараттық қауіпсіздік стандарты болсын, өнім немесе жүйе сәйкес келуі тиіс талаптардың жиыны болып саналады.

Ақпараттық қауіпсіздік саласындағы стандарттарға қажеттілік ұзақ уақыт бойы танылып, соңғы жылдары әжептәуір дамыды.

Әуелі АҚШ Қорғаныс министрлігінің «Сенімді компьютерлік жүйелерді бағалау критерийлері» әйгілі Қызғылт сары Кітабы жарияланды. Осы жылдардың басқа маңызды стандарттарына мыналар кіреді: "Ресей Федерациясның Мемлекеттік техникалық комиссиясының басшылық құжаттары», «Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері (ITSEC)», «Федералдық ақпараттың және ақпараттық жүйелердің қауіпсіздік жіктемесінің стандарттары», «Сенімді компьютерлік өнімді бағалаудың канадалық критериілері».

Соңғы жылдары түрлі елдерде компанияның ақпараттық қауіпсіздігін басқарудың тәжірибелік мәселелеріне арналған стандарттардың жаңа буыны пайда болды. Бірінші кезекте, бұл ақпараттық қауіпсіздікті басқарудың халықаралық стандарттары ISO15408, ISO17799 және т.б.

ISO/IEC17799: 2002 стандарты ақпараттық қауіпсіздік саласында ең белгілі стандарттардың бірі болып табылады. Онда ұйымдар мен кәсіпорындардың ақпараттық қауіпсіздігін қамтамасыз етудің келесі мәселелері қаралады:

* ақпараттық қауіпсіздікті қамтамасыз ету қажеттілігі
* ақпараттық қауіпсіздіктің негізгі түсініктері мен анықтамалары
* компаниядағы ақпараттық қауіпсіздіктің саясаты
* корпоративтік ақпараттық ресурстарының жіктемесі және басқару
* қызметкерлерді басқару және ақпараттық қауіпсіздік
* физикалық қауіпсіздік
* ақпараттық жүйелердің қауіпсіздігін әкімшілендіру
* қолжетімділікті басқару
* әзірлеу, пайдалану және техникалық қызмет көрсету жағдайында АЖ-ға арналған қауіпсіздік талаптары

Қазіргі таңда Қазақстанда бар ақпараттық қауіпсіздіктің әртүрлі стандарттарының арасында ақпараттық қауіпсіздікті реттейтін компьютерлік техниканың және құжаттардың қауіпсіздігін бағалау критерийлері бойынша нормативтік құжаттарды атап өту қажет.

Оларға ақпаратты өңдеу жүйелерін және ақпараттық жүйелерді криптографиялық қорғау бойынша нормативтік құжаттар жатады. Төменде осы кейбір стандарттардың тізімі келтірілген:

* ҚР СТ 34.026-2006 Ақпаратты қорғау. Терминдер мен анықтамалар.
* ҚР СТ 34.022-2006 Ақпаратты қорғау. Ақпараттық жүйелердің қауіпсіздігін жобалауға, орнатуға, реттеуге, пайдалануға және қамтамасыз етуге қойылатын талаптар.
* ҚР СТ 34.023-2006 Ақпараттық технологиялар. Ақпараттық жүйелердің қауіпсіздік талаптарына сәйкестігін бағалау әдістері.
* ҚР СТ МЕМСТ Р 50739-2006 Есептеу техникасы. Ақпаратты рұқсат етілмеген қолжетімділіктен қорғау. Жалпы техникалық талаптар.
* ҚР СТ ИСО/МЭК 14888-3-2006 Ақпараттық технологиялар. Ақпаратты қорғау әдістері. Қосымша арқылы цифрлық қолтаңбалар. 3-бөлім. Сертификаттар негізіндегі тетіктер.

**Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы құқықтық қарым-қатынастарды реттейтін актілері. Цифрлық қолтаңба. Кодтау.**

Мессенджерлерде тілдесу, онлайн төлемдер, электрондық қызметтер – осының барлығы заманауи адамның күнделікті өмірінің бір болігіне айналды. «Цифрлық Қазақстан» мемлекеттік бағдарламасын қабылдаумен қазақстандықтардың өміріне қарқынды түрде кірген цифрландыру негізгі салалар мен бизнес қана емес, сондай-ақ қоғамның бүкіл өмірі цифрландырылатын экономиканың жаңа моделін жасайды.

Мысалы, электрондық үкіметтің eGov.kz порталы азаматтардың мемлекеттік қызмет көрсетулерге жылдам қолжетімділігіболуы үшін жұмыс істейді. Бұл өтінімдердіберу, сертификаттарды, лицензияларды алу, тіркеу және басқа да операциялар сияқты қызмет көрсетулер. Барлық осы операциялар сіздің цифрлық қол қолтаңбаңызбен қол қойылкы мүмкін.

Цифрлық қолтаңба – бұл пайдаланушыларғаелдің қағидаларына сәйкес құжаттарға қол қоюға мүмкіндік беретін, ашық кілттер инфрақұрылымдарының (РКІ) стандарттарына негізделген электрондық қолтаңбаның типі.

Цифрлық қолтаңбаға қол қою ниетін атқаратын кез келген электрондық деректер кіреді. Қазақстан Үкіметінің 2003 жылғы 7 қаңтарда «Электрондық құжат және электрондық цифрлық қолтаңба туралы» заңды қабылдады.