№ 8 дәріс. Киберқауіпсіздік

Дәрістің мақсаты: Киберқауіпсіздіктің негізгі принциптерін, ақпараттық қауіпсіздіктің қатерлерін, қорғау шаралары мен құралдарын меңгеру.

Дәріс мазмұны: Ақпараттық қауіпсіздіктің қатерлері және олардың жіктелуі. Киберқауіпсіздік индустриясы. Киберқауіпсіздік және Интернетті басқару. Зиянды бағдарламалар. Ақпаратты қорғаудың шаралары мен құралдары. Ақпараттық қауіпсіздік саласындағы стандарттар мен спецификациялар. Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы реттеуші құқықтық қатынастар заңнамасы. Электрондық цифрлық қолтаңба. Шифрлау.

Ақпараттық қауіпсіздіктің қатерлері және олардың жіктелуі.

Қауіпсіздік қатері деп пайдаланушыға тікелей немесе жанама түрде зиян келтіретін, жүйеге ықтимал қауіпті әсерлер түсініледі. Қатерді тікелей жүзеге асыру шабуыл деп аталады.

Болуы мүмкін қатерлер мен қорғаныстың осал жерлері туралы білу, оларды әдетте осы қатерлер пайдаланады, қауіпсіздікті қамтамасыз етудің ең үнемді құралдарын таңдау үшін өте маңызды.

Ақпараттық қауіпсіздікке төнетін қатерлердің үш негізгі түрін ажыратуға болады:

1. Рұқсат етілмеген қол жеткізу. Пайдаланушының, ұйымда қабылданғанқауіпсіздік саясатына сәйкес рұқсаты жоқ компьютерлік жүйелерге, желілерге немесе деректерге қол жеткізуді алуы.
2. Тұтастықтың бұзылуы. Деректердің тұтастығы ақпараттың өзгеріссіз және дәл болып қалуын білдіреді. Тұтастықты бұзу қатері – бұл жасаушының немесе иесінің рұқсатынсыз деректерді кездейсоқ немесе қасақана өзгерту немесе жою мүмкіндігі.
3. Ақпараттың ашылуы. Ақпараттық қауіпсіздік қатерінің бұл түрі, құпия болып қалуы керек сезімтал ақпараттың жайылып кетуін және таралуын білдіреді.

Кездейсоқ және қасақана қатерлер болады.

Кездейсоқ қатерлер жабдықтың немесе программалық жасақтаманың қателіктерімен; адамның қателіктерімен; форс-мажорлық жағдайлармен байланысты.

Қасақана қатерлер ақпараттық жүйелерді пайдаланушыларға зиян келтіру мақсатын көздейді, және белсенді және сылбыр болып бөлінеді. Сылбыр қатер – бұл жүйенің күйін өзгертпестен ақпаратқа рұқсат етілмеген қол жетімділік, белсенді – ақпаратты ұстап алу және өзгерту әрекеттерімен байланысты.

Ақпаратқа және басқа ресурстарға заңды түрде қол жеткізуді әдейі бұғаттау болып табылатын «қызметтен бас тарту»; артықшылықтарды заңсыз пайдалану; зиянды бағдарламалар сияқты қатерлер де жиі кездеседі.

Ақпараттық қауіпсіздік қатерлерінің жіктелуі:

- ақпаратты ұрлау (көшіру);
- ақпаратты жою;
- ақпаратты өзгерту (бұрмалау);
- ақпараттың қолжетімділігін бұзу (бұғаттау);
- ақпараттың түпнұсқалығын жоққа шығару;
- жалған ақпарат таңу.

Зиянды бағдарламалар.

Зиянды бағдарламалар – компьютерге, желіге немесе серверге зиян келтіруі мүмкін кез келген бағдарлама немесе файл. Зиянды бағдарламалар құпия деректерді ұрлайды, шифрлайды және жояды, негізгі есептеу функцияларын өзгертеді немесе ұстайды және компьютерлердің немесе қосымшалардың белсенділігін қадағалайды.

«*Вирус*» – бұл вирустың көшірмесін өзіне қосатындай етіп, оларды өзгерту арқылы, басқа бағдарламаларға жұқтыруға қабілетті бағдарлама; «трояндық ат» – бұл жасырын немесе айқын бағдарламалық кодты қамтитын бағдарлама, оны орындау кезінде қауіпсіздік жүйесінің жұмысы бұзылады; «құрт» – бұл өзінен-өзі көбейетін, байланыс желілері бойынша жүйелер мен желілерде таралатын бағдарлама.

Руткиттер – бұл қылмыскерлердің немесе зиянды бағдарламалардың әрекеттерін көрінбейтін етіп жасайтын бағдарламалар. Руткит қылмыс іздерін жасыра отырып, киберқылмыскерлерге жүйеге кіруге, оны басқаруға, тыңшылыққа, деректерді ұрлауға, зиянды бағдарламалар мен шабуылдарды жүргізуге көмектеседі.

Бэкдор (ағылш. back door – «артқы есік») - компьютерді алыстан басқаруға мүмкіндік беретін қосымша. Бэкдор – бұл компьютерге, смартфонға және т.б. рұқсатсыз кіруге мүмкіндік беретін осалдық, басқаша айтқанда, бұл қаскүнем басқа біреудің құрылғысынан деректерді алып, оны қашықтан басқара алатын Саңылау(ілік, амал).

Жүктеуші – зиянды бағдарламаның толық нұсқасын одан әрі жүктеуге арналған код.

Зиянды бағдарламалар класына *снифферлерді* (желілік пакеттерді ұстап қалатын бағдарламалар, (ағылш. to sniff – иіскеу) – интернетке қосылған компьютерден кіретін және шығатын трафикті талдайтын бағдарламалықжасақтама), парольдерді таңдау бағдарламаларын, буфердің толып кетуіне шабуылдарды, кейбір қосымшаларда –дизасемблерлер мен ретке келтіргіштерді жатқызуға болады.

Киберқауіпсіздік индустриясы.

Киберқауіпсіздік индустриясы – бұл пайдаланушының немесе жүйенің ақпараттық қауіпсіздігіне жауап беретін сала.

Осы сектордың негізгі компаниялары:

- Cisco Systems

- Software Technologies
- Check Point
- MCAfee
- Касперский зертханасы

Киберқауіпсіздік және интернетті басқару

МСЭ-Т X.1205 (МСЭ-Международный Союз Электросвязи – Халықаралық электрбайланыс одағы) ұсынымына сәйкес: Киберқауіпсіздік – ұйым мен пайдаланушының ресурстарын, киберортаны қорғау үшін пайдалануға болатын құралдар, стратегиялар, қауіпсіздікті қамтамасыз ету принциптері, қауіпсіздік кепілдіктері, басшылық принциптері, тәуекелдерді басқару тәсілдері, іс-әрекеттер, кәсіптік даярлық, практикалық тәжірибе, сақтандыру және технологиялар жиынтығы. Ұйым мен пайдаланушының ресурстарына қосылған компьютерлік құрылғылар, персонал, инфрақұрылым, қосымшалар, қызметтер, электрбайланыс жүйелері және киберортада берілген және/немесе сақталған ақпараттың барлық жиынтығы кіреді. Киберқауіпсіздік киберортадағы тиісті қауіпсіздік қатерлеріне қарсы бағытталған, ұйымның немесе пайдаланушының ресурстарындағы қауіпсіздік қасиеттеріне қол жеткізу және сақтау әрекетінен тұрады.

Қауіпсіздікті қамтамасыз етудің жалпы міндеттеріне мыналар жатады:

- деректердің құпиялылығы – бұған тек өкілеттігі бар адамдар ғана қол жеткізе алады;
- қолжетімділік – қол жеткізу құқығы бар нақты пайдаланушылар ғана ақпараттарды пайдалана алады;
- деректердің тұтастығы – ақпараттың рұқсат етілмеген өзгеруіне тосқауыл қоюды көздейді;
- түпнұсқалық – ақпараттың толықтығы және жалпы дәлдігі;
- бас тартпаушылық – ақпараттың шығу көзін немесе авторлығын анықтау мүмкіндігі.

Ақпараттық қауіпсіздік жүйелерінің басты мақсаты – деректерді сыртқы және ішкі қатерлерден қорғауға кепілдік беру.

WGIG (Working Group on Internet Governance – Интернетті басқару жөніндегі жұмыс тобы) жұмыс тобы жан-жақты талқылауды ескере отырып, «интернетті басқару» ұғымының анықтамасын әзірледі: интернетті басқару бұл үкіметтердің, жеке сектордың және азаматтық қоғамның өздерінің тиісті рөлдерін, жалпы принциптерін, нормаларын, ережелерін, шешім қабылдау процедураларын және интернеттің эволюциясы мен қолданылуын реттейтін бағдарламаларды орындаудағы әзірлеуі мен қолданылуын білдіреді.

WGIG жұмыс тобы халықаралық деңгейде бекітуді және шешуді қажет ететін маңызды мәселелерді тұжырымдады:

– интернеттің түпкі аймағын және домендік атау жүйесінің (DNS) түпкі серверлерін әкімшілік басқару;
– жаңа IPv6 желілік хаттамасына көшу жағдайында желілік IP-адрестерді тағайындау және адрестік кеңістікті бөлу тәртібі;
– халықаралық деңгейде ақпараттық және телекоммуникациялық желілерді қосу тәртібін және олардың өзара әрекеттестігін нақтылау;

– ғаламдық желінің және оның пайдаланушыларының тұрақтылығы мен қауіпсіздігі;
– интернеттегі ақпараттың, соның ішінде спамның заңсыз таралуын болдырмау;
– интернетті пайдалану кезінде адамның негізгі құқықтары мен бостандықтарын, оның ішінде бірінші кезекте сөз бостандығы мен өз пікірін білдіру бостандығын қамтамасыз ету;
– интернетті басқарудың мемлекеттік саясатын әзірлеуге әрбір тілек білдірушінің конструктивті қатысуын қамтамасыз ету;
– ақпаратты және жеке өмірге қол сұғылмаушылық құқығын қорғау;
– желілік қызмет көрсету кезінде тұтынушылардың құқықтарын сақтау;
– көптілділік тәжірибесін және көпмәдениеттілік саясатын кеңейту.

Ақпаратты қорғаудың шаралары мен құралдары

Қауіпсіздікті қамтамасыз ету үшін АЖ-де ақпараттың қауіпсіздігін қамтамасыз етудің мынадай *әдістері* қолданылады: кедергі; қолжетімділікті басқару; шифрлау механизмдері; зиянды бағдарламалардың шабуылдарына қарсы іс-қимыл; регламенттеу; мәжбүрлеу; ниеттендіру.

Қауіпсіздік құралдарына мыналар жатады:

– *техникалық.* Бұл ақпараттық жүйелерге тәуелсіз жұмыс істейтін және қатерлерге қол жеткізуге кедергі келтіретін кез келген механикалық, электрлік және электрондық механизмдер (күзет және өрт дабылы жүйелері, цифрлық бейне бақылау, қол жеткізуді бақылау және басқару жүйесі – бұл ғимаратқа кіруді және шығуды бақылау механизмі және идентификаторлар арқылы жұмыс кестесін есепке алу, экрандалған жабдықты пайдалану және кабельдер);
– *аппараттық.* Бұл ақпараттық және телекоммуникациялық жүйелерге ендірілген кез-келген электрлік, электронды, оптикалық, лазерлік және басқа құрылғылар (шифрлауға, парольдерді сақтауға, адамның жеке сипаттамаларын өлшеуге (дауыс, ізтаңбалар және т. б.) арналған құрылғылар);
– *бағдарламалық жасақтама.* Бұл ақпараттық қауіпсіздікті қамтамасыз етуге байланысты мәселелерді шешуге арналған қарапайым және кешенді бағдарламалар (антивирустық бағдарлама, VPN, желіаралық экрандар, proxy-серверлер);
– *ұйымдастырушылық.* Бұл ұйымдық-техникалық (компьютерлік ғимараттармен қамтамасыз ету, кабельдік жүйені орнату және т. б.) және ұйымдық-құқықтық (ұлттық заңнамалық актілер мен нормалар, белгілі бір кәсіпорынның немесе мемлекеттің басшылығымен белгіленген жұмыс ережелері) құралдардың жиынтығы.

Шифрлау және электрондық цифрлық қолтаңба.

Кең таралған қорғау шараларының бірі шифрлау және электрондық-цифрлық қолтаңбаны пайдалану болып табылады.

Шифрлау – бұл деректерді тиісті ақпаратсыз (шифрлау кілтінсіз) оқуға болмайтын түрге түрлендіру. Міндет, егер олар шифрланған деректерге қол жеткізе алса да, оған арналмаған адамдардан ақпаратты жасыру арқылы құпиялылықты қамтамасыз етуден тұрады.

Ақпаратты шифрлау кепілдік береді:

- бөгде адамдар үшін ақпараттың қолжетімсіздігі;
- ақпараттың түпнұсқалығы (ақпарат бұрмаланбаған түрде түседі);
- ақпараттың тұтастығы (жеткізілетін деректер жіберу процесінде өзгеріссіз қалады).

Электрондық-цифрлық қолтаңба (ЭЦҚ) – бұл криптографиялық алгоритм бойынша арнайы бағдарламалық құрал арқылы қол қойылатын электрондыққұжатты түрлендіру арқылы қалыптасатын байттар тізбегі және электрондық құжаттың авторлығын тексеруге арналған.

Электрондық-цифрлық қолтаңба электрондық құжаттың түпнұсқалығын, тұтастығын және авторлығын растау болып табылады. ЭЦҚ – бұл электрондық тіркеу куәлігін (бұдан әрі мәтін бойынша-сертификат) және ЭЦҚ жабық кілтін пайдалана отырып, ақпаратты криптографиялық түрлендіру нәтижесінде алынған электрондық құжаттың деректемесі, қолмен қол қоюдың баламасы. ЭЦҚ жабық кілті мен сертификаты SMART-картада шығарылады, бұл осы ақпараттың тұтастығын бұзуды және ЭЦҚ жабық кілтін көшіруді болдырмайды. SMART-карта PIN-кодпен қорғалған, бұл оны тек сертификат иесінің пайдалануына кепілдік береді. Сертификат иесін анықтауға мүмкіндік бере отырып, ЭЦҚ электрондық құжатты қолдан жасаудан қорғауға, сондай-ақ ондағы ақпараттың бұрмаланбауын анықтауға көмектеседі.

ЭЦҚ шифрлаудың жалпы алгоритмдеріне мыналар жатады: RSA(Rivest, Shamir және Adleman фамилияларының аббревиатурасы), Эль-Гамаль, DSA(Digital Signature Algorithm – сандық қолтаңба алгоритмі) алгоритмдері.

Ақпараттық қауіпсіздік саласындағы стандарттар мен спецификациялар.

Ақпараттық жүйелердің қауіпсіздігі шаралары мен құралдарын сипаттауға мүмкіндік беретін бірқатар стандарттар мен спецификациялар бар. Үлестірілген жүйелердің ақпараттық қауіпсіздігі X.800 ұсынысымен реттеледі. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері ISO/IEC 15408 стандартында сипатталған.

- ISO/IEC 17799: 2005 «Ақпараттық технологиялар. Қауіпсіздік технологиялары. Ақпараттық қауіпсіздік менеджментінің практикалық ережелері».
- ISO/IEC 27001. «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар».

Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы реттеуші құқықтық қатынастар заңнамасы.

Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы реттеуші құқықтық қатынастар заңнама актілері:

- ҚР ақпараттық қауіпсіздік тұжырымдамасы (2011ж.)
- «Ұлттық қауіпсіздік туралы» ҚР Заңы (6-бап)
- «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» ҚР Үкіметінің 12.12.2016 №832 қаулысы.

Қазақстанның ақпараттық қауіпсіздігінің алғашқы тұжырымдамасы 2006жылы қабылданды және бірқатар нормативтік құқықтық актілерге негізделді:

- Конституция;

- «Қазақстан Республикасының Ұлттық қауіпсіздігі туралы»;
- «Мемлекеттік құпиялар туралы»;
- «Терроризмге қарсы күрес туралы»;
- «Электрондық құжат және электрондық цифрлық қолтаңба туралы»;
- «Ақпараттандыру туралы»;
- «Экстремизмге қарсы іс-қимыл туралы» заңдар;
- Қазақстан Республикасының ақпараттық кеңістігінің бәсекеге қабілеттілігіндамытудың 2006-2009 жылдарға арналған тұжырымдамасы;
- ТМД-ға қатысушы мемлекеттердің әскери саладағы ақпараттық қауіпсіздік тұжырымдамасы.

2011 жылы екінші тұжырымдама қабылданды, онда НҚА(Нормативтік құқықтық акт) тізімі «Техникалық реттеу туралы» (2004), «Лицензиялау туралы» (1995), «Бұқаралық ақпарат құралдары туралы», «Байланыс туралы» (2004) заңдар есебінен толықтырылды. Сондай-ақ ШЫҰ-ға мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімнің (2010) және ТМД-ға қатысушы мемлекеттердің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық тұжырымдамасының (2008) ережелері пайдаланылды.

Бақылау сұрақтары

1. Ақпараттық қауіпсіздік қатерлерін атаңыз?
2. Ақпараттық қауіпсіздік қатерлерінің жіктелуі
3. Зиянды бағдарламалар және олардың түрлері
4. Киберқауіпсіздік дегеніміз не?
5. Ақпараттық қауіпсіздіктің міндеттері қандай?
6. Ақпараттық қауіпсіздікті қорғау әдістері қалай жіктеледі?
7. Ақпаратты қорғаудың қандай құралдары бар?
8. Деректерді шифрлау дегеніміз не?
9. ЭЦҚ дегеніміз не?
10. Ақпараттық қауіпсіздікті реттейтін негізгі стандарттар?