ғ) Достарыңның поштасына “Туылған күніңмен!”, “Наурыз мерекесі құтты болсын!” деген хабарға қоса осы атты әдемі сурет қойып жөнелт;
д) Достарыңның поштасына “Менің жанұям”, “Сыныптас” атты хабарға қоса соған сай открытка жібер.

16-сабақ. АҚПАРАТТАРДЫ ҚОРҒАУ ЖӘНЕ АНТИВИРУСТАР ТУРАЛЫ

Барлық материалдық заттар сияқты ақпараттың да өз мәні бар. Сондықтан бір пайданы көздеп ақпаратты «ұрлау», «бұзу», «қажетсіз мәліметпен толтыру», ақпарат сақталған қондырғыларды істен шығару сияқты жағдайлар кездесіп тұрады. Демек, бұл сияқты зиянды істерден қорғалу өзекті мәселе екен.

Ақпарат және қылмыс

Соңғы кездері ақпаратты қорғау проблемалары тек мамандарды ғана емес, тіпті есептеу техникасын пайдаланушыларды да алаңдатып отыр. Бұл, әрине, компьютердің адам өмірі мен қызметіне жедел кіріп келуіне байланысты.

«Ақпарат» түсінігіне жанасу да түбегейлі өзгеруде. Бұл атау соңғы кезде көбірек сатып алынатын, сатылатын немесе бір затқа алмастырылатын өзіне тән өнімге айналып барады. Ондай өнім көпшілік жағдайда өзі сақталып жатқан есептеу техникасынан ондаған есе, тіпті жүздеген есе қымбат тұратынын айту қажет. Интернет ақпарат «ұрыларын» (ақпарат ұрылары компьютерлер жасалғанға дейін де болған) жаңа сатыға көтерді. Енді компьютер, модем және жеткілікті бағдарламалық қамтамасыз етуге ие білікті программист әлемнің кез келген бұрышындағы түрлі мемлекеттік ұйымдар, жекеменшік кәсіпорын, интернет қызметін пайдаланып жатқан тұлға, тағы басқаларға тиісті ақпараттарды өз бөлмесінен шықпай-ақ ұрлап алуы, оларды жаман пиғылда өзгертуі немесе басқа зиян тигізуі мүмкін. Бұл өздігінен ақпаратты қорғауды туындатады.

Компьютерлер адамның жұмысын жеңілдету үшін жасалған. Оның саны күн сайын артып келеді. Сонымен бірге қоғамның компьютер жүйесіне тәуелділігі де артып келеді. Қазір медицина, салық, банк жүйесі, транспорт сияқты салаларда басқару мен нақтама істері компьютерге жүктелген. Компьютер жүйелері әскери салада да маңызды орын алады.

Қоғамды компьютерлендірудің белгілі бір сатысында компьютерлер жеке және ұйымдасқан қылмыскер топтарды өзіне тартады. Олар жеткілікті техникалық және бағдарламалық құралдарға ие болып, ешбір қиындықсыз құпия мәліметтерді ұрлау, диверсия, шантаж тағы басқа істерді жүзеге асыруы мүмкін болып қалды. Әділет, криминалистика, ұлттық қауіпсіздік саласының мамандары жаңа, күтпеген проблемаларға бетпе-бет келді.

1971 жылы АҚШ-тың «Нью-Йорк Пенни Централ Рейлроуд» темір жол компаниясы бағалы жүк артылған 200 вагоны жоғалғанын байқап қалады. Бұл істі тексеру үдерісінде бірнеше басқа фирмалардың да вагондары жоғалғаны анықталады. Мұқият жүргізілген тексерудің нәтижесінде вагондардың жоғалуына компьютерге әдейі қате адрес көрсетілгені себеп болғаны анықталды. Бұл ресми тіркелген бірінші «электронды қылмыс» еді. Қазір компьютерлер де, байланыс жүйесі де жедел дәрежеде дамып кетті. Бұл «электронды қылмыскерлерге» жаңа мүмкіндіктер ашып берді.

Ақпартпен жұмыс істеудегі ақылақтық және құқықтық нормалар

Латын тіліндегі **media** (*medium*) сөзі құрал, делдал, орта мағыналарын берсе де, қазіргі күнде бұл сөз ағылшын тіліндегі мазмұнына сай радио, телевидение, мобильді телефон және Интернет құралдарын қамтыған “бұқаралық ақпарат құралдары” сияқты түсіндірілуде. Осы құралдар арқылы түрлі мазмұнда өте үлкен көлемдегі ақпараттар өтуде. Бұл ақпараттардың қайсысы пайдалы, қайсысы зиянды екенін ажыратып алу оңай емес. Әсіресе, Интернет жүйесінде жастардың көзқарасына, идеологиялық тәрбиесіне ұнамсыз әсер ететін, әдеп-ақылақ және құқықтық нормалардың бұзылуына себеп болатын мәліметтер көп. Ондай мәліметтерге мыналарды кіргізуге болады:

– жат, бұзғыншы идеялар (діни экстремизм, ұлтшылдық, садизм);

– шетел тұрмыс салтына сай, бірақ ұлттық идеологияға, мәдениетімізге қайшы идеялар, көзқарастар (киіну, шегу, персинг, татуировка т.б.);

– тексерілмеген немесе жалған мәліметтер;

– ұятсыз оқиғаларды қамтыған ақпараттар (суреттер, видеолар, әңгімелер).

Сондықтан, Интернет тармағында жұмыс істегенде ақылақтық және құқықтық нормаларға мойынсұнып мәлімет жіберу, алынатын мәліметтерді ұлттық идеологиямызға, мәдениетімізге, құндылықтарымызға, қасиетті әдет-ғұрыптарымызға қайшы, заңдылығымызға қарсы еместігін анықтай білу сауаттылығына ие болуымыз керек. Ондай сауаттылық media-сауаттылық деп аталады.

Жоғарыда айтылған қатерлерден сақтандыру мақсатында Өзбекстан Республикасының Тұңғыш Президенті Ислам Каримов былай деген: "... егер кімде-кім біздің тәуелсіз даму жолымызды, арман-мақсатымызға жету жолын, жаңа қоғам құру жолын тоспақшы болса, алдымен әлі сүйегі қатпаған, дербес көзқарасы қалыптасып үлгермеген жастарымыздың жүрегі мен санасының морт екенін пайдалынып, олардың руханиятын бұзып, біздің ежелгі қасиетіміздегі ғұрып әдеттерімізге мүлдем қайшы идеялармен шалғытып, өзінің арам пиғылын, жиреніште ниеттерін жүзеге асыру жолында құрал етіп пайдаланады".

Вирустың әсері

Бүгінде компьютер жүйелеріне білімін арттыру немесе жай ғана «әзілдесіп» бұзықтық жасап жатқан «жас программистер» көбірек зиянын тигізуде. Өйткені олар өте көпшілікті құрайды. Олардың кейбіреулері біреуге зиянын тигізіп жатқанын білмейді де.

Интернет арқылы тигізілетін негізгі зияндар:

– Тармаққа қосылған уақытта компьютеріңе рұқсатсыз «кіру» және оны сенің мүддеңе қайшы алыстан басқару.

– Интернетке беріліп жатқан ақпараттарды «жолда ұстап алып», олардан нұсқа алу немесе өзгерту.

– Түрлі вирус (компьютердің жадындағы мәліметтерді өшіру, өзгерту сияқты істерді орындайтын және басқа да бағдарлама құрамына қосылып алу «жұғу» қасиеті бар арнайы бағдарлама) бағдарламаларын веб-беттерге «жасырып қою».

– Түрлі мемлекеттік ұйымдар мен жеке кәсіпорындарға тиісті ақпараттарды ұрлау мен бәсекелес ұйымдарға сату немесе белгілі мөлшерде төлем талап ету.

– Қоғам идеологиясы мен руханиятына қайшы келетін ақпараттарды Интернетте жариялау.

Кейбір вирус бағдарламаларының атынан-ақ оның атқаратын ісін түсінуге болады. Мысалы, Black Hole (қара түнек, яғни экранның сол бұрышынан қара түнек ашады), Black Friday (қара жұма,

жұма күні істеп жатқан файлдарды өшіреді), Friday 13 (он үшінші жұма, яғни 13 дата күндері істеп жатқан файлдарды өшіреді), «жайлап әсер ететін вирус» (компьютер ісі бірнеше жүз еселеп жай істейтін болады) т.с.с.

Вирустардың классификациясы

Вирустарды шартты мынадай түрге бөлуге болады:

– файл вирустары (COM, EXE және DLL-ге зиян жеткізеді);

– Boot-вирустар (дискеттерді бастапқы жүктейтін секторларды (немесе MBR – Master Boot Record) қатты дисктің жүктеуші саласына зиян тигізеді):

– **макровирустар;**

– **тармақ вирустары.**

Файл вирустары компьютерлерде ең көп тараған вирустар. Олар барлық вирустардың шамамен 80% -ын құрайды. Бұл категория вирустары өте шыдамды болып, дер кезінде сақтық шаралары қарастырылмаса шынайы эпидемияға айналады. Мысалы, RCE-1813 немесе Иерусалим (Quddus), Black Friday (қара жұма).

– Boot-вирустар – өзін дисктің операцион жүйесін жүктейтін 0-трекіне жазып алады. Ондай вирустар пайдаланушы әлі бағдарламаны іске қоспай-ақ алдымен операциондық жүйе (OS) жүктелмей-ақ белсенді болады және тарайды.

Boot-вирустар файл вирустарынан ерекшеленеді. Олардың саны файл вирустарына қарағанда едәуір кем және жай тарайды.

Макровирустар – мәліметтерді қайта өңдейтін түрлі жүйелерге (мәтін редакторлар, электронды кестелер) орнатылған макротіл мүмкіндіктерін пайдаланады. Олар әсіресе Microsoft Word және Excel бағдарламасына кең тараған. Мұндай вирустар залалданған файлдар іске қосылғанда белсенді болады және осы түрдегі файлдар іске қосылса оларды да залалдайды. Олар тек жеке компьютерлерді ғана емес, тіпті осы бағдарламалар орнатылған тармақтағы компьютерлерді де залалдайды.

Тармаққа залал келтіретін вирустар репликаторлар деп аталып, тармақтағы барлық немесе кейбір абоненттерді залалдайды. Тармақ вирустары өзін кең тарату үшін тармақ протоколдары немесе компьютер және электронды пошта бұйрықтарын пайдаланады. Бүгінде кең тараған осы түрдегі вирустар – трояндар және пошта вирустары. Мұндай вирустар мәліметтерді ұрлауға кең мүмкіндік береді. Олардың ең «танымалысы» Морриса

аттысы. 1988 жылы бұл вирус Интернет тармағындағы 30000 компьютердің 6000-ына залал тигізген.

Вирустардан сақтану

Мұндай қауіптің алдын алудың бірнеше шарасы бар. Оларға мойынсұну қауіпті толық жоймаса да, едәуір дәрежеде кемейтеді. Төменде осы шаралардың негізгісі берілген.

– Жеке және локалды тармақтағы компьютерлерге сырттан Интернет арқылы кіруді шектейтін және бақылайтын техникалық және бағдарламалық құралдарды пайдалану.

– Интернет арқылы тек сенімді деректерден ақпарат алу мен олардың түпнұсқаға сәйкестігін тексеру.

– Мәліметтерді жеткізу мен қабылдауда криптография (ақпаратты кодтау) әдістерін пайдалану.

– Компьютер вирустарына қарсы бақылау және емдеу бағдарламаларын пайдалану.

Сенің жеке компьютеріңде пайда көру үшін ұрлауға тұратындай бағалы ақпарат болмауы мүмкін. Дегенмен бұл ақпарат сен үшін қажет. Компьютер вирустары болса, оны өшіріп жіберуі мүмкін. Компьютер вирустары тарихи Синсинати қаласы (Огайо штаты) университетінің ғылыми қызметкері, компьютер қауіпсіздігі саласының танымал маманы, Фред Коен атымен байланысты. Коен бағдарламалық құралдардан заңсыз нұсқа көшіруге қарсы қорғаныс проблемаларына іс жүргізіп, жаңа бағдарлама жасады. Бұл бағдарламаның қайта тіктеу мен жетілдіру және компьютер жадындағы маңызды мәліметтерді өшіру, жүйе файлдарын «бұзу» сияқты істерді орындау қасиеттері бар, бағдарламалық құралдардан заңсыз нұсқа алу уақтында іске қосылады. Ақпаратты ұрлардан қорғауға бағытталған бұл бағдарлама кейіннен компьютер вирустарының жасалуына түрткі болды.

Компьютердегі мәліметтерді вирустардан қорғау үшін АҚШ, Канада, Ресейдің бірнеше фирмалары антивирус бағдарламаларын жасауда.

Қазір мынадай антивирус бағдарламалары кең тараған:

DrWeb for Windows	Kaspersky Anti-Virus	Norton Antivirus	Aidstest
Avira Internet Security	McAfee VirusScan	Avast Antivirus	NOD32

1. Ақпараттарды қорғау не үшін керек?
2. Интернет арқылы компьютер және оның ақпарат ресурстарына қандай залал тигізу мүмкін?
3. Вирустардың қандай топтары бар?
4. Файл вирустары қалай «көбейеді»?
5. Ақпарат қауіпсіздігі және «электронды қылмыскерлерден» қорғалуды қамтамасыз ететін шаралар туралы айтып бер.
6. Криптография дегенде не түсінесің?
7. Компьютер вирустарының жасалуына кім түрткі болды?
8. Компьютер вирустарына қарсы қалай күресуге болады?
9. Boot-вирустар туралы айтып бер.

1. Мағынасына қарай қой:

Интернет ақпарат «ұрыларын»	жеңілдету мақсатында жасалды
Компьютер адамның жұмысын	жаңабасқышқа көтереді
Компьютер вирустары болса оларды өшіріп жіберуі немесе	жаңа, күтпеген проблемаға кездесті
Әділет, криминалистика, ұлттық қауіпсіздік саласы мамандары	пайдалануға болмайтын дәрежеде өзгертуі мүмкін

2. Нүктелердің орнына оң жақ бағандағы қажетті сөздерді қойып көшір.

Қазір компьютер жүйелеріне өз білімін жетілдіру немесе жай « әзілдесіп» ... жасап жатқан жас программистер көбірек залал тигізуде	атқаратын
Кейбір вирус бағдарламаларының атынан-ақ ...ісін түсініп алуға болады	пайда көру
Сенің жеке компьютеріңде ...мақсатында ұрлауға тұрарлық бағалы ақпарат болмауы мүмкін	арандатушылық

3. Мына пікірлердің қайсысы дұрыс:

а) Компьютер вирустарын пайдалану үшін арнайы бағдарлама – антивирустар жасауға тура келді.

ә) Қоғамды компьютерлендірудің белгілі бір басқышында вирустар жеке және ұйымдасқан қылмыскер топтарды өзіне тартады.

б) Интернет ақпарат «ұрыларын» жаңа сатыға көтерді.