# Ақпаратты қорғаудың бағдарламалық мүмкіншіліктері

**Лекция - 3**

# Ақпаратты қорғаудың бағдарламалық құралдары

- Ақпаратты қорғаудың кіріктірілген құралдары
- Вирусқа қарсы бағдарлама (антивирус) — компьютерлік вирустарды анықтауға және жұқтырған файлдарды емдеуге, сондай — ақ файлдарды немесе операциялық жүйені зиянды кодпен жұқтырудың алдын алуға арналған бағдарлама.
- Ақпаратты рұқсатсыз кіруден қорғаудың мамандандырылған бағдарламалық құралдары кіріктірілген құралдарға қарағанда жақсы мүмкіндіктер мен сипаттамаларға ие. Шифрлау бағдарламалары мен криптографиялық жүйелерден басқа, ақпаратты қорғаудың көптеген басқа құралдары бар.

- Брандмауэр (брандмауэр немесе желіаралық қалқан деп те аталады). Жергілікті және ғаламдық желілер арасында олар арқылы өтетін барлық желілік/транспорттық деңгей трафигін тексеретін және сүзетін арнайы аралық серверлер құрылады. Бұл корпоративтік желілерге сырттан рұқсатсыз кіру қаупін күрт төмендетуге мүмкіндік береді, бірақ бұл қауіпті толығымен жоймайды. Әдістің неғұрлым қауіпсіз нұсқасы маскарадтау әдісі болып табылады, жергілікті желіден шығатын барлық трафик брандмауэр серверінің атынан жіберіліп, жергілікті желіні дерлік көрінбейтін етеді.
- Прокси-серверлер (прокси-сенімхат, сенімді тұлға). Жергілікті және ғаламдық желілер арасындағы барлық желілік/транспорттық деңгей трафигіне толығымен тыйым салынады - мұндай маршруттау жоқ және жергілікті желіден ғаламдық желіге қоңыраулар арнайы делдалдық серверлер арқылы жүзеге асырылады. Әлбетте, бұл жағдайда ғаламдық желіден жергілікті желіге қоңырау шалу мүмкін емес. Бұл әдіс жоғары деңгейде – мысалы, қолданба деңгейінде (вирустар, Java және JavaScript коды) шабуылдардан жеткілікті қорғанысты қамтамасыз етпейді.
- VPN (виртуалды жеке желі) рұқсат етілмеген адамдар трафикті тыңдай алатын желілер арқылы құпия ақпаратты тасымалдауға мүмкіндік береді. Қолданылатын технологиялар: PPTP, PPPoE, IPSec.

# NSD қорғау жүйелерінің жіктелуі

- Компьютерді басқа адамдардың шабуылынан қорғау жүйелері өте алуан түрлі және оларды келесі топтарға жіктеуге болады:жалпы бағдарламалық қамтамасыз етумен көзделген өзіндік қорғау құралдары;
- есептеу жүйесінің құрамындағы қорғау құралдары;
- ақпаратты сұрау арқылы қорғау құралдары;пассивті қорғаныс құралдары және т. б.

Басқа біреудің шабуылынан қорғау үшін белгілі бір қауіпсіздік шаралары қажет. Бағдарламалық жасақтамамен жүзеге асырылуы керек арнайы функциялар: объектілер мен субъектілерді сәйкестендіру,есептеу техникасына қол жетімділікті шектеу (кейде толық оқшаулау),ақпаратпен және бағдарламалармен әрекеттерді бақылау және тіркеу.

Сәйкестендіру процедураларында әртүрлі әдістер қолданылады:Қарапайым, күрделі және бір реттік парольдер,әкімшімен сұрақтар мен жауаптар алмасу, жеке сипаттамаларды талдау құралдары,кілттер, магниттік карталар, белгішелер және т. б.,аппаратураға арналған арнайы сәйкестендіргіштер немесе бақылау сомалары.Сәйкестендіруден кейін қорғау 3 деңгейде жүзеге асырылады:аппаратура,бағдарламалық қамтамасыз ету,деректер.Аппаратура және бағдарламалық қамтамасыз ету деңгейінде қорғау есептеу ресурстарына қолжетімділікті басқаруды көздейді.

Деректер деңгейінде қорғау жұмыс барысында оған жүгінген кезде ақпаратты қорғауға және оны байланыс арналары арқылы беру кезінде ақпаратты қорғауға бағытталған.Тіркеу құралдары, сондай-ақ қол жеткізуді басқару құралдары NSD-ден қорғаудың тиімді әдістеріне жатады.

Алайда, егер қол жеткізуді басқару құралдары мұндай әрекеттерді болдырмауға арналған болса, онда тіркеудің міндеті – жасалған әрекеттерді анықтау.

- Ақпаратты көшіруден қорғау
- Ақпаратты көшіруден қорғау барлық қорғау жүйелеріне ортақ бірқатар функцияларды орындау арқылы жүзеге асырылады:бағдарлама іске қосылатын ортаны анықтау,бағдарлама іске қосылған ортаның аутентификациясы,рұқсат етілмеген ортадан ұшыруға жауап беру,рұқсат етілген қол жеткізуді тіркеу,жүйенің жұмыс істеу алгоритмдерін зерттеуге қарсылық.Рұқсат етілмеген ортадан іске қосу реакциясы хабарламаларды шығаруға дейін азаяды.Компьютерлерді пайдаланудың барлық жағдайлары үшін ақпараттың қауіпсіздігін қамтамасыз ету міндеттерінің бірі кез келген қалпына келтіру шараларын дайындау және жүзеге асыру кезінде орын алуы мүмкін жойылудан ақпаратты қорғау болып табылады.Ақпаратты өшіруге дейін компьютерлердің жұмысын бұзу үшін жасалған вирустық бағдарламалар ерекше қауіпті.Вирустарды анықтау және жою үшін антивирустар қолданылады. Олар мамандандырылған және әмбебап болып бөлінеді. Айырмашылығы мынада: арнайы антивирустар бұрыннан жазылған вирустармен ғана жұмыс істей алады, ал әмбебаптар әлі жазылмаған вирустармен де жұмыс істей алады. Әмбебап антивирустардың ішінде резиденттік антивирустар мен аудиторлық бағдарламалар өте кең таралған. Сонымен қатар, вирустардан қорғау үшін әртүрлі ұйымдастыру шараларының кешені қолданылады.