3 Дәріс. Ақпаратты қорғау жабдықтары. Қорғау механизмдері. Жай құпиялық қасиеттер.

.

- **Дәрістің негізгі мазмұны**
- Компьютерлік вирустармен күресу үшін, оларды зерттейтін және антивирустық (вирусқа қарсы) программалар жазатын мамандар бар. Ресейдегі атақты программистер: Д.Лозинский, Д.Мостовой, И.А. Данилов, Н. Безруков және т.б.
- Компьютерге вирус, негізінен дискеттер мен лазерлік диск, сондай-ақ компьютерлік желі арқылы кіріп, қатты дискіні зақымдайды. Вирус көбіне дискінің жүктейтін секторына және EXE, COM, SYS немесе BAT кеңейтулері бар атқарылатын файлдарға жиі жұғады. Мәтіндік және графикалық файлдарға сирегірек жұғады.
- Вирустарды табуға және жоюға мүмкіндік беретін программалар **антивирустік программалар** деп аталады. Windows-та вирусқа қарсы программалар жеткілікті. Бірақ кез келген вирусты іздеп табатын және оны толық жоятын программа әлі шыққан жоқ. Белгілі антивирустік программаларды бірнеше типтерге бөлуге болады.

- **А) Антивирустық программаға қойылатын талаптар.**
- Вирустардың саны мен түрлері өте көп және оларды тез әрі тиімді табу үшін антивирустық программалар мына параметрлерге сай болу керек:
- **Жұмыстың тұрақтылығы мен сенімділігі (**егер компьютердегі антивирустық программа дұрыс жұмыс жасамаса, онда рның ең жақсысының пайдасы аз)
- **Программаның вирустық базасының көлемі** (программамен дұрыс анықтаған вирустардың саны)
- **Программаның жұмысының жылдамдығы**
- **Көпплатформалық** (программаның нұсқалары әртүрлі операциондық жүйеде жұмыс істеуі керек).

- **А) Антивирустық программаға қойылатын талаптар.**
- Вирустардың саны мен түрлері өте көп және оларды тез әрі тиімді табу үшін антивирустық программалар мына параметрлерге сай болу керек:
- **Жұмыстың тұрақтылығы мен сенімділігі (**егер компьютердегі антивирустық программа дұрыс жұмыс жасамаса, онда рның ең жақсысының пайдасы аз)
- **Программаның вирустық базасының көлемі** (программамен дұрыс анықтаған вирустардың саны)
- **Программаның жұмысының жылдамдығы**
- **Көпплатформалық** (программаның нұсқалары әртүрлі операциондық жүйеде жұмыс істеуі керек).

- **Фагтар** немесе **доктор-программалар**, сондай-ақ **вакцина-программалар** вируспен зақымдалған файлдарды тауып қана қоймай, оларды «емдейді» де, яғни программаны вируспен зақымдалғанға дейінгі қалпына келтіре отырып, файлдардан вирус программасының тәнін жояды. Фагтар өз жұмысының басында вирустарды жедел жадтан іздейді, оларды жояды, тек содан кейін ғана файлдарды «емдеуге» кіріседі. Фагтардың ішінде *полифагтар,* яғни вирустардың көп мөлшерін жоятын доктор программалары ерекше. Ең кең таралған полифагтар Aidstest жасаушысы – Д. Лозинский, Scan, Norton AntiVirus, Doctor Web жасаушысы – И.Данилов программалары болып табылады.

- **Ревизор-программалар** вирустардан қорғайтын құралдардың ең сенімдісі. Ревизор программалардың алғашқы қалпын, яғни компьютердің вируспен зақымдалмаған кезін есте сақтайды, содан кейін оқтын-оқтын ағымдағы жағдайды алғашқы жағдаймен салыстырып отырады. Егер өзгеріс болса, онда дисплейдің экранына хабарлама шығарады. Ресейде Д.Мостов жасаған ADinf ревизор программасы кең таралған.
- **Фильтр-программалар** немесе **«күзетшілер»** - ұдайы компьютер жадында болатын шағын резидентті программалар. Олар компьютердің операцияларын бақылайды және компьютер жұмысының барысында вирустарға тән күмәнді әрекеттерді табады. Пайдаланушылар, әдетте күзетшіні қолданбайды, өйткені әрдайым берілетін ескерту жұмысқа кедергі келтіреді. Фильтр-программалар вирусты көбеймей тұрып, оның өмірінің ең алғашқы сатысында табуға мүмкіндік береді, бірақ олар файлдар мен дискілерді «емдемейді», сондықтан вирустарды жою үшін фагтарды қолдану қажет болады.
-

- **В) Антивирустық программаларға қысқаша шолу**
- Антивирустық программаларды таңдаған кезде тек ғана вирустарды табу қасиетіне карамай, сонымен қатар жаңа вирустарды табу, антивирустың базасының вирустар санын анықтауына, базаны жаңалау жиілігіне және қосымша қызметтеріне де қарау керек.
- Қазіргі кезде көптеген антивирустық программалар бар. Солардың танымалдарын қарастырайық.
- **Norton AntiVirus 4.0 и 5.0 (производитель: «Symantec»).**
- Вирустарды тану пайызы өте жоғары (100 пайыз). Программада белгісіз жаңа вирустарды табу механизмі жұмыс істейді. Бұл программаның кемшілігі баптауы қиын (бірақ базалық баптауын өзгерту талап етілмейді).
- **Dr Solomon’s AntiVirus (производитель: «Dr Solomon’s Software»).**
- Ең жақсы антивирустардың бірі болып саналады. Танымал әрі жаңа вирустарды 100 пайыз табады.

- **Dr.Web (производитель: «Диалог Наука»)**
- Танымал антивирустық программа. Вирустарды жақсы табады, бірақ басқа антивирустық программаларға қарағанда базасы әлдеқайда кішкентай.
- **Kaspersky Anti-Virus антивирустық программасы**
- Kaspersky Anti-Virus Scanner (Kaspersky AV Scanner) антивирустық сканер – пайдаланушы сұрауы бойынша компьютерді вирустар барына тексеру және бар болған жағдайда вирустарды жою.
- Жұмыс кезінде антивирустық сканер келесі функциялар орындайды.
- Тексеруге көрсетілген дискілерде, жүктеме секторларда және жедел жадыда файлдардың барлық типтеріндегі вирустарды анықтайды және жояды.
- PKLITE, LZEXE, DIET, COM2EXE және басқа қысу утилиттерімен қысылған файлдардағы вирустарды анықтайды және жояды.
- Барлық танымал форматтарда (ZIP, ARJ, LHA, RAR және т.б.) архивтелген файлдарда вирустарды анықтайды және жояды.
- Ең танымал почталық жүйелердің локальды почтаық жәшіктеріндегі вирустарды анықтайды және жояды.
- Таныс емес вирустарды іздеудің дамыған эвристикалық механизмін қолданады (тиімділігі - 92%).

- ***Антивирустық сканерді қосу***
- Қосудың ең тез әдістерінің бірі–Windows-тың басты менюі арқылы қосу. Ол үшін Пуск (Start) батырмасын басып, Программы (Programs) бөлімін таңдап, Kaspersky Anti-Virus тобына өтіңіз де, Kaspersky Anti-Virus Scanner пунктін таңдаңыз.
- Программаны қосқан соң экранда программаның басты терезесі ашылады, есептер панелінде белгі пайда болады, оны тышқанның оң жақ батырмасымен шерту арқылы жүйелік меню ашуға болады.
- Жүйелік меню келесі пункттерден тұрады:
- Параметры Kaspersky Anti-Virus Scanner… — программаның басты менюін ашу.
- Начать сканирование / Остановить сканирование — сканерлеуді бастау / сканерлеуді аяқтау.

- Қазіргі кезде шетел фирмалары мен мамандары үлкен антивирустық бағдарламаны құрды. Олардың көбі кең таралып, вирустардан қорғанудың жаңа құралы ретінде қолданылуда.
- Дербес компьютерлердің тұтынушылары АҚ «Диалог-Наука» өндіріп шығарған Adinf және Adinf Cure Module антивирустық программаларын қолдануда. Aidstest бағдарламасы өзінің жақсы жұмыс істеуі үшін оперативті жадта басқа резиденттік антивирустық бағдарламаны жоқ болуын талап етеді. Aidstest программасын іске қосқанда ол бірінші оперативті жадта вирустың бар-жоғын тексеріп, оны қауіпсіз қылады. Вирустарды қауіпсіз қылғаннан кейін, компьютерді жүктеу керектігіне сұраныс болады. Компьютерді RESET кнопкасымен жүктеген дұрыс, әйтпесе егер оны Ctrl+Alt+Del клавиштерімен жүктегенде онда вирус сақталып қалуы мүмкін. Сол себепті компьютерге салынған дискіні антивирустық бағдарламасымен тексеру керек.
- Полиморфты вирустармен күресу үшін жақында салыстырмалы түрде шыққан полифаг- бағдарлама Doctor-Web-ті қолдану тиімді.

- Ревизор ADINF программасы мутант вирустарды және бүгінгі күнге белгісіз вирустарды қосқанда кез-келген вирустарды табуға мүмкіндік береді. Бір логикалық дискіні тексеру уақыты өте аз.Сондықтан көп уақытты жұмсамай ADINF программасын күнделікті қолдануға болады.