Дәріс 3. Вирус түрлері туралы түсінік. Ақпараттық жүйенің ықтимал бұзылуының түрлері

Жоспары:

1 Компьютерлік вирус ұғымы
2 Компьютерлік вирустар классификациясы
3 АЖ-ның ықтимал бұзылуының түрлері

Компьютерлік вирус-бұл компьютерлік технологиялар мен ақпараттық технологиялардың даму процесінде пайда болған құбылыс.

Компьютерлік вирустар өз атауын биологиялық вирустармен белгілі бір ұқсастыққа байланысты:

- өзін-өзі көбейту қабілеті;
- жоғары таралу жылдамдығы;
- зардап шеккен жүйелердің селективтілігі (әр вирус тек белгілі бір жүйелерге немесе жүйелердің біртекті топтарына әсер етеді);
- әлі жұқтырмаған жүйелерді жұқтыру қабілеті;
- олармен күресудің қиындықтары және т. б.

Жақында компьютерлік және биологиялық вирустарға тән осы ерекшеліктерге модификациялар мен вирустардың жаңа ұрпақтарының пайда болу жылдамдығын үнемі арттыруға болады.

Ақпараттық жүйеге енгеннен кейін компьютерлік вирус зиянсыз визуалды немесе дыбыстық эффектілермен шектелуі мүмкін, бірақ деректердің жоғалуына немесе бұрмалануына, құпия ақпараттың ағып кетуіне әкелуі мүмкін. Бүгінгі таңда компьютерлерге көптеген маңызды мәселелерді шешуге сенеді. Сондықтан ақпараттық жүйенің істен шығуы өте ауыр зардаптарға әкелуі мүмкін.

Өзін-өзі көбейтетін жасанды құрылымдарды зерттеу өткен ғасырдың ортасында жүргізілді. Алғашқы белгілі басылым 1951 жылдан басталады онда Джон фон Нейман өзін-өзі көбейтетін компьютерлік бағдарламаларды құру мәселесін тұжырымдап, зерттеді. Компьютерлік вирус термині кейінірек пайда болды. Оны алғаш рет Оңтүстік Калифорния университетінің қызметкері Фред Коэн 1984 жылы АҚШ-та өткен Ақпарат қауіпсіздігі жөніндегі жетінші конференцияда қолданды. Бұл термин бағдарламалық кодтың зиянды бөлігі деп аталды.

Компьютерлік вирустардың ең алғашқы мысалы 60-шы жылдары негізгі кадрларда мезгіл-мезгіл пайда болатын "қоян бағдарламалары" (қоян) болуы мүмкін. Олар ешқандай зиян келтірмеді, бірақ жүйенің ресурстарын көбірек түсіріп, басқа тапсырмалардан процессор уақытын алып, өздерін бірнеше рет көшіруге мүмкіндік алды.

Сірә," қояндар " жүйеден жүйеге берілмеді және тек жергілікті құбылыс болды - компьютерге қызмет көрсететін бағдарламашылардың қателіктері немесе еркеліктері.

70-ші жылдардың басында ғаламдық компьютерлік желілер арқылы өзін-өзі көбейтетін "the Creeper" вирусы пайда болды. Бұл зиянсыз болды, бірақ ол басқа біреудің компьютеріне иесінің білместен және оның қалауына қарсы кіруге болатындығын көрсетті. Бұл вируспен күресу үшін "The Reaper" (Reaper) бағдарламасы құрылды - алғашқы белгілі антивирустық бағдарлама. Ол байлам сияқты репродукцияланып, соңғысының кездескен барлық көшірмелерін жойды.

Сонымен, *компьютерлік вирус* дегеніміз не? Тарихи тұрғыдан алғанда, алғашқы анықтаманы 1984 жылы Ф. Коэн берген: "компьютерлік вирус-бұл басқа бағдарламаларды жұқтыруы мүмкін, оларды өзгертілген көшірмесін қосу арқылы өзгерте алады, ал соңғысы одан әрі көбею қабілетін сақтайды".

Қазіргі уақытта компьютерлік вирус деп келесі қасиеттері бар бағдарламалық кодты түсіну әдеттегідей:

- түпнұсқамен міндетті түрде сәйкес келмейтін, бірақ түпнұсқаның қасиеттеріне ие жеке көшірмелерді жасау мүмкіндігі (өзін-өзі көбейту);
- есептеуіш жүйенің орындалатын объектілеріне жасалатын көшірмелерді енгізуді қамтамасыз ететін тетіктің болуы.

Бұл қасиеттер қажет, бірақ жеткіліксіз.

Бұл қасиеттер есептеу ортасында осы зиянды бағдарламаның деструктивті және жасырын әрекеттерінің қасиеттерімен толықтырылуы керек.

Евгений Касперский орындалатын кодтың кейбір реттілігі вирус болуы үшін тек міндетті шартты тұжырымдау мүмкін деп санайды.

Компьютерлік вирустың міндетті (қажетті) қасиеті-сіздің көшірмелеріңізді жасау (түпнұсқамен сәйкес келмеуі керек) және оларды есептеу желілеріне және/немесе файлдарға, компьютердің жүйелік аймақтарына және басқа орындалатын объектілерге енгізу мүмкіндігі. Бұл жағдайда телнұсқалар одан әрі тарату қабілетін сақтайды.

Айта кету керек, бұл шарт түпкілікті емес.

Компьютерлік вирустар классификациясы

Әдебиетте вирустарды жіктеуге болатын төрт негізгі белгі берілген::

- тіршілік ету ортасы;
- тіршілік ету ортасын жұқтыру тәсілі;
- жұмыс алгоритмінің ерекшеліктері;
- деструктивті мүмкіндіктер.

Тіршілік ету ортасы бойынша компьютерлік вирустар файлдық, жүктеу, желілік және макровирустарға бөлінеді.

Файлдық вирустар орындалатын файлдарға орналастырылады-бұл вирустың ең көп таралған түрі. Файлдық вирусты енгізу барлық танымал операциялық жүйелердің барлық орындалатын файлдарына мүмкін. Бүгінгі күні орындалатын

объектілердің барлық түрлеріне әсер ететін вирустар белгілі: командалық файлдар (bat), жүктелетін драйверлер (sys) және орындалатын екілік файлдар (exe, com).

Жүктеу вирустары өздерін дискінің жүктеу секторына (жүктеу секторы) немесе қатты дискінің жүйелік жүктеушісі (Master Boot Record) бар секторға жазады. Кейде жүктеу вирустары бутовые деп аталады. Дискілерді жұқтырған кезде, жүктеу вирустары жүйені жүктеу кезінде басқаруды алатын кез-келген бағдарламаның орнына өз кодтарын "ауыстырады".

Вирус жүйені қайта іске қосқан кезде оны жадқа санауға және басқаруды бастапқы жүктеуші кодына емес, вирус кодына беруге" мәжбүр етеді". Дискіні жұқтырған кезде вирус көп жағдайда бастапқы жүктеу секторын (немесе MBR) дискінің басқа секторына (мысалы, бірінші бос) тасымалдайды. Егер вирустың ұзындығы сектордың ұзындығынан үлкен болса, онда вирустың бірінші бөлігі жұқтырған секторға орналастырылады, қалған бөліктері басқа секторларға орналастырылады (мысалы, бірінші бос).

Желілік вирустар оларды тарату үшін протоколдарды немесе компьютерлік желілер мен электрондық пошта командаларын пайдаланады. Желілік вирустар кейде "құрт"типті бағдарламалар деп аталады. Желілік құрттар nternet құрттары (Интернет арқылы таралады), LAN құрттары (жергілікті желі арқылы таралады), IRC құрттары Internet Relay Chat (чаттар арқылы таралады) болып бөлінеді. Аралас түрлері де бар.

Макровирустар-бұл кейбір деректер жүйелеріне енгізілген макро тілдік бағдарламалар (атап айтқанда Microsoft Word, Microsoft Excel редакторлары). Олардың көбеюі үшін мұндай вирустар макро тілдердің мүмкіндіктерін пайдаланады және олардың көмегімен өздерін бір вирус жұққан файлдан (құжат немесе кесте) басқаларына ауыстырады. Вирустар вирус жұққан файлды ашқанда немесе жапқанда басқарылады, стандартты файл функцияларын ұстайды, содан кейін қандай да бір жолмен кіретін файлдарды жұқтырады.

Тіршілік ету ортасын жұқтыру әдісіне сәйкес компьютерлік вирустар резидент және резидент емес болып бөлінеді. Вирус және ол енгізілген объект Операциялық жүйе үшін біртұтас болғандықтан, жүктелгеннен кейін олар бір мекен-жай кеңістігінде орналасады. Нысан аяқталғаннан кейін ол жедел жадтан шығарылады, сонымен бірге вирус бір уақытта түсіріліп, сақтаудың пассивті сатысына өтеді.

Алайда, вирустардың кейбір түрлері жадта сақталуы мүмкін және вирус тасымалдаушы аяқталғаннан кейін белсенді болып қалады. Бұл вирустар резидент деп аталды. Осылайша, резиденттік вирустар - бұл компьютер жұқтырған кезде өзінің резиденттік бөлігін жедел жадта қалдыратын вирустар, содан кейін ол операциялық жүйенің инфекция объектілеріне жүгінуін тоқтатады және оларға енгізіледі.

Жұмыс алгоритмінің ерекшеліктері бойынша компьютерлік вирустар спутниктік вирустар (серіктес), құрт вирустары (құрт), жасырын вирустар (көрінбейтін вирустар) және полиморфты вирустар болып бөлінеді.

Спутниктік вирустардың әсер ету механизмі орындалатын файлдардың көшірмелерін жасаудан тұрады. Көшірмелерге орындалатын файлмен бірдей атау беріледі, бірақ кеңейтім com болып өзгереді. Жалпы атауы бар файлды іске қосқан кезде, амалдық жүйе алдымен вирус болып табылатын com кеңейтімі бар файлды жүктейді. Файл-вирус файлды eche кеңейтімімен іске қосады.

Құрт вирустары желіден жұмыс станциясына түседі, желінің басқа абоненттеріне вирустың мекен-жайларын есептейді және вирустың таралуын жүзеге асырады.

Вирус файлдарды өзгертпейді және дискілерді жүктеу секторларына жазылмайды.

Жасырын вирустар өздерінің тіршілік ету ортасында болуын амалдық жүйенің зардап шеккен файлдарға, секторларға жүгінуін тоқтату арқылы жасырады және операциялық жүйені инфекцияланбаған ақпарат аймақтарына бағыттайды, осылайша вирус жұққан файлдардың "тазалығын" еліктейді. Вирус

ол резидент, амалдық жүйенің бағдарламалары ретінде жасырылған және жадта қозғалуы мүмкін. Мұндай вирустар үзілістер болған кезде белсендіріледі, орындалады

белгілі бір әрекеттер, соның ішінде камуфляж, содан кейін ғана Басқару осы үзілістерді өңдейтін операциялық жүйенің бағдарламаларына беріледі. Осылайша, жасырын вирустар жүйеде олардың болуын жасыра алады және антивирустық бағдарламалармен анықталудан аулақ болады.

Деструктивті мүмкіндіктерге сәйкес компьютерлік вирустар зиянсыз, қауіпті емес, қауіпті және өте қауіпті болып бөлінеді.

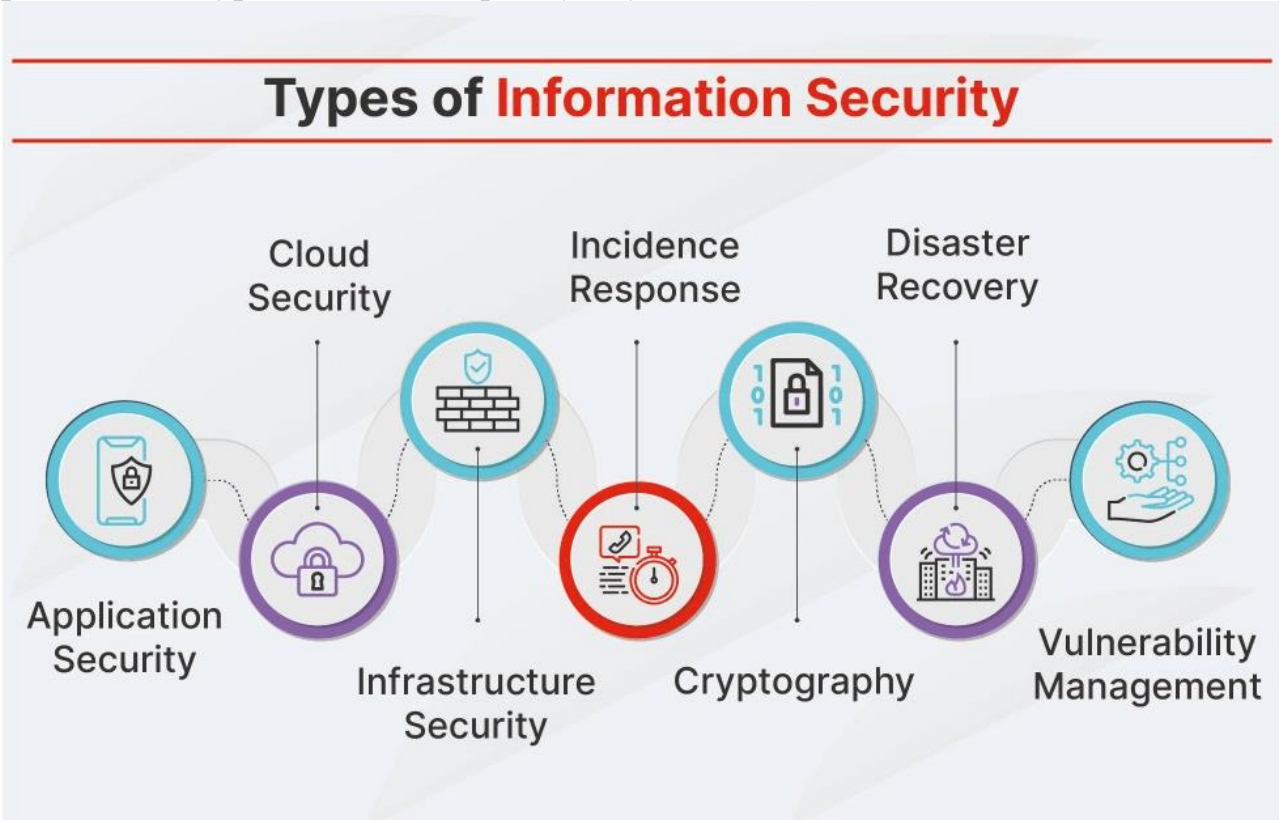
Зиянсыз вирустар-бұл компьютердің жұмысына ешқандай әсер етпейтін, тек дискідегі бос жадты азайтатын вирустар. Олар тек өзін-өзі тарату механизмін жүзеге асырады.

ақпараттық қауіпсіздік найзағайларын әртүрлі белгілер бойынша жіктеуге болады:

Қауіптер бағытталған ақпараттық қауіпсіздік аспектісі бойынша:

Құпиялылық қатерлері (ақпаратқа заңсыз қол жеткізу). Құпиялылықты бұзу қаупі-бұл ақпарат оған қол жеткізуге құқығы жоқ адамға белгілі болады. Бұл есептеу жүйесінде сақталған немесе бір жүйеден екіншісіне берілетін кейбір шектеулі ақпаратқа қол жеткізілген кезде орын алады. Құпиялылықты бұзу қаупіне байланысты "ағып кету" термині қолданылады. Мұндай қауіптер "адам факторы" (мысалы, бір немесе басқа пайдаланушыға басқа Пайдаланушының артықшылықтарын кездейсоқ беру), бағдарламалық және аппараттық құралдардың жұмысындағы ақауларға байланысты туындауы мүмкін. Қолжетімділігі шектеулі ақпаратқа мемлекеттік құпия[2] және құпия ақпарат[3] (коммерциялық құпия, Дербес деректер, кәсіптік түрлері құпия: дәрігерлік,

адвокаттық, банктік, қызметтік, нотариаттық, сақтандыру, тергеу және сот ісін жүргізу құпиясы, хат алмасу, телефон арқылы сөйлесу, пошта жөнелтімдері, телеграф немесе өзге де хабарламалар (байланыс құпиясы)жатады, ресми жарияланғанға дейін өнертабыстың, пайдалы модельдің немесе өнеркәсіптік үлгінің мәні туралы мәліметтер (ноу-хау) және т.б.).



Тұтастық қатерлері (деректердің заңсыз өзгеруі). Тұтастықты бұзу қаупі-бұл ақпараттық жүйеде сақталған белгілі бір ақпаратты өзгерту ықтималдығымен байланысты қауіптер. Тұтастықтың бұзылуына әртүрлі факторлар себеп болуы мүмкін — қызметкерлердің қасақана әрекеттерінен жабдықтың істен шығуына дейін.

Қолжетімділік қатерлері (ақпараттық жүйенің ресурстарына қол жеткізуді мүмкін етпейтін немесе қиындататын әрекеттерді жүзеге асыру). Қолжетімділіктің бұзылуы қызметке немесе ақпаратқа қол жеткізу бұғатталатын немесе белгілі бір бизнес мақсаттарының орындалуын қамтамасыз етпейтін уақыт ішінде мүмкін болатын жағдайларды жасауды білдіреді.

Қауіптер көзінің орналасуы бойынша:

Ішкі (қауіп көздері жүйенің ішінде орналасқан);

Сыртқы (қауіп көздері жүйеден тыс).

Келтірілген залалдың мөлшері бойынша:

Жалпы (жалпы қауіпсіздік объектісіне зиян келтіру, айтарлықтай зиян келтіру);

Жергілікті (қауіпсіздік объектісінің жекелеген бөліктеріне зиян келтіру);

Жеке (қауіпсіздік объектісі элементтерінің жекелеген қасиеттеріне зиян келтіру).

Ақпараттық жүйеге әсер ету дәрежесі бойынша:

Пассивті (жүйенің құрылымы мен мазмұны өзгермейді);

Белсенді (жүйенің құрылымы мен мазмұны өзгеріске ұшырайды).

Пайда болу табиғаты бойынша:

Табиғи (объективті) - адамның еркіне тәуелді емес объективті физикалық процестердің немесе табиғи табиғи құбылыстардың ақпараттық ортаға әсерінен туындаған;

Жасанды (субъективті) - адамның ақпараттық саласына әсер етуден туындаған. Жасанды қауіптердің ішінде өз кезегінде:

Күтпеген (кездейсоқ) қауіптер — бағдарламалық жасақтаманың, персоналдың қателіктері, жүйелердің дұрыс жұмыс істемеуі, есептеу және коммуникациялық техниканың істен шығуы;

Қасақана (қасақана) қауіптер — ақпаратқа заңсыз қол жеткізу, заңсыз қол жеткізу үшін пайдаланылатын арнайы бағдарламалық жасақтаманы әзірлеу, вирустық бағдарламаларды әзірлеу және тарату және т.б. қасақана қауіптер адамдардың әрекеттерінен туындайды. Ақпараттық қауіпсіздіктің негізгі мәселелері ең алдымен қасақана қауіп-қатерлермен байланысты, өйткені олар қылмыстар мен құқық бұзушылықтардың басты себебі болып табылады[4].

Ұсынылған әдебиеттер:

Негізгі әдебиеттер:

1. Нестеров, С. А. Основы информационной безопасности: учебник для вузов/ С. А. Нестеров. - Санкт-Петербург : Лань, 2021., 324 с. — ISBN 978-5-8114-6738-9.

2. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9

3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3

Қосымша әдебиеттер:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534- 07248-8

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва :

Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0