Видовете вируси са няколко основни с множество от подвидове. В тази версия са описани 30 вида вируси и 8 вида вирусоподобни програми. Често вирусите представляват наколко от тези "видове" събрани в един вирус. Пример: резидентни и Stealth едновременно или други качества като често пъти са по много. Комбинациите между тези "видове" е най-коварното при вирусите. Вирусите са написани като изпълним код който се самозаписва някъде из програмата като модифицира програмата да изпълнява този код или кодът се записва с стартовите сектори на дискетите или хард диска за да се изпълни. Така вирусът става активен и нанася своя удар върху софтуера. Има и вирусоподобни програми, които помагат на вирусите.

@Резидентни - те остават резидентни в паметта (така както остава някой драйвер до изключването или рестартирането на компютъра). От паметта вирусът може да се размножава и да смущава работата на компютъра и да повреждa файлове и цели програми.

@Boot - тези вируси се самокопират в зареждащия сектор на дискетите и на хард диска, като копират системните файлове (ако хард дискът или дискетата са системни) на друго място на дискетата или на хард диска. Така, при опит да се зареди от заразената системна дискета, вирусите се зареждат успоредно с ОС и нанасят своите удари върху софтуера.

@Вируси с директно действие – това са вируси, които се стартират, нанасят своя удар върху софтуера и се "самоизключват", но остават като инфекция.

@Stealth - вирусите са най – коварните, защото те причиняват големи щети и остават резидентни в RAM. Те още прикриват симптомите на вирусната инфекция и взаимодействат с различни антивирусни програми, като принуждават програмата да каже, че няма вируси. Тези вируси не показават промени по размерите на файла, който са инфектирали, което ги прави трудни за засичане и обезвреждане! Самият вирус лесно се укрива и трудно се премахва. Секторите от хард диска и (или) дискетата, където е записан оригиналът на вируса, се маркират като лоши (механично повредени), въпреки че не са повредени по никакъв начин. Всички анти-вирусни програми, които проверяват хард диска или дискетите "виждат" маркираното "Лош сектор" и го прескачат и не засичат вируса. Друга мярка за защита е заетата техника от полиморфичните вируси на самопроменящ се код на вируса за дпълнителна самозащита.

@Макро вируси – вируси, специално написани на "Word macro language" и на "Visual

Basic Macro language", като създават отделни макроси - вируси. Тези вируси често предизвикват правописни и стилистични грешки по текстовете на "WinWord", "MacWord", "DosWord", а също и по таблиците на "DosExcel", "WinExcel и "MacExcel" . Тези вируси не правят разлика между отделните версии на Word и Excel. Макро вирусите се пренасят като макроси по документи и таблици със записани макроси. Стартирането на макросите стартира и макро вирусите. Нападат първо файла Normal.dot (когато става дума за Word) или Normal.xlt (когато става дума за Excel), а после и всеки отворен документ.

@Логическите вируси предизвикват не само множество щети, но и много логически грешки по време на работа. Те се активират, ако определени условия се изпълнят правилно.

@Time-bomb вирусите са вируси с назначена дата на активиране. Ако попаднат в компютъра преди датата на активирането им, те само се размножават без да предизвикват повреди. На датата на активирането или след нея вирусите се активират и нанасят своя удар. Пример за такъв вирус е CIH (т.нар. Чернобил), който се активира на 26-ти април.

@MBR (Master Boot Record) вирусите работят на принцип, близък на Boot вирусите. С тази разлика, че те не копират системните файлове, а се "смесват" с тях и ги модифицират, за да приемат вируса като част от тях, което прави невъможно премахването им. Когато от заразен системен хард диск или заразена от системна дискета, се зарежда ОС, вирусите се зареждат отново, успоредно с нея и нанасят своя жесток удар върху софтуера.

@BIOS вирусите - това са тези вируси които освен че причиняват щети, правят и промени по BIOS-а на компютъра или се записват там. Най-честите промени са свързани с флопитата-често се обявява, че флопитата не са инсталирани и компютърът не може да ги използва. Разбира се, често пъти вирусите така разбъркват данните от BIOS-а, че компютърът не може да се стартира. Вирусите, причинили всякакви промени по BIOS-а, не позволяват нормалното пре-конфигуриране. Трети вируси се самозаписват в BIOS-а и се самостартират от там (още преди ОС да е заредена). Борбата с тези вируси е най-сложна защото те контролират целия хардуер и софтуер.

@Размножаващи се - тези вируси само се размножават - без да причиняват нинакви повреди и каквито и да било други щети и последици.

@Joke programs - всъщност те не са вируси, а шегаджийски програми, които се разпространяват като вирусите. Тези програми не причиняват никакви щети. Те само извеждат глупави съобщения и още по-глупави шеги.

@Virus creating tool viruses - не са вируси а инструменти за създаване на вируси в големи количества. Вирусите, създадени от тези инструменти, обикновено са шифровани и лесно засечими, както и лесно отстраними.

@ANTI-VIRUS viruses - не са вируси, а антивирусни програми, които се разпространяват като вирусите и обикновено са блок за самотестване срещу вируси. Желателно е да не ги допускате по хард диска, дисковете и дискетите си.

@Хардуерните вируси са вируси, които спъват работата на хардуера по всякакви начини, симулирайки хардуерни проблеми, механически повредени сектори по дисковете и дискетите, повреди по тях, провалят тестовете на дисковите контролери и принуждават копютърът да не работи с дадени компоненти от хардуера. Вируса *FireBurn* е точно такъв - с цел самосъхранение блокира клавиатурата и мишката

@COM вирус е този вирус, който напада и заразява само

“-.COM” файлове.

@EXE вирус е този вирус, който напада и заразява само

“-.EXE” файлове.

@COM/EXE вирус е този вирус, който напада и заразява както “-.COM”, така и файлове на “-.EXE”.

@Суматорните вируси са предвидени да събират и закръглят стойности предизвиквайки много големи бъркотии. Започвайки от най-ниските нива на Excel, стигайки до най-високите нива на счетоводни, ведомствени, подбанкови и банкови нива и функции. Тези вируси могат да объркат сметки, подменят стойности на резултати и знаци, в зависимост от индентификацията на дадено действие и сумите и вида на стойностите. Често тези вируси вкарват в обръщение неверни стойности, представяйки ги за верни, както и да отхвърлят верните стойности, като ги представят за грешни.

@Псевдорутерите са вируси, които само смущават трансфера на данни, като предизвикват частични задръствания по мрежите и трансферните линии. Попаднали на подходящо устройство или в главния компютър на мрежа, те започват да се размножавт и да предизвикват тотални задръствания по мрежите и трансферните линии, препращайки информацията по различни вектори, където тя се губи. *E-mail* и локалните мрежи са главното им поле на действие.

@Информационни замърсители са вируси с функции като на псевдорутерите (само че за предизвикахето на тотално задръстване и объркване на мрежите и на трансферните линии не е необходимо да са в главен компютър или устройство, а където и да било по мрежата и устройствата). Често тези вируси пращат пратка на адрес, различен от този който потребителят е посочил или обявяват съществуващ адрес в мрежа за невалиден или ако се набере грешен адрес, вирусите го приемат за валиден и пращат информацията в различни вектори на трансфер, където тя се губи.

@Полиморфните вируси са много трудни за засичане, идентифициране и премахване, защото те постоянно променят своя код. Няма два еднакви кода на един и същ полиморфичен вирус, който е способен да направи хиляди самомодификации, с цел да се самопредпази от антивирусните програми. Принципът на полиморфията при вирусите е всяко копие да се кодира различно.

@Биокомпютърните вируси са много интересни. Те представляват нещо като един вирус разделен на две "половини" които "половини" са програмирани да се търсят взаимно (една - друга) и когато се открият - да се съединят и да образуват вируса. Всяка (коя да е) "половина" поотделно е безобидна, но ако двете се съберат заедно, вирусът образува и се активира и нанася своя удар срещу софтуера.

@Бинарни вируси са вирусите, които са написани на машинен език и също като биокомпютърните вируси са в две части които взаимно се търсят една друга. Това че са написани на машинен език ги прави малки и трудно засечими.

@RAM вирусите са вируси, които само се размножават и седят в оперативната памет (RAM) и окупират голяма част от нея и не се улавят от антивирусните програми, сканиращи RAM за резидентни вируси. Те не причиняват никакви щети, но бързо и лесно се размножават. Тези вируси често пъти заставят програмата да не стартира и да изведе съобщение за недостатъчно RAM-памет, въпреки че компютърът в повечето случай има достатъчно количество RAM-памет, за да изпълни програмата

@Companion вирусите с вируси, които са нещо средно между шегаджийските програми *(joke programs),*
RAM-вирусите и размножаващите се вируси. Този тип вируси се записват в началото на програмата и при неиното изпълнение вируса задава някакъв въпрос. При правилен, отгвор вирусът стартира програмата. При грешен - вирусът или блокира компютъра, или го рестартира.

@Вируси - убийци - по непотвърдени данни тази категория вируси не поврежда данни или каквото и да било друго, но убива оператора. Такъв вирус са използвали в КГБ като крайна мярка на защита на компютрите им през Студената война. Вирусът се е казвал “666” и няма нищо общо с разпространения глупав файлов “666” вирус, носещ същото име за заблуда и е объркал до такава степен мозъчните вълни, че е причинявял невероятно главоболие и... смърт! Много любопитни хакери, кракери и американски експерти и програмисти са се опитвали да откраднат вируса, но никой още не е успял...

@FAT Scrabmlers - тези вируси така разбъркват двете копия на FAT, че всичко, записано на диска, става негодно за каквито и да е манипулации. Двете Копия на FAT се разбъркват - всяко по различен начин (с цел максимални щети). Няма друг изход, освен форматиране от BIOS и след това предформатна подготовка с FDISK и повторно форматиране с Format /u /c /s.

@Java вируси - това са вируси, които могат да заразяват само *Java* програми и заразяват всякакви компютри и операционни среди, защото се стартират не от ОС, а от браузъра.

@E - Mail вируси - особено актуална категория вируси. Разпространява се чрез електронна поща и използва адресната книга, за да нападне нови компютри.

@WAP вируси – току-що появила се категория с един-единствен представител – “*Timofo nica”.*
Нападат GSM, Palm PC и лаптопи, ако те използват WAP. Засега няма данни за вредни кодове, но се очаква да се получи нещо като разбъркване на мрежите, сривове, раздуване на телефонни сметки, разпращане на телефонни номера или адреси.

Забележка: Вирусите за *PC* не могат да заразяват *Power Machintosh* и вирусите за *Powe r Machintosh*
не могат са заразяват
PC
компютри, защото има разлики в интерфейса на двете групи хардуер. Двете групи са взаимно несъвместими. Тази забележка не важи за точка 28
(Java вирусите).

@Червеи (Worms) – програми, които се самокопират, но и заразяват други програми (не винаги причинявят щети).

@Host червеи - имат нужда от локална мрежа, за да се самокопират и за да могат да функционират.

@Net Worm - разпространява части от себе си по мрежа и има нужда от нея, за да може частите му да работят съвместно. Може да съществува и на единичен компютър, но се самокопира на различни места и/или дялове на хард диска.

@Троянски кон - това са програми, които са скрити в други програми. Тази система е ефективна, докато основната програма върши нещо. Във фонов режим се имплантира вирус или се създават други проблеми. Пример за това е FreeWare програмата *ProMail 2000 v. 1.02,*
която служи като оптимизатор на мрежовия трафик и разпределение на пощата. Програмата създава файла
ACCOUNT.INI
, в който се съдържат всички имена, пароли и привилегии за достъп на всички потребители и информация за степента на защита на мрежата, който файл се копира и копието му се изпраща като прикачен файл по електронна поща до създателя на програмата.

@"Терористи" (Droppers) – програми, направени за заобикаляне на антивирусните защити. При създаване се използва мощна криптираща система със защитна цел. Тази криптираща система прави невъзможно откриването от антивирусни програми. "Терористите" най-често траспортират и имплантират други вируси.

@Бомби - тези програми изчакват определено събитие на компютъра, което ще ги стартира и те ще инсталират вируса, който носят със себе си. Тези програми имат много и разнообразни начини на действие (все вредни) и се стартират от разнообразни събития в компютъра Ви или в определени дни.

@INI програми - тези програми са във формат на стандартен INI файл. Много опасни и силно разрушителни. Модифицират се системните файлове на Windows. Това реално са вредни опции в “-.INI” файловете.

@BAT инфектори - асоциират се с “-.BAT” файлове. Може да се асоцират всякакви унищожителни програми, съвместими с *PC*. Това е или елементарен BAT код, или е програма, която се извиква с модифицирани “-.BAT” файлове.