Компьютерная безопасность и защита информации:

Основные понятия, методы, средства

Информационная безопасность (ИБ). Угрозы безопасности информации. Методы защиты информации. Организационные, программно-технические, законодательные меры обеспечения ИБ. Вирусы. Основные свойства вирусов. Классификация вирусов. Пути заражения вирусами. Антивирусная защита. Пакеты антивирусных программ. Архивация данных.

Информационная безопасность

Информационная безопасность – состояние сохранности информационных ресурсов и защищённости законных прав личности и общества в информационной сфере.

Угроза безопасности – действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов.

Атака – реализованная угроза.

Причины потери информации

- ✓ Первая – **объективная**, связанная с выходом из строя аппаратуры (например, поломка жесткого диска с необратимой потерей отдельных секторов), порча отдельных файлов вследствие сбоев электропитания и т.д.

- ✓ Вторая – **человеческий фактор** - связана с ошибками разработчиков информационных систем (программ) и их пользователей, а также с чьими-то предумышленными действиями.

Утечка информации и несанкционированный доступ

Возможные направления:

- чтение остаточной информации в памяти компьютера после выполнения санкционированных запросов;
- копирование носителей информации и файлов информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- маскировка под запрос системы;
- использованием программных ловушек;

Программы-ловушки – это резидентные программные модули, обеспечивающие после их запуска легального или несанкционированного (скрытного внедрения) съем информации с одного или нескольких информационных внутренних или внешних каналов информационной системы, компьютера или доступной части сети, например, путем перехвата соответствующих прерываний

Утечка информации и несанкционированный доступ

Возможные направления:

- чтение остаточной информации в памяти компьютера после выполнения санкционированных запросов;
- копирование носителей информации и файлов информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- маскировка под запрос системы;
- использованием программных ловушек;
- использование недостатков операционной системы;
- незаконное подключение к аппаратуре и линиям связи;
- злоумышленный вывод из строя механизмов защиты;
- внедрение и использование компьютерных вирусов.

Угрозы безопасности при использовании e-mail

- Адреса электронной почты используются для рассылки спама. Адрес попадает в базы данных спамеров незаконным путем.
- Адреса электронной почты в Интернете легко подделать.
- Электронные письма могут быть легко модифицированы. Стандартное SMTP-письмо не содержит средств проверки целостности.
- Электронное письмо скорее похоже на открытку — его могут прочитать на каждой промежуточной станции.
- Нет гарантий доставки электронного письма.

Угрозы безопасности при использовании e-mail

- **Почтовая бомба** — это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока она не выйдет из строя.
- **Фишинг** (англ. phishing, от phony – обман и fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, цель которого получить идентификационные данные пользователей. Организаторы рассылают письма, в которых созданы ссылки на сайты, которые являются копией настоящих.
- «**Нигерийские письма**» – вид интернет-мошенничества, цель которого поиск жертвы, которая будет переводить деньги за несуществующие товары, услуги, мероприятия.

Защита информации

Защита информации – комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостность, доступность и, если нужно, конфиденциальность информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

Методы защиты информации

Ограничение доступа к информации

Заключается в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контрольного доступа лиц, связанных с объектом защиты по своим функциональным обязанностям, т.е. выделение специальных территорий, специальных зданий и помещений, создание контрольно-пропускного режима.

Задача подобных средств ограничения доступа – *исключить случайный и преднамеренный доступ посторонних лиц к комплексам средств автоматизации*.

Методы защиты информации

Распределение доступа к информации

Заключается в разделении информации на части и организации доступа к ним пользователей в соответствии с их функциональными обязанностями и полномочиями. Деление информации может производиться по степени важности или секретности, по функциональному назначению и другим признакам.

Задача этого метода *– существенно затруднить преднамеренный перехват информации нарушителем, предусмотреть механизм разделения привилегий при доступе к особо важным данным.*

Методы защиты информации

Распределение доступа к информации

Идентификация объектов – установление их подлинности в вычислительной системе и допуск к информации ограниченного пользования. Для этого каждому объекту или субъекту присваивается *уникальный номер* (образ, имя или число).

Объекты идентификации:

- человек (оператор, пользователь, должностное лицо);
- технические средства (ЭВМ, носители информации);
- информация (программы, документы, распечатки).

Методы защиты информации

Распределение доступа к информации

В качестве идентификаторов личности широко распространено применение *паролей*, которые записываются на специальные носители (*электронные ключи* или *карточки*).

Электронный ключ — электронное устройство, имеющее память, с записанной в ней аутентификационной информацией, с возможностью считывания этой информации неким идентифицирующим/ аутентифицирующим устройством.

Методы защиты информации

Криптографическое преобразование информации

Защита информации заключается в преобразовании ее составных частей (слов, букв, цифр, слогов) с помощью специальных алгоритмов и аппаратных решений (криптографические средства).

Управление процессом *шифрования* осуществляется с помощью периодически меняющегося кода ключей, обеспечивающего каждый раз оригинальное представления информации при использовании одного и того же алгоритма или устройства. Для ознакомления с зашифрованной информацией применяется процесс *декодирования* информации.

Методы защиты информации

Криптографическое преобразование информации

Метод повышает безопасность передачи данных в сетях ЭВМ, данных в удаленных устройствах памяти и при обмене информацией между удаленными объектами.

Методы защиты информации

Законодательные меры по защите информации

Заключаются в исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность за противоправные действия.

Цели законодательных мер *– предупреждение и сдерживание потенциальных нарушителей, а также привлечение к ответственности лиц за попытку преднамеренного несанкционированного доступа к информации.*

Методы защиты информации

Законодательные меры по защите информации

Законодательство Российской Федерации о защите информации основывается на следующих документах:

- ✓ Конституция Российской Федерации,
- ✓ Гражданский Кодекс РФ,
- ✓ Уголовный Кодекс РФ,
- ✓ Закон «Об информации, информационных технологиях и защите информации», N 149-ФЗ от 27.07.2006 г. http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=183056;fld=134;dst=100168;rnd=203280.635851457238273;;ts=020328004171474138656828

Методы защиты информации

Законодательные меры по защите информации

- ✓ Закон Российской Федерации "О безопасности", № 390-ФЗ от 28 декабря 2010 года,

http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=187049;dst=0;rnd=203280.04118967509475585;SRDSMODE=QSP_GENERAL;SEARCHPLUS=%uF0A7%093акон%20Российской%20Федерации%20%22О%20безопасности%22%2C%20;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=852122626203280783240527701383 9

Методы защиты информации

Законодательные меры по защите информации

- ✓ Закон Российской Федерации «О связи», N 126-ФЗ от 7.7.2003 (изменен 9 мая 2005 года),

http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=194751;dst=0;rnd=203280.7089516610363498;SRDSMODE=QSP_GENERAL;SEARCHPLUS=%uF0A7%093акон%20Российской%20Федерации%20%ABO%20связи%BB%2C%20;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=190791561203280106939729816307 4

Методы защиты информации

Законодательные меры по защите информации

- ✓ Закон «О государственной тайне», РФ N 5485-1 от 21.07.1993 г. (изменен 8 марта 2015 года),

http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=176315;dst=0;rnd=203280.421552062992298;SRDSMODE=QSP_GENERAL;SEARCHPLUS=%uF0A7%093акон%20%ABO%20государственной%20тайне%BB%2C%20;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=196733561720328024256922892650912

Методы защиты информации

Законодательные меры по защите информации

Тексты документов см. в некоммерческая интернет-версия Консультант-плюс:

http://base.consultant.ru/cons/cgi/online.cgi?req=home;rnd=0.735053279750118 8

Методы защиты информации

Законодательные меры по защите информации

Уголовный кодекс РФ содержит главу 28 "Преступления в сфере компьютерной информации", согласно которой преступлениями в сфере компьютерной информации являются:

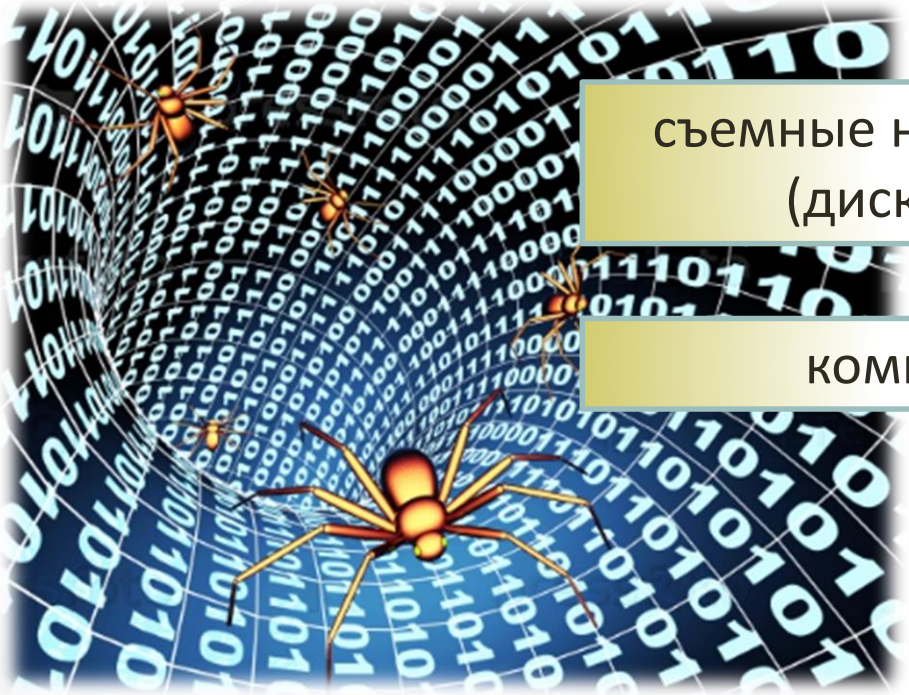
- Неправомерный доступ к компьютерной информации (ст.272 УК РФ);
- Создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ);
- Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ).

Компьютерные вирусы

Компьютерный вирус – это специально написанная программа, как правило, небольшая по размерам, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области дисков и в вычислительные сети (причем эти копии сохраняют способность к размножению) с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе на компьютере.

Компьютерные вирусы

Основные пути проникновения вирусов в компьютер:



- съемные носители информации (диски и флэш-карты)
- компьютерные сети

Компьютерные вирусы

Процесс внедрения вирусом своей копии в другую программу (системную область диска и т.д.) называется **заражением**, а объект, содержащий вирус (программа или иной), является **зараженным**.

Зараженный диск – это диск, в загрузочном секторе которого находится вирус.

Зараженный файл – это файл, содержащий внедренный в него вирус.

Признаки проявления вирусов

- невозможность загрузки операционной системы;
- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- блокировка ввода с клавиатуры;
- замедление работы компьютера;
- изменение размеров, даты и времени создания файлов;
- значительное увеличение количества файлов на диске;
- исчезновение файлов и каталогов или искажение их содержимого;
- существенное уменьшение размера свободной оперативной памяти;

Признаки проявления вирусов

- блокировка записи на жесткий диск;
- непредусмотренное требование снять защиту с дискеты;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые «зависания» и сбои в работе компьютера.

Профилактика защиты от вирусов

Профилактика защиты от вирусов

- ✓ Установить на компьютере современное вирусное программное обеспечение и постоянно обновлять его;
- ✓ перед считывание информации с переносных источников памяти (дискет лазерных дисков и флэш-карт) всегда проверять их на наличие вирусов;
- ✓ при переносе на компьютер файлов в архивированном виде проверять сам архив или файлы в процессе их распаковки на жесткий диск (такая возможность предусмотрена современными антивирусными программами);
- ✓ использовать антивирусные программы для контроля всех файлов, получаемых из компьютерных сетей;

Профилактика защиты от вирусов

- ✓ периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования памяти, системных областей дисков и файлов, предварительно загрузив операционную систему с защищенного от записи системного диска (компакт-диска или флэш-карты);
- ✓ защищать дискеты (флэш-карты) от записи при работе на других компьютерах, если на них не должна производиться запись информации;
- ✓ обязательно делать архивные копии информации на альтернативных носителях (дисках или флэш-картах).

Классификация вирусов

По разрушительным возможностям

- **Неопасные вирусы**.

  Они уменьшают объем памяти в результате своего распространения и иногда выдают какие-либо текстовые, графические или звуковые сообщения, но не осуществляют сознательной порчи информации;

- **Опасные вирусы**.

  Приводят к различным нарушениям в работе компьютера, например, выполняют перезагрузку компьютера, блокируют или изменяют функции клавиш клавиатуры, замедляют работу компьютера и т.п.;

- **Очень опасные вирусы**.

  Приводят к потере программ и данных, стиранию информации в системных областях памяти и даже к выходу из строя комплектующих частей компьютера, например, жесткого диска и материнской платы.

Классификация вирусов

По способу заражения

- **Резидентные вирусы** при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы ко всем объектам (файлам, загрузочным секторам дисков и т.п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

- **Нерезидентные вирусы** не заражают память компьютера и являются активными ограниченное время. Такие вирусы активизируются в определенные моменты, например, при обработке документов текстовым процессором.

Классификация вирусов

По среде обитания

- Файловые вирусы;
- Загрузочные вирусы;
- Файлово-загрузочные вирусы;
- Сетевые вирусы.

Классификация вирусов

По среде обитания

Файловые вирусы заражают исполняемые файлы (.exe, .com) и различные вспомогательные файлы, загружаемые при выполнении других программ. Вирус в зараженных файлах начинает свою работу при запуске той программы, в которой он находится. Некоторые вирусы умеют заражать драйверы устройств. Такой вирус начинает свою работу при загрузке данного драйвера.

Классификация вирусов

По среде обитания

Загрузочные вирусы внедряются в начальный сектор дисков, содержащий загрузчик операционной системы. Такие вирусы начинают свою работу при загрузке компьютера с зараженного диска. Загрузочные вирусы являются резидентными и заражают вставляемые в компьютер диски.

Классификация вирусов

По среде обитания

Файлово-загрузочные вирусы заражают одновременно файлы и загрузочные сектора дисков (часто заражают системные файлы). Как правило, такие вирусы имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют технологии «стелс» и «полиморфик».

Классификация вирусов

По среде обитания

Сетевые вирусы распространяются по различным компьютерным сетям, например, по сети интернет. Такие вирусы самостоятельно передают свой код на удаленный сервер или рабочую станцию. Часто сетевые вирусы обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайне мере, «подтолкнуть» пользователя к запуску зараженного файла.

Классификация вирусов

По особенностям алгоритма

- Компаньоны (спутники);
- Репликаторы (черви);
- Паразиты;
- Троянские вирусы (квазивирусы);
- Невидимки (стелс);
- Макровирусы

Классификация вирусов

По особенностям алгоритма

Компаньоны (спутники) не изменяют файлы, а создают для исполняемых программ (.exe) одноименные командные программы (.com), которые при выполнении исходной программы запускаются первыми, а затем передают управление исходной программе (существовали ранее, обычно в ОС DOS).

Классификация вирусов

По особенностям алгоритма

Репликаторы (черви) распространяются по компьютерным сетям, проникая в память компьютеров, вычисляя адреса других сетевых компьютеров и рассылая по ним свои копии. Такие вирусы не изменяют файлы или сектора на дисках.

Паразиты при распространении своих копий изменяют содержимое файлов и секторов диска. К этой группе относятся вирусы, не являющиеся спутниками и червями.

Классификация вирусов

По особенностям алгоритма

Троянские вирусы (квазивирусы) маскируются под какие-нибудь полезные программы и активизируются при наступлении некоторого события (условия срабатывания). Такие вирусы содержат некоторые деструктивные действия, связанные с нарушением безопасности компьютерной системы, например, передают конфиденциальную информацию (пароли) или модифицируют программы систем защиты.

Классификация вирусов

По особенностям алгоритма

Невидимки (стелс) перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо себя незараженные файлы участки диска, поэтому их очень трудно обнаружить и обезвредить.

Классификация вирусов

По особенностям алгоритма

Мутанты (призраки) также маскируются, постоянно модифицируя себя таким образом, что не содержат одинаковых фрагментов. Такие вирусы содержат алгоритмы шифровки-расшифровки и хранят свое тело в закодированном виде, постоянно меняя параметры кодировки. Поэтому такие вирусы самые сложные в обнаружении.

Классификация вирусов

По особенностям алгоритма

Макровирусы заражают документы, в которых предусмотрено выполнение макрокоманд (макросов). При открытии такого документа вначале исполняются содержащиеся в нем макросы (в том числе и макровирусы). Таким образом, вирус получает управление и совершает все вредные действия (в частности, находит и заражает еще не зараженные документы).

Антивирусное ПО

Специальные программы для обнаружения, уничтожения и защиты от компьютерных вирусов называются **антивирусными программами**.

Современные антивирусные программы представляют собой многофункциональные продукты, сочетающие в себе как профилактические возможности, так и средства лечения от вирусов и восстановления данных.

Требования к антивирусным программам

- *Стабильность и надежность работы*;
- *Объем вирусной базы* (количество обнаруживаемых программой вирусов);
- *Скорость работы программы*;
- *Наличие дополнительных возможностей*,
  - алгоритмов определения неизвестных программе вирусов (эвристическое сканирование),
  - умение работать с файлами различных,
  - возможность восстанавливать зараженные файлы, наличие резидентного фильтра, осуществляющего проверку всех файлов «на лету», т.е. автоматически, по мере их записи на диск;
- *Многоплатформенность* (наличие версий программы под различные операционные системы).

Антивирусное ПО

	Антивирус Касперского, Kaspersky Anti-Virus (производитель «Лаборатория Касперского», с 1994 г.), лицензия – коммерческая
	Dr. Web (производитель «Диалог-Наука», с 1994 г.) Лицензия: Shareware
	McAfee VirusScan (производитель Symantec).

Антивирусное ПО

	Avira (производитель Avira GmbH & Co. KG, с 1986 г.)
	AVG Anti-Virus (разработчик AVG Techologies), лицензия – проприетарная
	АНТИВИРУС ESET NOD32 (разработчик ESET, лицензия – проприетарная)
	Avast! (разработчик AVAST Software, лицензия – условно-бесплатная)

Антивирусное ПО

Детекторы

Детекторы обеспечивают обнаружение вирусов в оперативной памяти и на внешних носителях, выдавая соответствующие сообщения. Они выполняют поиск известных вирусов по *сигнатуре* (повторяющемуся участку кода) и позволяют обнаруживать только известные вирусы (это недостаток).

Требуют регулярного обновления

Антивирусное ПО

Доктора (фаги)

Доктора (фаги) не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файлов тело вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов.

Требуют регулярного обновления

Антивирусное ПО

Фильтры (сторожа)

Небольшие резидентные программы, предназначенные для обнаружения подозрительных действий в работе компьютера, характерных для вирусов:

- запись в загрузочные сектора диска;
- прямая запись на диск по абсолютному адресу;
- изменение атрибутов файлов;
- попытка коррекции исполняемых файлов (.exe, .com);
- загрузка резидентной программы.

Антивирусное ПО

Фильтры (сторожа)

Способны обнаружить вирус на самой ранней стадии его существования до размножения.

не лечат файлы и диски,

существенно замедляют работу компьютера, так как они отслеживают любые действия компьютера, перехватывая все запросы к операционной системе на выполнение «подозрительных» действий.

Антивирусное ПО

Ревизоры (инспекторы)

Запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран. Как правило, сравнение состояний производят сразу после загрузки операционной системы.

При сравнении проверяются состояние загрузочного сектора и таблицы размещения файлов, длина, дата и время модификации файлов, контрольная сумма файла и другие параметры.

Антивирусное ПО

Вакцинаторы

Предотвращают заражение файлов известными вирусами. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедриться.

Применяются редко, так как имеют ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

Профилактика почтовых вирусов

- ✓ регулярное обновление почтовой программы и операционной системы;
- ✓ корректное обращение со всеми почтовыми вложениями, прикрепленными к основному сообщению:
- ✓ вложения, полученные из неизвестных источников, следует удалять, не открывая;
- ✓ нельзя сразу запускать программы, полученные по электронной почте, особенно вложения. Необходимо сохранить файл на диске, проверить его антивирусной программой и только затем запускать
- ✓ адекватная настройка почтовой программы, которая препятствует автоматическому воспроизведению сообщений и вложений.

Архивация данных

Для создания копий информации используются специализированные программы, которые можно разделить на два класса:

- **Программы резервного копирования**, соединяющие несколько файлов (и каталогов) в единый файл;
- **Программы-упаковщики (архиваторы)**, сокращающие объем исходных данных в результате компрессии (сжатия).

Архивация данных

Архиватор – это специальная программа, позволяющая работать с архивными файлами, т.е. запаковывать (сжимать) исходные файлы в архив и распаковывать (восстанавливать) их из архивов.

Архивный файл – это специальный файл, в котором по определенным алгоритмам сжатия упакован один или несколько объектов (папки, текстовые или табличные документы, рисунки, фотографии, программы или другие файлы) с целью более рационального размещения на диске (или передачи другим пользователям, в том числе по каналам связи).

Архивация данных

При выборе инструмента для работы с упакованными файлами (архивами) следует учитывать два фактора:

Эффективность – оптимальный баланс между экономией дисковой памятью и производительностью работы;

Совместимость – возможность обмена данными с другими пользователями.

Архивация данных

Показатели, характеризующие эффективность работы любого архиватора:

Коэффициент сжатия - отражает отношение размера архивного (сжатого) файла к исходному;

Коэффициент уменьшения - показывает, во сколько раз архивный файл меньше исходного.

Примеры архиваторов

		
Коммерческое	**Условно-бесплатное**	**Свободное**
с 20 апреля 1995 г.		С 18 июля 1999 г.

Выводы

Многообразие информации, циркулирующей в обществе, в том числе передаваемой по сетям, приводит к возникновению различных факторов, угрожающих ее безопасности.

Под *угрозой безопасности* понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов.

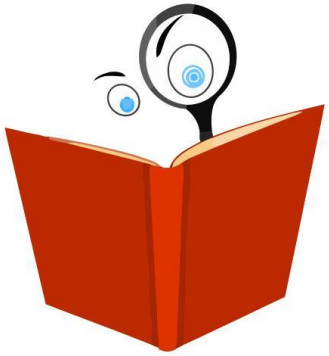
Безопасность информации может быть обеспечена реализацией комплекса организационных, программно-технических и законодательных мер.

Причинами таких событий, как потеря данных, «зависание» системы, выход из строя отдельных частей компьютера может быть вызвана заражением компьютера вирусом.

Выводы

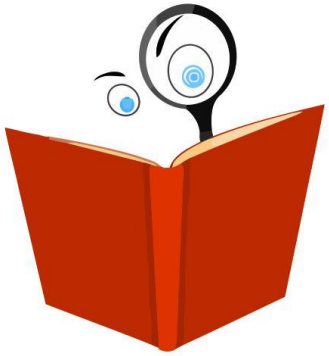
Защиту информации от компьютерных вирусов обеспечивает использование антивирусного программного обеспечения.

Для создания копий информации используются программы резервного копирования и архиваторы.



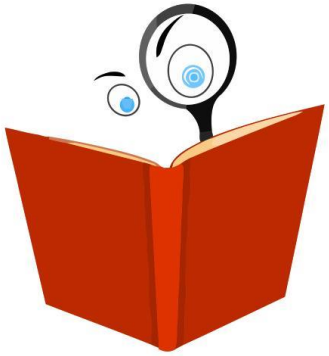
Словарь терминов

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.



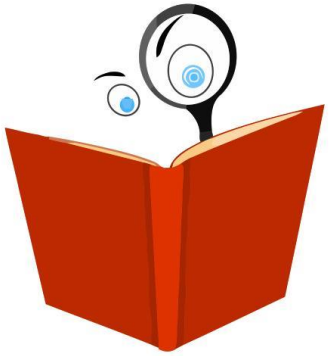
Словарь терминов

Архивный файл – это специальный файл, в котором по определенным алгоритмам сжатия упакован один или несколько объектов (папки, текстовые или табличные документы, рисунки, фотографии, программы или другие файлы) с целью более рационального размещения на диске (или передачи другим пользователям, в том числе по каналам связи).



Словарь терминов

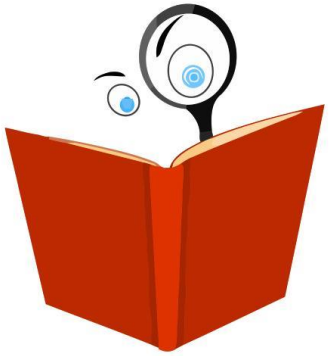
Компьютерный вирус – это специально написанная программа, как правило, небольшая по размерам, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области дисков и в вычислительные сети (причем эти копии сохраняют способность к размножению) с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе на компьютере.



Словарь терминов

Полиморфный вирус – это меняющийся зашифрованный вирус, который постоянно мутирует, избегая таким путем антивирусных сканеров, опознающих вирусы по так называемой сигнатуре – неизменному фрагменту кода.

Стелс-вирус – вирус, использующий специальные приемы, чтобы скрыться от антивирусных программ (например, он может временно выгружаться из памяти).



Словарь терминов

Программы-ловушки – это резидентные программные модули, обеспечивающие после их запуска легального или несанкционированного (скрытного внедрения) съем информации с одного или нескольких информационных внутренних или внешних каналов информационной системы, компьютера или доступной части сети, например, путем перехвата соответствующих прерываний. По способу доставки и внедрения программы– ловушки можно разделить на вирусные, сетевые или файловые.

Литература и Internet-источники

- Симонович С.В. Информатика. Базовый курс: Учебник для вузов. Стандарт третьего поколения. – СПб.: Питер, 2015. – 640 с.
- Хлебников А.А. Информационные технологии: учебник. – М.: КНОРУС, 2014. – 472 с.
- Острейковский В.А. Информатика: Учеб. для вузов. – М.: Высшая школа, 2001. – 511 с.
- https://ru.wikipedia.org/wiki/
- http://lms.tpu.ru/mod/glossary/view.php?id=11172 (Глоссарий по ИТ)
- http://www.zonazakona.ru/articles/index.php?a=18 (Компьютерные преступления)

Литература и Internet-источники

- http://www.ceae.ru/urids-komp-prestup.htm (Компьютерные преступления в УК РФ)
- http://www.kaspersky.com/
- http://www.kaspersky.ru/
- https://sites.google.com/site/antivirusnyeprogrammyivirusy/home/komputernye (Антивирусные программы и вирусы)
- http://studopedia.ru/9_120867_sredstva-informatsionnogo-vozdeystviya-i-ih-priznaki.html (Средства информационного воздействия и их признаки)
- http://www.plam.ru/compinet/osnovy_informatiki_uchebnik_dlja_vuzov/index.php