Лекция № 11.

Компьютерная безопасность и защита информации

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.

1. Необходимость защиты информации

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

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

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

Можно указать, как минимум, две 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.

Существует достаточно много возможных направлений *утечки информации* и путей *несанкционированного доступа* в вычислительных системах и сетях. В их числе:

- 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[1];
- использование недостатков операционной системы;
- незаконное подключение к аппаратуре и линиям связи;
- злоумышленный вывод из строя механизмов защиты;
- внедрение и использование компьютерных вирусов.

Угрозы безопасности информации возникают и при использовании электронной почты. К ним относятся:

[1] **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.

- Адреса электронной почты используются для рассылки спама[2]. Адрес попадает в базы данных спамеров незаконным путем.
- Адреса электронной почты в Интернете легко подделать. Практически нельзя сказать наверняка, кто написал и послал электронное письмо.
- Электронные письма могут быть легко модифицированы. Стандартное SMTP[3]-письмо не содержит средств проверки целостности.
- Существует ряд мест, где содержимое письма может быть прочитано теми, кому оно не предназначено. Электронное письмо скорее похоже на открытку — его могут прочитать на каждой промежуточной станции.
- Нет гарантий доставки электронного письма. Хотя некоторые почтовые системы предоставляют пользователям возможность получить сообщение о доставке, часто такие уведомления означают лишь то, что почтовый сервер получателя (а не обязательно сам пользователь) получил сообщение.
- 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.

Обеспечение безопасности информации при работе на автономно работающих компьютерах и в сетях достигается комплексом организационных, технических и программных мер.

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).

2. Методы защиты информации

Рассмотрим основные методы защиты информации.

Ограничение доступа к информации

Заключается в создании некоторой физической[4] замкнутой преграды вокруг объекта защиты с организацией контрольного доступа лиц, связанных с объектом защиты по своим функциональным обязанностям, т.е. выделение специальных территорий, специальных

[2] **Спам** (англ. *spam*) — массовая рассылка коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать. Также, название распространяемых материалов. Распространителей спама называют спамерами. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем. Доля спама в мировом почтовом трафике составляет от 60% (2006) до 80% (2011). https://ru.wikipedia.org/wiki/

[3] **SMTP** (англ. *Simple Mail Transfer Protocol* — простой протокол передачи почты) — это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

[4] **Физические средства защиты** – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

зданий и помещений, создание контрольно-пропускного режима. ***Задача подобных средств ограничения доступа*** *– исключить случайный и преднамеренный доступ посторонних лиц к комплексам средств автоматизации*. Ограничение доступа к информации обеспечивается и с помощью аппаратных средств с самым различными принципами действия. Так, в целях контроля доступа к внутренним линиям связи и технологическим органам управления используется аппаратура контроля вскрытия устройств.

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.*

Для ограничения и распределения доступа к информации используется **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).

В вычислительной системе объектами идентификации являются:

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

В качестве идентификаторов личности для реализации разграничения широко распространено применение *паролей*, которые записываются на специальные носители (*электронные ключи*[5] или *карточки*). Установление подлинности объекта может производиться человеком, аппаратным устройством, программой, вычислительной системой и т.д.

Криптографическое преобразование информации

Этот метод повышает безопасность передачи данных в сетях ЭВМ, данных в удаленных устройствах памяти и при обмене информацией между удаленными объектами. Защита информации методом *криптографического преобразования*[6] заключается в преобразовании ее составных частей (слов, букв, цифр, слогов) с помощью специальных алгоритмов и аппаратных решений. 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. Без знания ключа эта процедура может быть практически невыполнима даже при известном алгоритме шифрования. Для ознакомления с зашифрованной информацией применяется процесс *декодирования* информации. Появление и развитие электронных элементов позволили разработать недорогие устройства, обеспечивающие преобразование информации.

---

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

[6] **Криптографические средства** – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

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.*

Законодательство Российской Федерации о защите информации основывается на следующих документах[7]:

- 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)
- 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%09Закон%20Российской%20Федерации%20%22О%20безопасности%22%2C%20;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=8521226262032807832405277013839
- 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%09Закон%20Российской%20Федерации%20%ABО%20связи%BB%2C%20;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=19079156120328010693972 98163074
- 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=203280.4215520629922298;SRDSMODE=QSP_GENERAL;SEARCHPLUS=%uF0A7%09Закон%20%ABО%20государственной%20тайне%BB%2C%20;EXCL=PBUN%2CQSBO%2CKRBO%2CPKBO;SRD=true;ts=196733561720328024256922892650912

и других актов законодательства, регулирующих отношения, связанные с мерами защиты 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);

[7] Тексты документов см. в некоммерческая интернет-версия Консультант-плюс http://base.consultant.ru/cons/cgi/online.cgi?req=home;rnd=0.7350532797501188

- Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ).

Выбор конкретных средств защиты зависит от требований, предъявляемых к защите информации, ее целостности, важности, сроков хранения и др.

Большинство современных компьютеров обеспечивает возможность использования пароля для защиты от несанкционированного доступа. Такая парольная защита может быть реализована как на аппаратном, так и на программном уровне. В ряде случаев без ввода пароля загрузить операционную систему и сделать доступным жесткие диски с данными практически невозможно для обычного пользователя и может быть весьма сложным делом для профессионала, особенно при отсутствии времени. В качестве первого уровня защиты можно пользоваться этим.

Более эффективную защиту обеспечивают специализированные программы или аппаратные средства, созданные и служащие исключительно в целях предотвращения несанкционированного доступа. Так, существуют специальные платы, встраиваемые в компьютер.

Достаточно надежными и простыми могут быть для пользователя программные средства. На сегодняшний день существует множество систем, осуществляющих защиту информации, хранящейся на компьютере, программным способом: с помощью шифрования, кодирования и т.д. Степень их реальной защиты в каждом случае различна. Многие программные системы защиты способны уберечь только от пользователя среднего уровня, но не профессионала. Дело в том, что в определенных секторах жесткого диска хранится служебная информация, содержащая некоторые сервисные сведения. Такие сектора недоступны для записи обычных файлов, но ряд защитных программ пользуются этой частью диска. При некотором умении и наличии специальных программных средств к ней можно легко получить доступ, например, загрузившись с системного диска, а затем внести определенные изменения и т.д., которые позволят обойти защиту и открыть доступ к хранящейся на диске информации.

Другой, еще более простой возможностью создания пользовательской защиты является «закрытие» конкретных документов штатными средствами программ, в которых они создаются. Так, ряд продуктов пакета Microsoft Office предлагает для этих целей собственные возможности защиты на уровне отдельных файлов. Например, работая в Word, можно защитить документ, установив пароль. Паролем может служить комбинация букв, цифр, символов и пробелов. Следует отметить, что регистр букв (прописные или строчные) также имеет значение. Защищенный документ невозможно будет открыть без правильного ввода пароля. Аналогичная возможность существует и в Excel. Здесь также можно защитить файл паролем или объявить его файлом только для чтения без возможности внесения изменений.

3. Компьютерные вирусы

При работе с современным персональным компьютером пользователя может подстерегать множество неприятностей: потеря данных, «зависание» системы, выход из строя отдельных частей компьютера и др. Одной из причин этих проблем наряду с ошибками в программном обеспечении и неумелыми действиями оператора ПК могут быть проникшие в систему *компьютерные вирусы*. Это едва ли не главные враги компьютера, которые подобно биологическим вирусам размножаются, записываясь в системные области диска

или присоединяясь к файлам, и производят различные нежелательные действия, которые зачастую имеют катастрофические последствия.

Причины появления распространения компьютерных вирусов, с одной стороны, скрываются в теневых сторонах человеческой личности (зависть, месть, тщеславие), с другой стороны, обусловлены отсутствием аппаратных средств защиты и противодействия со стороны операционной системы ПК.

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.

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**.

Основными путями проникновения вирусов в компьютер являются съемные носители информации (диски и флэш-карты), а также компьютерные сети. Заражение жесткого диска вирусом может произойти при загрузке компьютера с диска, содержащего вирус. Такое заражение может быть и случайным, например, если системную дискету не вынули из дисковода и перезагрузили компьютер. Заразить дискету гораздо проще – вирус может попасть на нее, даже если дискету просто вставили в дисковод зараженного компьютера и просмотрели ее содержимое. **Зараженный диск** – это диск, в загрузочном секторе которого находится вирус.

После запуска программы, содержащей вирус, становится возможным заражение других файлов. **Зараженный файл** – это файл, содержащий внедренный в него вирус.

При заражении компьютера вирусом очень важно своевременно его обнаружить, так как действия вирусов могут наносить большой вред владельцам компьютеров. Приведем основные 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;
- 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.

Перечисленные признаки необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому иногда затруднена правильная диагностика состояния компьютера.

Сегодня известно огромное количество вирусов. Так, в антивирусных базах «Касперского» содержится более 6,5 млн. записей (на начало 2012 г.). Как и обычным вирусам, для размножения компьютерным вирусам нужен **носитель** – здоровая программа или документ, в котором они прячут участки своего программного кода.

Сам вирус невелик, редко его размер измеряется килобайтами. В тот момент, когда пользователь запускает на своем компьютере программу или открывает документ, вирус активизируется и заставляет компьютер следовать его инструкциям. Это приводит к удалению какой-либо информации, причем чаще всего безвозвратно. Современные вирусы могут испортить не только программы, но и «железо». Например, уничтожают содержимое BIOS материнской платы или повреждают жесткий диск.

Вирусы появились более 40 лет назад. Именно тогда, в конце 1960-х гг., когда о ПК можно было читать лишь в фантастических романах, в нескольких больших ЭВМ, располагавшихся в крупных исследовательских центрах США, обнаружились очень необычные программы. Они не выполняли распоряжения человека, как другие программы, а действовали сами по себе. Причем своими действиями они сильно замедляли работу компьютера, но при этом ничего не портили и не размножались.

В 1970-х гг. были зарегистрированы первые вирусы, способные к размножению и получившие собственные имена. Так, большой компьютер Univac 1108 «заболел» вирусом Pervading Animal, а компьютеры семейства IBM-360/370 были заражены вирусом Christmas Tree.

В 1980-х годах число активных вирусов измерялось уже сотнями. А появление и распространение ПК породило настоящую эпидемию – счет вирусов пошел на тысячи. Правда, термин «компьютерный вирус» появился только в 1984 г. (впервые его использовал в своем докладе на конференции по информационной безопасности сотрудник Лехайского университета США Ф. Коуэн).

Первые компьютерные вирусы были простыми и неприхотливыми, не скрывались от пользователей и скрашивали свое разрушительное действие (удаление файлов, разрушение логической структуры дисков) выводимыми на экран картинками и шутками («Назовите точную высоту горы Килиманджаро в миллиметрах! При введении неправильного ответа все данные на вашем винчестере будут уничтожены!»). Выявить такие вирусы было нетрудно, так как они присоединялись к исполняемым (.exe, .com) файлам, изменяя их оригинальные размеры.

Позднее вирусы стали прятать свой программный код так, что ни один антивирус не мог его обнаружить. Такие вирусы назывались *невидимками*.

В 1990-х годах вирусы стали мутировать, т.е. постоянно изменять свой программный код, при этом пряча его в различных участках жесткого диска. Такие вирусы-мутанты стали называть *полиморфными*.

В 1995 году после появления операционной системы Windows 95 были зарегистрированы вирусы, работающие под управлением Windows. Примерно через полгода были обнаружены вирусы, которые действовали в документах, подготовленных в программах пакета Microsoft Office. Долгое время заражение вирусами файлов документов считалось невозможным, так как документы не содержали исполнимых программ. Однако программисты корпорации Microsoft встроили в текстовый процессор Word и табличный процессор Excel язык программирования VBA, предназначенный для создания специальных до-

полнений к процессорам (**макросов**). Эти макросы сохранялись в теле документов Microsoft Office и легко могли быть заменены вирусами. После открытия зараженного файла вирус активизировался и заражал все документы пакета. Первоначально макровирусы наносили вред только текстовым документам, позднее стали уничтожать информацию.

Весомый вклад в распространение вирусов внесла сеть Интернет. Впервые внимание общественности к проблеме интернет-вирусов было привлечено после появления знаменитого «червя Морриса»[8], распространившегося по всей мировой сети. А к 1998 году Интернет стал главным поставщиком вирусов. Возник даже целый класс интернет-вирусов, названных *троянскими*. Поначалу эти программы не причиняли вреда компьютеру и хранящейся в нем информации, зато с легкостью могли украсть логин и пароль для доступа к сети, а также другую секретную информацию.

В течение 1998-1999 гг. мир потрясли несколько разрушительных вирусных атак – в результате деятельности вирусов Chernobyl, Melissa и Win95.CIH были выведены из строя около миллиона компьютеров во всех странах мира (вирусы портили жесткий диск и уничтожали BIOS материнской платы).

Для защиты от компьютерных вирусов следует соблюдать основные правила работы на ПК:

- 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;
- 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).

4. Классификация компьютерных вирусов

В основе классификации компьютерных вирусов лежат четыре признака.

По разрушительным возможностям выделяют три вида вирусов:

[8] **Червь Морриса** (англ. *Morris worm*) или **интернет-червь 2 ноября 1988** (англ. *Internet worm of November 2, 1988*) — один из первых сетевых червей, распространяемых через Интернет. Написан аспирантом Корнелльского университета Робертом Таппаном Моррисом, и запущен 2 ноября 1988 года в Массачусетском технологическом институте. Это был первый вирус (парализовал работу шести тысяч интернет-узлов в США), получивший значительное внимание в средствах массовой информации. Он привёл к первой судимости в США по Computer Fraud and Abuse Act 1986 года.

- **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.

По способу заражения выделяют два вида вирусов:

- **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.

По среде обитания выделяют четыре вида вирусов:

- **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;
- **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;
- **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»;
- **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.

По особенностям алгоритма выделяют семь видов вирусов:

- **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);

- **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;
- **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;
- **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;
- **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;
- **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).

Отдельно стоит выделить **студенческие вирусы** – элементарные вирусы, созданные ради забавы студентами, которые только научились программировать и решили попробовать свои силы. Но есть и исключения, например, написанный студентом вирус Chernobyl.

Четкого разделения между типами вирусов не существует, и все они могут составлять комбинацию вариантов взаимодействия, т.е. своеобразный «вирусный коктейль».

Вирус является программой, поэтому объекты, не содержащие программ и не подлежащие преобразованию в программы, не могут быть заражены вирусом (исключение составляют документы, поддерживающие макросы). К числу таких объектов относятся текстовые файлы (кроме командных файлов и текстов программ), документы не поддерживающие макросы редакторов, информационные файлы баз данных и т.д. Вирус может только испортить такие объекты, но не заразить их.

5. Антивирусные программы

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.

Количество и разнообразие вирусов очень велико, поэтому, чтобы быстро и эффективно их обнаружить, антивирусная программа должна отвечать определенным требованиям:

- *Стабильность и надежность работы* является определяющими параметрами, так как даже самый лучший антивирус окажется совершенно бесполезным, если он не сможет нормально функционировать на компьютере, например, в результате какого-либо сбоя в работе программ процесс проверки компьютера не пройдет до конца. Тогда всегда есть вероятность того, что какие-то зараженные файлы остались незамеченными;
- *Объем вирусной базы* (количество обнаруживаемых программой вирусов). С учетом постоянного появления новых вирусов база должна регулярно обновляться.
- *Скорость работы программы* является одним из основных требований к любой антивирусной программе, так как огромный поток информации требует быстрой проверки файлов и дисков компьютера;
- *Наличие дополнительных возможностей*, например, алгоритмов определения неизвестных программе вирусов (эвристическое сканирование). Сюда же следует отнести умение работать с файлами различных типов (архивы, документы) и возможность восстанавливать зараженные файлы, не стирая их с жесткого диска, а только удалив из них вирусы. Немаловажным является 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).

Антивирусные программы выпускает ряд компаний. К наиболее распространенным относят следующие программы:

KASPERSKY SECURITY	Антивирус Касперского, Kaspersky Anti-Virus (производитель «Лаборатория Касперского», с 1994 г.), лицензия – коммерческая
	Dr. Web (производитель «Диалог-Наука», с 1994 г.) Лицензия: Shareware
McAfee	McAfee VirusScan (производитель Symantec).
AVIRA	Avira (производитель Avira GmbH & Co. KG, с 1986 г.)
AVG	AVG Anti-Virus (разработчик AVG Techologies), лицензия – проприетарная
	АНТИВИРУС ESET NOD32 (разработчик ESET, лицензия – проприетарная)

	Avast! (разработчик AVAST Software, лицензия – условно-бесплатная)

Разнообразие существующих антивирусных программ привело к необходимости их классифицировать в зависимости от принципов работ. Выделяют пять групп подобных программ:

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).

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.

Постоянное появление новых вирусов приводит к быстрому устареванию детекторов и докторов поэтому требуется регулярное обновление их версий.

Фильтры (сторожа)

Фильтры (сторожа) представляют собой 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.

При попытке какой-либо программы произвести указанные действия сторож посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не лечат файлы и диски. Для уничтожения вирусов требуется применять другие программы, например, фаги. К недостаткам сторожей можно отнести существенное замедление работы компьютера, так как они отслеживают любые действия компьютера, перехватывая все запросы к операционной системе на выполнение «подозрительных» действий.

Ревизоры (инспекторы)

Ревизоры 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 срав-

нении проверяются состояние загрузочного сектора и таблицы размещения файлов, длина, дата и время модификации файлов, контрольная сумма файла[9] и другие параметры.

Ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут отличить изменения версии проверяемой программы от изменений, внесенных вирусом.

Вакцинаторы (имунизаторы)

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. В настоящее время вакцины редко применяются, так как имеют ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

Наиболее распространены программы доктора и фильтры. А современные антивирусные пакеты включают все необходимые компоненты для противостояния любым вирусам. Например, «Антивирус Касперского» (Kaspersky Anti-Virus) содержит программу-фильтр Kaspersky Anti-Virus Monitor, доктор Kaspersky Anti-virus Scanner и ревизор Kaspersky Anti-Virus Inspector.

Несмотря на широкую распространенность антивирусных программ, вирусы продолжают «плодиться». Чтобы справиться с ними, необходимо создавать более универсальные и качественно-новые антивирусные программы, которые будут включать в себя все положительные качества своих предшественников. Защищенность от вирусов зависит и от грамотности пользователей.

6. Профилактика почтовых вирусов

В настоящее время электронная почта является наиболее популярным средством для распространения компьютерных вирусов. Но надо учитывать, что заражение вирусами этой категории происходит не в результате поступления почтового сообщения, а наступает в результате некорректных действий пользователя при просмотре вредоносного сообщения и связано с наличием ошибок и уязвимостей в почтовых программах и операционных системах. К мерам профилактики почтовых вирусов относятся следующие мероприятия:

- 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.

[9] **Контро́льная су́мма** — некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении.

7. 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).

Сжатие информации в архивных файлах производится за счет устранения избыточности различными способами, например, за счет упрощения кодов, исключения из них постоянных битов или представления повторяющихся символов в виде коэффициентов повторения соответствующих символов. Алгоритмы подобного сжатия информации реализованы в специальных программах – **архиваторах.**

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

В отличие от программ резервного копирования архиваторы позволяют сжимать информацию в памяти компьютера с помощью специальных математических методов. При этом создается копия файла меньшего размера, что дает возможность разместить на диске больше информации. Кроме того, в одном архиве может храниться сразу несколько различных объектов (файлов и/или папок).

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).

В файловой системе компьютера каждый архив имеет строго заданный тип (расширение). Наиболее часто встречаются следующие архивные файлы: .zip, rar, .cab, .arj и др. Для каждого из них существуют свои архиваторы (Zip, Rar, Arj и др.), но существуют и универсальные программы, работающие со многими типами архивов (например, WinRar).

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.

Существуют два показателя, характеризующих эффективность работы любого архиватора:

- *Коэффициент сжатия*, отражающий отношение размера архивного (сжатого) файла к исходному;
- *Коэффициент уменьшения*, показывающий, во сколько раз архивный файл меньше исходного.

Кроме используемой программы (со своим методом сжатия) степень сжатия также зависит и от типа исходного файла. Наиболее хорошо сжимаются графические и текстовые файлы (коэффициент сжатия может достигать 5-40%), меньше сжимаются файлы ис-

полняемых программ (коэффициент сжатия 60-90%), а архивные файлы практически не сжимаются.

Сегодня фактор совместимости более важен, так как по достигаемой степени сжатия конкурирующие архивные форматы различаются лишь на проценты (а не разы), а вычислительная мощность современных компьютеров делает время обработки архивов не столь существенным показателем, как раньше. Поэтому при выборе инструмента для работы с архивами важнейшим критерием для большинства пользователей (тех, для кого обмен большими массивами данных представляет насущную проблему) является способность программы «понимать» наиболее распространенные архивные форматы. В России наиболее распространены два формата .zip и .rar.

В настоящее время существует несколько десятков архиваторов, которые отличаются перечнем функций и параметрами работы, однако лучшие из них имеют примерно одинаковые характеристики (например, WinRar и WinZip, которые работают в среде Windows, имеют удобный интерфейс и множество сервисных функций).

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

Потребность в архивации связана с необходимостью копирования данных на диски с целью сохранения ценной информации и программного обеспечения компьютера для защиты от повреждения и уничтожения. Однако следует учитывать, что архивация зараженного вирусом файла не избавляет файл (компьютер) от вируса, но и способствует его дальнейшему распространению.

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. Защиту информации от компьютерных вирусов обеспечивает использование антивирусного программного обеспечения.

Для создания копий информации используются программы резервного копирования и архиваторы.

Использованная и рекомендуемая литература и Internet-источники

1. Симонович С.В. Информатика. Базовый курс: Учебник для вузов. Стандарт третьего поколения. – СПб.: Питер, 2015. – 640 с.
2. Острейковский В.А. Информатика: Учеб. для вузов. – М.: Высшая школа, 2001. – 511 с.
3. Хлебников А.А. Информационные технологии: учебник. – М.: КНОРУС, 2014. – 472 с.
4. https://ru.wikipedia.org/wiki/
5. http://www.zonazakona.ru/articles/index.php?a=18 (Компьютерные преступления)
6. http://www.ceae.ru/urids-komp-prestup.htm (Компьютерные преступления в УК РФ)
7. http://www.kaspersky.com/
8. http://www.kaspersky.ru/
9. https://sites.google.com/site/antivirusnyeprogrammyivirusy/home/komputernye (Антивирусные программы и вирусы)
10. http://studopedia.ru/9_120867_sredstva-informatsionnogo-vozdeystviya-i-ih-priznaki.html (Средства информационного воздействия и их признаки)
11. http://www.plam.ru/compinet/osnovy_informatiki_uchebnik_dlja_vuzov/index.php

Контрольные вопросы

1. Дайте определение понятия «информационная безопасность» (ИБ).
2. Какие вам известны угрозы безопасности информации?
3. Какие вам известны источник угроз безопасности информации?
4. Дайте классификацию вирусов.
5. Основные свойства вирусов.
6. Основные пути заражения вирусами.
7. Какие законодательные акты Российской Федерации регулируют правовые отношения в сфере информационной безопасности (ИБ)?
8. Какие виды ответственности предусматриваются за нарушения в сфере ИБ?
9. Перечислите программно-технические меры обеспечения ИБ?
10. Способы обеспечения сохранения и безопасного восстановления информации.
11. Что такое антивирусная защита?
12. Классификация программных средств антивирусной защиты.
13. Примеры антивирусных программ.

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.

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).

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.

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

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.

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