Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тверской государственный университет»

Факультет прикладной математики и кибернетики
Направление «Фундаментальная информатика и информационные технологии»

Курсовая работа
по дисциплине
«Системы специального назначения»

Тема: «Основные направления и методология обеспечения компьютерной безопасности.»

Выполнила:

студентка 36 группы
Демьянова Виктория Вадимовна

Проверил:

Гончаров Сергей Николаевич

Тверь - 2017

Оглавление:

1. Введение

На сегодняшний день вопрос о компьютерной безопасности возникает особо часто. Этот вопрос гораздо более серьезен, чем может показаться несведущему человеку на первый взгляд и касается не только владельцев бизнесов, использующих большие системы из десятков и сотен компьютеров и беспокоящихся о сохранении коммерческой тайны, но и домашних пользователей даже одного компьютера, периодически выходящего с него в Интернет.

В чем же заключается уязвимость компьютерной системы? В самых общих чертах - это возможность злоумышленника тем или иным образом использовать ресурсы компьютера, а также украсть или изменить информацию, содержащуюся на компьютере. И даже если вы никогда никому не платили с помощью компьютера, не подключались к своему банковскому счету и не посылали электронных писем, содержимое которых вы бы хотели сохранить в тайне, информация, например, о том, какие именно WEB сайты и в какое время вы посещали, может вам навредить.

В настоящее время все большее значение приобретает обеспечение компьютерной безопасности. Это связано с возрастающим объемом поступающей информации, совершенствованием средств ее хранения, передачи и обработки. Перевод значительной части информации в электронную форму, использование локальных и глобальных сетей создают качественно новые угрозы конфиденциальной информации.

Компьютерные преступления в рассматриваемом аспекте можно охарактеризовать как противоправные посягательства на экономическую безопасность предпринимательства, в которых объектом либо орудием преступления является компьютер.

2. Основные угрозы компьютерной безопасности

Что является непосредственным объектом компьютерных преступлений? Им может являться как информация (данные), так и сами компьютерные программы.

Преступник получает доступ к охраняемой информации без разрешения ее собственника или владельца либо с нарушением установленного порядка доступа. Способы такого неправомерного доступа к компьютерной информации могут быть различными: кража носителя информации, нарушение средств защиты информации, использование чужого имени, изменение кода или адреса технического устройства, представление фиктивных документов на право доступа к информации, установка аппаратуры записи, подключаемой к каналам передачи данных. Причем доступ может быть осуществлен в помещениях фирмы, где хранятся носители, из компьютера на рабочем месте, из локальной сети, из глобальной сети.

Таким образом, обеспечение безопасности информации в КС должно предусматривать защиту всех компонент от внешних и внутренних воздействий (угроз).

Под угрозой безопасности информации понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса.

Первый класс: угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют случайными или непреднамеренными.

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным - до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для КС, т.к. последние подвергаются физическому

разрушению, информация утрачивается или доступ к ней становится невозможен.

Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы отдельных узлов и устройств могут также привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее устройство и т.п.

Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты информации.

Согласно данным Национального Института Стандартов и Технологий США (NIST) 65% случаев нарушения безопасности информации происходит в результате ошибок пользователей и обслуживающего персонала. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводит к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Характеризуя угрозы информации в КС, не связанные с преднамеренными действиями, в целом, следует отметить, что механизм их реализации изучен достаточно хорошо, накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффективная система эксплуатации КС, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

Второй класс угроз безопасности информации в КС составляют преднамеренно создаваемые угрозы.

Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами. Угрозы этого класса в соответствии с их

физической сущностью и механизмами реализации могут быть распределены по пяти группам:

- традиционный или универсальный шпионаж и диверсии;
- несанкционированный доступ к информации;
- электромагнитные излучения и наводки;
- модификация структур КС;
- вредительские программы.

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсии, которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих КС. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов.

3. Основные направления обеспечения компьютерной безопасности

Обеспечение безопасности деятельности со стороны компьютерных систем представляет собой один из блоков проблемы безопасности вообще. Защита от компьютерных преступлений должна начинаться с разработки концепции информационной безопасности фирмы. На основе вышеназванных принципов — вероятности угрозы, возможности защиты и экономической целесообразности защиты информации разрабатываются конкретные способы зашиты.

Способы защиты можно разделить на три группы: правовые, организационные и технические.

Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

К основным организационным мероприятиям можно отнести:

- организацию режима и охраны. Их цель: исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.;
- организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;
- организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
- организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Организационные способы связаны с ограничением возможного несанкционированного физического доступа к компьютерным системам. Они основаны на принципах управления коллективом и предприятием (службой) и принципах законности. Основные направления организационной зашиты компьютерной системы включают:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- мероприятия, осуществляемые при подборе и подготовке персонала системы;
- организацию охраны и надежного пропускного режима;
- организацию учета, хранения, использования и уничтожения документов и носителей с информацией;
- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- организацию явного и скрытого контроля за работой пользователей;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

Организационные способы защиты необходимы для обеспечения эффективного применения других направлений и средств защиты в части, касающейся регламентации действий людей. В то же время, организационные способы защиты необходимо поддерживать более надежными физическими и техническими и всеми другими средствами. В связи с этим в системе организационного обеспечения компьютерной безопасности выделяют два направления:

- направление, связанное с реализацией, мер организационно-правового характера;
- направление, связанное с реализацией мер организационно-технического характера.

Первое направлено на реализацию правовых методов защиты информации и поддержание правового режима обработки информации. Второе

направлено на поддержание правового режима обработки информации методами инженерно-технической защиты.

Техническая защита – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

По функциональному назначению средства технической защиты делятся на следующие группы:

- физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий. К физическим средствам относятся механические, электромеханические электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещение несанкционированного доступа (входа выхода) проноса (выноса) средств и материалов, и других возможных видов преступных действий;
- аппаратные средства. Сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача аппаратных средств – обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности;
- программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных;
- 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.

Технические способы предполагают использование средств программно-технического характера, направленных, прежде всего, на ограничение доступа пользователя, работающего с компьютерными системами фирмы, к той информации, обращаться к которой он не имеет права.

Специалисты-практики выделяют следующие основные направления технической защиты компьютерной системы:

- защита информационных ресурсов от несанкционированного доступа и использования — используются средства контроля включения питания и загрузки программного обеспечения, а также методы парольной защиты при входе в систему;
- защита от утечки по побочным каналам электромагнитных излучений и наводок — с помощью экранирования аппаратуры, помещений, применением маскирующих генераторов шумов, дополнительной проверкой аппаратуры на наличие компрометирующих излучений;
- защита информации в каналах связи и узлах коммутации — используются процедуры аутентификации абонентов и сообщений, шифрование и специальные протоколы связи;
- защита юридической значимости электронных документов — при доверительных отношениях двух субъектов предпринимательской деятельности, когда возникает необходимость передачи документов (платежных поручений, контрактов) по компьютерным сетям — для определения истинности отправителя документ дополняется «цифровой подписью» — специальной меткой, неразрывно логически связанной с текстом и формируемой с помощью секретного криптографического ключа;
- защита автоматизированных систем от компьютерных вирусов и незаконной модификации — применяются иммуностойкие программы и механизмы модификации фактов программного обеспечения.

Правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе. Современные условия требуют и определяют необходимость комплексного подхода к формированию законодательства по защите информации, его состава и содержания, соотнесения его со всей системой законов и правовых актов РФ.

Выделяется следующая структура правовых актов, ориентированных на правовую защиту информации:

- первый блок – конституционное законодательство. Нормы, касающиеся вопросов информатизации и защиты информации, входят в него как составные элементы;
- второй блок – общие законы, кодексы (о собственности, о недрах, о земле, о правах граждан, о гражданстве, о налогах, об антимонопольной деятельности), которые включают нормы по вопросам информатизации и информационной безопасности;
- третий блок – законы об организации управления, касающиеся отдельных структур хозяйства, экономики, системы государственных

органов и определяющие их статус. Они включают отдельные нормы по вопросам защиты информации;

- четвертый блок – специальные законы, полностью относящиеся к конкретным сферам отношений отраслям хозяйства, процессам. В их число входит и Закон РФ «Об информации, информатизации и защите информации»;
- пятый блок – законодательство субъектов РФ, касающееся защиты информации;
- шестой блок – подзаконные нормативные акты по защите информации;
- седьмой блок – это правоохранительное законодательство России, содержащее нормы об ответственности за правонарушения в сфере информатизации.

Специальное законодательство в области безопасности информационной деятельности может быть представлено совокупностью законов. В их составе особое место принадлежит базовому Закону «Об информации, информатизации и защите информации», который закладывает основы правового определения всех важнейших компонентов информационной деятельности.

Настоящий Федеральный закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Действенным способом ограничения несанкционированного доступа к компьютерным системам является также регулярная смена паролей, особенно при увольнении работников, обладающих информацией о способах защиты.

4. Методология обеспечения компьютерной безопасности

Защита информации в компьютерной системе – комплекс методов, предотвращающих или снижающих возможность образования каналов утечки информации и/или каналов воздействия на компьютерную систему.

Канал утечки информации – состоит из источника информации, канала распространения информации от источника и средства извлечения информации из этого канала. Канал утечки информации связан с пассивным воздействием (с использованием телекоммуникационных каналов передачи информации, либо с использованием технических каналов утечки информации) злоумышленника на объект. Через канал утечки реализуется угроза конфиденциальности информации в компьютерной системе.

4.1 Угрозы безопасности информации в компьютерных системах

Под угрозой безопасности информации понимается потенциально возможное событие, процесс или явление, которое может привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Всё множество потенциальных угроз безопасности информации в автоматизированных информационных системах (АИС) или в компьютерных системах (КС) может быть разделено на два класса: случайные угрозы и преднамеренные угрозы.

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называются случайными или непреднамеренными.

К случайным угрозам относятся: стихийные бедствия и аварии, сбои и отказы технических средств, ошибки при разработке АИС или КС, алгоритмические и программные ошибки, ошибки пользователей и обслуживающего персонала.

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным – до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом может происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию. Согласно тем же, статистическим данным только в результате ошибок пользователей и обслуживающего персонала происходит до 65% случаев нарушения безопасности информации.

Следует отметить, что механизм реализации случайных угроз изучен достаточно хорошо и накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных

средств, эффективная система эксплуатации автоматизированных информационных систем, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

Угрозы, которые связаны со злоумышленными действиями людей, а эти действия носят не просто случайный характер, а, как правило, являются непредсказуемыми, называются преднамеренными.

К преднамеренным угрозам относятся: традиционный или универсальный шпионаж и диверсии, несанкционированный доступ к информации, электромагнитные излучения и наводки, несанкционированная модификация структур, вредительские программы.

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсий. К методам шпионажа и диверсий относятся: подслушивание, визуальное наблюдение, хищение документов и машинных носителей информации, хищение программ и атрибутов систем защиты, подкуп и шантаж сотрудников, сбор и анализ отходов машинных носителей информации, поджоги, взрывы, вооруженные нападения диверсионных или террористических групп.

Несанкционированный доступ к информации – это нарушение правил разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем. Несанкционированный доступ возможен:

- при отсутствии системы разграничения доступа;
- при сбое или отказе в компьютерных системах;
- при ошибочных действиях пользователей или обслуживающего персонала компьютерных систем;
- при ошибках в системе распределения доступа;
- при фальсификации полномочий.

Процесс обработки и передачи информации техническими средствами компьютерных систем сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках. Всё это получило название:” побочные электромагнитные излучения и наводки” (ПЭМИН). Электромагнитные излучения и наводки могут быть использованы злоумышленниками, как для получения информации, так и для её уничтожения.

Большую угрозу безопасности информации в компьютерных системах представляет несанкционированная модификация алгоритмической, программной и технической структуры системы.

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших название “вредительские программы”.

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- “логические бомбы”;
- “черви”;
- “троянские кони”;
- “компьютерные вирусы”.

Логические бомбы – это программы или их части, постоянно находящиеся в ЭВМ или вычислительных систем (КС) и выполняемые только при соблюдении определённых условий. Примерами таких условий могут быть: наступление заданной даты, переход КС в определённый режим работы, наступление некоторых событий заданное число раз и тому подобное.

Черви – это программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в вычислительных системах (ВС) или в сети и само воспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и блокировке системы.

Троянские кони – это программы, полученные путём явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

Компьютерные вирусы – это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путём создания своих копий, а при выполнении определённых условий оказывают негативное воздействие на КС.

Базовая система защиты информации создается на основе использования правовых, технических, организационных и программных методов, соотношение между которыми выбирается для конкретной компьютерной сети исходя их целей функционирования сети и возможных угроз.

Защита информации в компьютерных системах обеспечивается созданием комплексной системы защиты. Комплексная система защиты включает:

- правовые методы защиты;
- организационные методы защиты;
- методы защиты от случайных угроз;
- методы защиты от традиционного шпионажа и диверсий;

- методы защиты от электромагнитных излучений и наводок;
- методы защиты от несанкционированного доступа;
- криптографические методы защиты;
- методы защиты от компьютерных вирусов.

К правовым методам относятся:

- разработка законодательных норм, устанавливающих ответственность за совершение компьютерных преступлений;
- совершенствование уголовного и гражданского законодательства в области информационных технологий;
- защита авторских прав сетевых публикаций и т.п.

К организационным методам относятся:

- выработка плана мероприятий по мерам безопасности локальной сети и каналов связи;
- организация охраны компьютерных систем;
- подбор персонала и организация системы доступа;
- исключение случаев ведения дела одним специалистом;
- формирование правил разграничения доступа;
- оформление документов, регулирующих ответственность лиц по обеспечению безопасности и т.п.

Среди методов защиты имеются и универсальные, которые являются базовыми при создании любой системы защиты. Это, прежде всего, правовые методы защиты информации, которые служат основой легитимного построения и использования системы защиты любого назначения. К числу универсальных методов можно отнести и организационные методы, которые используются в любой системе защиты без исключений и, как правило, обеспечивают защиту от нескольких угроз.

Методы защиты от случайных угроз разрабатываются и внедряются на этапах проектирования, создания, внедрения и эксплуатации компьютерных систем. К их числу относятся:

- создание высокой надёжности компьютерных систем;
- создание отказоустойчивых компьютерных систем;
- блокировка ошибочных операций;
- оптимизация взаимодействия пользователей и обслуживающего персонала с компьютерной системой;
- минимизация ущерба от аварий и стихийных бедствий;
- дублирование информации.

При защите информации в компьютерных системах от традиционного шпионажа и диверсий используются те же средства и методы защиты, что и

для защиты других объектов, на которых не используются компьютерные системы. К их числу относятся:

- создание системы охраны объекта;
- организация работ с конфиденциальными информационными ресурсами;
- противодействие наблюдению и подслушиванию;
- защита от злоумышленных действий персонала.

Все методы защиты от электромагнитных излучений и наводок можно разделить на пассивные и активные. Пассивные методы обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов. Активные методы защиты направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих приём и выделение полезной информации из перехваченных злоумышленником сигналов. На электронные блоки и магнитные запоминающие устройства могут воздействовать мощные внешние электромагнитные импульсы и высокочастотные излучения. Эти воздействия могут приводить к неисправности электронных блоков и стирать информацию с магнитных носителей информации. Для блокирования угрозы такого воздействия используется экранирование защищаемых средств.

Для защиты информации от несанкционированного доступа создаются:

- система разграничения доступа к информации;
- система защиты от исследования и копирования программных средств.

Исходной информацией для создания системы разграничения доступа является решение администратора компьютерной системы о допуске пользователей к определённым информационным ресурсам. Так как информация в компьютерных системах хранится, обрабатывается и передаётся файлами (частями файлов), то доступ к информации регламентируется на уровне файлов. В базах данных доступ может регламентироваться к отдельным её частям по определённым правилам. При определении полномочий доступа администратор устанавливает операции, которые разрешено выполнять пользователю. Различают следующие операции с файлами:

- чтение (R);
- запись;
- выполнение программ (E).

Операции записи имеют две модификации:

- субъекту доступа может быть дано право осуществлять запись с изменением содержимого файла (W);

- разрешение дописывания в файл без изменения старого содержимого (A).

Система защиты от исследования и копирования программных средств включает следующие методы:

- методы, затрудняющие считывание скопированной информации;
- методы, препятствующие использованию информации.

Под криптографической защитой информации понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий. По виду воздействия на исходную информацию методы криптографического преобразования информации разделяются на следующие группы:

- шифрование;
- стенография;
- кодирование;
- сжатие.

Вредительские программы и, прежде всего, вирусы представляют очень серьёзную опасность для информации в компьютерных системах. Знание механизмов действия вирусов, методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и потерь от их воздействия.

Компьютерные вирусы - это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения в компьютерных системах. Вирусы могут выполнять изменение или уничтожение программного обеспечения или данных, хранящихся в компьютерных системах. В процессе распространения вирусы могут себя модифицировать.

Все компьютерные вирусы классифицируются по следующим признакам:

- по среде обитания;
- по способу заражения;
- по степени опасности вредительских воздействий;
- по алгоритму функционирования.

По среде обитания компьютерные вирусы подразделяются на:

- сетевые;
- файловые;
- загрузочные;
- комбинированные.

Средой обитания сетевых вирусов являются элементы компьютерных сетей. Файловые вирусы размещаются в исполняемых файлах. Загрузочные вирусы находятся в загрузочных секторах внешних запоминающих устройств. Комбинированные вирусы размещаются в нескольких средах обитания. Например, загрузочно-файловые вирусы.

По способу заражения среды обитания компьютерные вирусы делятся на:

- резидентные;
- нерезидентные.

Резидентные вирусы после их активизации полностью или частично перемещаются из среды обитания в оперативную память компьютера. Эти вирусы, используя, как правило, привилегированные режимы работы, разрешённые только операционной системе, заражают среду обитания и при выполнении определённых условий реализуют вредительскую функцию.

Нерезидентные вирусы попадают в оперативную память компьютера только на время их активности, в течение которого выполняют вредительскую функцию и функцию заражения. Затем они полностью покидают оперативную память, оставаясь в среде обитания.

По степени опасности для информационных ресурсов пользователя вирусы разделяются на:

- безвредные;
- опасные;
- очень опасные.

Безвредные вирусы создаются авторами, которые не ставят себе цели нанести какой-либо ущерб ресурсам компьютерной системы. Однако такие вирусы всё-таки наносят определённый ущерб:

- расходуют ресурсы компьютерной системы;
- могут содержать ошибки, вызывающие опасные последствия для информационных ресурсов;
- вирусы, созданные ранее, могут приводить к нарушениям штатного алгоритма работы системы при модернизации операционной системы или аппаратных средств.

Опасные вирусы вызывают существенное снижение эффективности компьютерной системы, но не приводят к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах.

Очень опасные вирусы имеют следующие вредительские воздействия:

- вызывают нарушение конфиденциальности информации;
- уничтожают информацию;

- вызывают необратимую модификацию (в том числе и шифрование) информации;
- блокируют доступ к информации;
- приводят к отказу аппаратных средств;
- наносят ущерб здоровью пользователям.

По алгоритму функционирования вирусы подразделяются на:

- не изменяющие среду обитания при их распространении;
- изменяющие среду обитания при их распространении.

Для борьбы с компьютерными вирусами используются специальные антивирусные средства и методы их применения. Антивирусные средства выполняют следующие задачи:

- обнаружение вирусов в компьютерных системах;
- блокирование работы программ-вирусов;
- устранение последствий воздействия вирусов.

Обнаружение вирусов и блокирование работы программ-вирусов осуществляется следующими методами:

- сканирование;
- обнаружение изменений;
- эвристический анализ;
- использование резидентных сторожей;
- вакцинирование программ;
- аппаратно-программная защита.

Устранение последствий воздействия вирусов реализуется следующими методами:

- восстановление системы после воздействия известных вирусов;
- восстановление системы после воздействия неизвестных вирусов.

4.2 Профилактика заражения вирусами компьютерных систем

Главным условием безопасной работы в компьютерных системах является соблюдение правил, которые апробированы на практике и показали свою высокую эффективность.

Правило первое. Обязательное использование программных продуктов, полученных законным путём. Так как в пиратских копиях вероятность наличия вирусов во много раз выше, чем в официально полученном программном обеспечении.

Правило второе. Дублирование информации, то есть создавать копии рабочих файлов на съёмных носителях информации (дискеты, компакт-диски и другие) с защитой от записи.

Правило третье. Регулярно использовать антивирусные средства, то есть перед началом работы выполнять программы-сканеры и программы-ревизоры. Эти антивирусные средства необходимо регулярно обновлять.

Правило четвертое. Проявлять особую осторожность при использовании новых съёмных носителей информации и новых файлов. Новые дискеты и компакт-диски необходимо проверять на отсутствие загрузочных и файловых вирусов, а полученные файлы – на наличие файловых вирусов. Проверка осуществляется программами-сканерами и программами, осуществляющими эвристический анализ (Aidstest, Doctor Web, AntiVirus). При первом выполнении исполняемого файла используются резидентные сторожа. При работе с полученными документами и таблицами нужно запретить выполнение макрокоманд встроенными средствами текстовых и табличных редакторов (MS Word, MS Excel) до завершения полной проверки этих файлов на наличие вирусов.

Правило пятое. При работе в системах коллективного пользования необходимо новые сменные носители информации и вводимые в систему файлы проверять на специально выделенных для этой цели ЭВМ. Это должен выполнять администратор системы или лицо, отвечающее за безопасность информации. Только после всесторонней антивирусной проверки дисков и файлов они могут передаваться пользователям системы.

Правило шестое. Если не предполагается осуществлять запись информации на носитель, то необходимо заблокировать выполнение этой операции.

Постоянное выполнение изложенных правил позволяет значительно уменьшить вероятность заражения программными вирусами и обеспечить защиту пользователя от безвозвратных потерь информации.

В особо ответственных системах для борьбы с вирусами используются аппаратно-программные средства (например, Sheriff).

4.3 Порядок действий пользователя при обнаружении заражения вирусами компьютерной системы

Не смотря на строгое выполнение всех правил профилактики заражения вирусами компьютерной системы, нельзя полностью исключить возможность их заражения. Однако если придерживаться определённой последовательности действий при заражении вирусами, то последствия пребывания вирусов в компьютерной системе можно свести к минимуму.

О наличии вирусов можно судить по следующим событиям:

- появление сообщений антивирусных средств о заражении или о предполагаемом заражении;

- явные проявления присутствия вирусов (сообщения, выдаваемые на монитор или принтер, звуковые эффекты, уничтожение файлов и другие);
- неявные проявления заражения, которые могут быть вызваны сбоями или отказами аппаратных и программных средств, “зависаниями” системы, замедлением выполнения определённых действий, нарушением адресации, сбоями устройств и другими проявлениями.

При получении информации о предполагаемом заражении пользователь должен убедиться в этом. Решить такую задачу можно с помощью всего комплекса антивирусных средств. Если заражение действительно произошло, тогда пользователю следует выполнить следующую последовательность действий:

- выключить ЭВМ для уничтожения резидентных вирусов;
- осуществить загрузку эталонной операционной системы со сменного носителя информации, в которой отсутствуют вирусы;
- сохранить на сменных носителях информации важные файлы, которые не имеют резидентных копий;
- использовать антивирусные средства для удаления вирусов и восстановления файлов, областей памяти. Если работоспособность компьютерной системы восстановлена, то завершить восстановление информации всесторонней проверкой компьютерной системы с помощью всех имеющихся в распоряжении пользователя антивирусных средств. Иначе продолжить выполнение антивирусных действий;
- осуществить полное стирание и разметку (форматирование) несъёмных внешних запоминающих устройств. В персональных компьютерах для этого могут быть использованы программы MS-DOS FDISK и FORMAT. Программа форматирования FORMAT не удаляет главную загрузочную запись на жёстком диске, в которой может находиться загрузочный вирус. Поэтому необходимо выполнить программу FDISKc недокументированным параметром MBR, создать с помощью этой же программы разделы и логические диски на жёстком диске. Затем выполняется программа FORMAT для всех логических дисков;
- восстановить операционную систему, другие программные системы и файлы с резервных копий, созданных до заражения;
- тщательно проверить файлы, сохранённые после обнаружения заражения, и, при необходимости, удалить вирусы и восстановить файлы;
- завершить восстановление информации всесторонней проверкой компьютерной системы с помощью всех имеющихся в распоряжении пользователя антивирусных средств.

4.4 Особенности защиты информации в базах данных

Базы данных рассматриваются как надёжное хранилище структурированных данных, снабжённое специальным механизмом для их эффективного использования в интересах пользователей (процессов). Таким механизмом является система управления базами данных (СУБД). Под системой управления базами данных понимается программные или аппаратно-программные средства, реализующие функции управления данными, такие как: просмотр, сортировка, выборка, модификация, выполнение операций определения статистических характеристик и другие.

Базы данных размещаются:

- на компьютерной системе пользователя;
- на специально выделенной ЭВМ (сервере).

На компьютерной системе пользователя, как правило, размещаются личные или персональные базы данных, которые обслуживают процессы одного пользователя.

На серверах базы данных размещаются в локальных и корпоративных компьютерных сетях, которые используются, как правило, централизованно. Общедоступные глобальные компьютерные сети имеют распределённые базы данных. В таких сетях серверы размещаются на различных объектах сети. Серверы – это специализированные ЭВМ, приспособленные к хранению больших объёмов данных и обеспечивающие сохранность и доступность информации, а также оперативность обработки поступающих запросов. В централизованных базах данных решаются проще проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. Достоинством распределённых баз данных является их высокая защищённость от стихийных бедствий, аварий, сбоев технических средств и диверсий, если осуществляется дублирование этих данных.

Особенности защиты информации в базах данных:

- необходимость учёта функционирования СУБД при выборе механизмов защиты;
- разграничение доступа к информации реализуется не на уровне файлов, а на уровне частей баз данных.

При создании средств защиты информации в базах данных необходимо учитывать взаимодействие этих средств не только с операционной системой, но с СУБД. При этом возможно встраивание механизмов защиты в СУБД или использование их в виде отдельных компонент. Для большинства СУБД придание им дополнительных функций возможно только на этапе их разработки. В эксплуатируемые системы управления базами данных дополнительные компоненты могут быть внесены путём расширения или модификации языка управления.

4.5 Законодательные акты РФ, регулирующие правовые отношения в сфере компьютерной безопасности и защиты государственной тайны

В государстве должна проводиться единая политика в области безопасности информационных технологий. Это требование нашло отражение в “Концепции национальной безопасности Российской Федерации”, утверждённой Указом Президента РФ № 1300 от 17 декабря 1997 года. В этом документе отмечается, что в современных условиях всеобщей информатизации и развития информационных технологий резко возрастает значение обеспечения национальной безопасности РФ в информационной сфере. Значимость обеспечения безопасности государства в информационной сфере подчёркнута и в принятой в сентябре 2000 года “Доктрине информационной безопасности Российской Федерации”. В этих документах определены важнейшие задачи государства в области информационной безопасности:

- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями её распространения;
- совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое внедрение, унификация средств поиска, сбора, хранения и анализа информации с учётом вхождения России в глобальную информационную инфраструктуру;
- разработка соответствующей нормативной правовой базы в интересах обеспечения информационной безопасности;
- координация деятельности органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;
- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;
- защита государственного информационного ресурса и, прежде всего, в федеральных органах власти и на предприятиях оборонного комплекса.

25 февраля 1995 года Государственной Думой принят Федеральный закон “Об информации, информатизации и защите информации”. В законе даны определения основных терминов: информация, информатизация, информационные системы, информационные ресурсы, конфиденциальная информация, собственник и владелец информационных ресурсов, пользователь информации. Государство гарантирует права владельца информации, независимо от форм собственности, распоряжаться ею в пределах, установленных законом. Владелец информации имеет право защищать свои информационные ресурсы, устанавливать режим доступа к ним. В этом законе определены цели и режимы защиты информации, а также

порядок защиты прав субъектов в сфере информационных процессов и информатизации.

Другим важным правовым документом, регламентирующим вопросы защиты информации в КС, является закон РФ “О государственной тайне”, принятый 21.07.93 года. Закон определяет уровни секретности государственной информации и соответствующую степень важности информации.

Отношения, связанные с созданием программ и баз данных, регулируются законом РФ от 23.09.92 года “О правовой охране программ для ЭВМ и баз данных” и законом РФ от 09.07.93 года “Об авторском праве и смежных правах”.

Важной составляющей правового регулирования в области информационных технологий является установление ответственности граждан за противоправные действия при работе с КС. Преступления, совершённые с использованием КС или причинившие ущерб владельцам КС, получили название компьютерных преступлений.

В Уголовном кодексе РФ, принятом 1 января 1997 года, включена глава № 28, в которой определена уголовная ответственность за преступления в области компьютерных технологий.

В статье 272 предусмотрены наказания за неправомерный доступ к компьютерной информации. Это правонарушение может наказываться от штрафа в размере 200 минимальных зарплат до лишения свободы на срок до 5 лет.

Статья 273 устанавливает ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Это правонарушение может наказываться от штрафа до лишения свободы на срок до 7 лет.

В статье 274 определена ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Если такое деяние причинило существенный вред, то виновные наказываются лишением права занимать определённые должности или заниматься определённой деятельностью на срок до 5 лет. Если те же деяния повлекли тяжкие последствия, то предусмотрено лишение свободы на срок до 4 лет.

5. Заключение

Во всех странах убытки от злонамеренных действий непрерывно возрастают. Причем основные причины убытков связаны не столько с недостаточностью средств безопасности как таковых, сколько с отсутствием взаимосвязи между ними, т.е. с нереализованностью системного подхода. Поэтому необходимо опережающими темпами совершенствовать средства защиты.

6. Список литературы

1) Симонович С.В. Информатика. Базовый курс для ВУЗов, 2009.

2) Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009.

Также использованы интернет ресурсы:

1) Виды информации и ее свойства. Викиучебник, http://ru.wikibooks.org.

2) Википедия – свободная энциклопедия, http://ru.wikipedia.org.