Российская Федерация

Федеральное агентство по образованию

Государственное образовательное учреждение высшего профессионального образования

Брянский государственный университет имени академика И.Г. Петровского

Социально-экономический институт

Факультет технологий и дизайна

Реферат

На тему: "Основы защиты информации и сведений, составляющих государственную тайну. Правовая охрана программ для ЭВМ"

Выполнил:

cтудент 1с курса ОЗО

Цыганок М.И.

Проверила:

Преподаватель

Володина Ю.А.

Брянск-2010

Оглавление

Глава 1. Понятие и классификация информации по доступу к ней

1.1 Понятие и сущность компьютерной информации, ее отличие от других видов информации

1.2 Основные понятия и виды информации

1.3 Понятие Государственной тайны

Глава 2. Виды и источники угрозы информации

2.1 Виды умышленных угроз безопасности информации

2.2 Вирус – источник угрозы информации

Глава 3. Способы защиты информации

3.1 Блок законов Российской Федерации о защите информации

3.2 Закон "О правовой охране программ для электронных вычислительных машин и баз данных"

3.3 Комплексный подход к обеспечению информационной безопасности

3.4 Использование программных и программно-аппаратных средств обеспечения безопасности информации

Глава 4. Основные методы защиты информации

4.1 Использование Криптографических методов

4.2 Методы защиты информации в Internet

4.3 Метод парольной защиты

4.4 Административные методы защиты

4.5 Оценка эффективности систем защиты программного обеспечения

Заключение

Список литературы

Глава 1. Понятие и классификация информации по доступу к ней

1.1 Понятие и сущность компьютерной информации, ее отличие от других видов информации

В истории развития цивилизации выделяют несколько важных периодов становления информационных технологий, которые приводили к существенному изменению жизни человека.

На первых этапах развития человеческого общества общение между людьми носило примитивный характер. С возникновением различных ремесел и торговли между людьми начинает осуществляться обмен не только материальными ценностями, но и навыками, знаниями, идеями. Главными "инструментами" общения в этот период были язык и слух человека, а его мозг являлся естественным хранилищем знаний. Не случайно в период первобытно - общинного строя особая роль принадлежала людям преклонного возраста, как наиболее опытным и мудрым. Информация формировалась в устных преданиях, рассказах, песнях и с помощью речи передавалась из поколения в поколение.

Первые изменения в информационном обмене между людьми произошли с появлением письменности. Информация стала накапливаться не только в человеческой памяти. Она регистрировалась на камне, папирусе, бересте и бумаге. Переворот в накоплении и распространении информации произошел с изобретением книгопечатания. Знания отдельных людей, перенесенные на бумагу, становились достоянием многих. Это привело к интенсификации информационных обменов, возникновению новых идей в науке, способствовало ускорению роста промышленного производства. Книгопечатание явилось переломным моментом в сфере накопления и распространения знаний, открыло новую эпоху в жизни человечества, которую исследователи называют эпохой бумажной информатики.

Развитие человеческого общества сопровождалось ростом объема накопленных знаний и сведений как о самом человеке, так и об окружающем его мире. Начиная с начала XX в. темпы роста информации резко возросли. Так, если в XIX в. общая сумма человеческих знаний удваивалась через каждые 50 лет, то к 1950 г. — через 10 лет, а к 1970 г. — через каждые 5 лет. За последние два десятилетия с развитием средств массовых коммуникаций (печать, радио, телевидение, кино) объем информации резко возрос. Последнее наблюдается в науке и технике, экономике и политике, в других областях человеческой деятельности, в том числе и в правоохранительной. Это привело к возникновению противоречия, при котором производство информации стало значительно опережать возможности ее усвоения и использования. Сложившаяся ситуация характеризуется двумя положениями: с одной стороны, избыточным информационным потоком, с другой — информационным голодом. В первом случае потребитель буквально "захлебывается" и "тонет" в огромном объеме интересующей его информации. Во втором — потребитель не успевает отслеживать нужную ему информацию. Так, в России ежегодно находится в обращении около 800—850 млрд. документов. В их составлении участвуют миллионы людей. При этом используется реально только около 10% этих документов, поскольку их не успевают переработать традиционными (ручными или механизированными) методами и использовать для принятия управленческих решений. Исследования показывают, что руководители предприятий, учреждений и организаций более 70% времени расходуют на бумаготворчество.

В условиях традиционных методов (ручных, механизированных) переработка больших объемов информации в приемлемые сроки становится затруднительной, а подчас и невозможной. Остро встал вопрос об изменении технологии обработки информации, привлечении таких средств, которые освободили бы человека от трудоемкой работы, связанной с поиском, передачей, преобразованием, хранением и выдачей информации.

Появление вычислительной техники, и прежде всего электронно-вычислительных машин (ЭВМ), стало основой новой информационной технологии. Они стали применяться для создания комплексных автоматизированных систем информационного обеспечения, сводящих участие человека в этом процессе к минимуму (ЭВМ в автоматизированном режиме собирает, передает, обрабатывает, хранит и по запросу выдает необходимую информацию). Сегодня ЭВМ становятся основным инструментом для управления информацией и ее обработки, а человечество вплотную приблизилось к новому этапу своего развития — этапу безбумажной информатики.

Появление ЭВМ и их широкое использование в повседневной человеческой деятельности сравнимо по значению с двумя величайшими техническими свершениями — овладением огнем и использованием силы пара. Каждое такое свершение, как известно, явилось переворотом в жизни человечества. тайна информация вирус парольный

Стремительное развитие науки и техники позволит в обозримом будущем преобразовать традиционные информационные технологии, создать информационную индустрию и освободить человека от рутинных операций по сбору, обработке и хранению информации.

Дальнейшее накопление информации на машиночитаемых носителях (магнитные и оптические диски, магнитные ленты), глобальный охват населения средствами связи, позволяющими доставлять информацию в любую точку нашей планеты, автоматизированная обработка информации с использованием компьютера — вот те основные технические достижения, которые являются основой современной информационной технологии.

В самом общем виде информация (от лат. informatio — разъяснение, изложение) — это сведения о предметах, явлениях и процессах окружающего нас мира.

Федеральный закон "Об информатизации, информации и защите информации" определяет информацию как "сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы представления". В этой же статье приводятся определения документированной информации, информации о гражданах и конфиденциальной информации. К первой относится "зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать". Под второй понимаются "сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность". Конфиденциальной информацией считается "документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации".

Законодатель, не сформулировав понятия компьютерной информации, привел несколько отправных терминов и определений, которые позволили исследователям определиться с анализируемой дефиницией.

Одно из первых определений компьютерной информации принадлежит Н. Винеру. Он определял ее как "обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств. Процесс получения и использования информации является процессом нашего приспособления к случайностям внешней среды и нашей жизнедеятельности в этой среде". Другими словами, под компьютерной информацией понималось средство, позволяющее снять неопределенность в познании того или иного объекта. Отталкиваясь от средства хранения и передачи, можно говорить о том, что компьютерная информация — это информация, которая передается, обрабатывается и хранится с использованием электронно-вычислительной техники. Компьютерная информация может быть перенесена в пространстве, сохранена во времени, передана другому субъекту или техническому устройству (например, другому компьютеру), подвергнута иным операциям.

Как представляется, наиболее удачное определение сформулировано В. В. Крыловым. Он пишет: "Компьютерная информация есть сведения, знания или набор команд (программ), предназначенных для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях, — идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования".

Под собственником информационных ресурсов, информационных систем, технологий и средств их обеспечения понимается субъект, в полном объеме реализующий полномочия владения, пользования и распоряжения указанными объектами.

Владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения является субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения ими в пределах, установленных законом.

И, наконец, пользователем (потребителем) информации признается субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Действия других лиц, не являющихся собственником или владельцем информационных ресурсов, информационных систем, средств и технологий их обеспечения, а равно не являющихся законными пользователями информации,

признаются нарушением и, следовательно, влекут юридическую ответственность. В отдельных случаях действия таких лиц содержат признаки преступления, предусмотренного ст. 272 УК РФ (неправомерный доступ к компьютерной информации).

К уголовной ответственности по ст. 272 УК РФ следует, например, привлекать лицо, несанкционированно осуществившее доступ к охраняемой законом компьютерной информации, если указанные действия повлекли уничтожение этой информации, ее блокирование, модификацию либо копирование, а равно нарушение работы ЭВМ, системы ЭВМ или их сети.

1.2 Основные понятия и виды информации

Информация - сведения (сообщения, данные) независимо от формы их представления; (ФЗ РФ "Об информации, информационных технологиях и о защите информации от 27 июля 2006 года N 149-ФЗ).

#### **Доступ к информации** - получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Под информацией, применительно к задаче ее защиты понимается сведения о лицах, предметах, фактах, событиях явлениях и процессах независимо от формы их представления.

Информационные процессы – процессы сбора, накопления, обработки хранения, распределения и поиска информации.

Информационная система - совокупность документов и массивов документов и информационных технологий. Информационными ресурсами называют документы или массив документов существующие отдельно или в составе информационной системы. Процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства называется информатизацией. Информация по типам доступа может делиться на следующие категории:

1.3 Понятие Государственной тайны

Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно - розыскной деятельности, распространение которых может нанести ущерб безопасности государства.

В России перечень сведений, составляющих государственную тайну, определяется федеральным законом "О государственной тайне", на основании которого межведомственная комиссия по защите государственной тайне формирует перечень сведений, отнесенных к государственной тайне.

Государственную тайну составляют:

1) сведения в военной области:

* о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил РФ, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;
* о планах строительства Вооруженных Сил РФ, других войск РФ, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно - исследовательских и опытно - конструкторских работ по созданию и модернизации образцов вооружения и военной техники;
* о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;
* о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;
* о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;
* о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

* о содержании планов подготовки РФ и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;
* об использовании инфраструктуры РФ в целях обеспечения обороноспособности и безопасности государства;
* о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в РФ в целях обеспечения безопасности государства;
* об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;
* о достижениях науки и техники, о научно - исследовательских, об опытно - конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;
* об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых РФ (по списку, определяемому Правительством РФ);

3) сведения в области внешней политики и экономики:

* о внешнеполитической, внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести ущерб безопасности государства;
* о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

* о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
* о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно - розыскную деятельность;
* об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;
* о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;
* о методах и средствах защиты секретной информации;
* об организации и о фактическом состоянии защиты государственной тайны;
* о защите Государственной границы РФ, исключительной экономической зоны и континентального шельфа РФ;
* о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в РФ;
* о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

Лица, допущенные к сведениям уровня "совершенно секретно" или "особой важности" могут быть ограничены в своем праве выезда за границу. Такое ограничение может быть установлено исключительно в индивидуальном порядке органами безопасности, на основании заключения об осведомленности лица в сведениях, составляющих государственную тайну.

Должностные лица и граждане, виновные в нарушении законодательства РФ о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

Глава 2. Виды и источники угрозы информации

2.1 Виды умышленных угроз безопасности информации

Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов ИС, не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т.д.

Активные угрозы имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, вывод из строя компьютера или его операционной системы, искажение сведений в БД, разрушение ПО компьютеров, нарушение работы линий связи и т.д. Источником активных угроз могут быть действия взломщиков, вредоносные программы и т.п.

Умышленные угрозы подразделяются также на внутренние (возникающие внутри управляемой организации) и внешние.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение промышленный шпионаж — это наносящие ущерб владельцу коммерческой тайны незаконные сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности информации и нормального функционирования ИС относятся:

• утечка конфиденциальной информации;

• компрометация информации;

• несанкционированное использование информационных ресурсов;

• ошибочное использование информационных ресурсов;

• несанкционированный обмен информацией между абонентами;

• отказ от информации;

• нарушение информационного обслуживания;

• незаконное использование привилегий.

Утечка конфиденциальной информации — это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

• разглашения конфиденциальной информации;

• ухода информации по различным, главным образом техническим, каналам;

• несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

Несанкционированный доступ — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Пути несанкционированного доступа требуют достаточно больших технических знаний и соответствующих аппаратных или программных разработок со стороны взломщика. Например, используются технические каналы утечки — это физические пути от источника конфиденциальной информации к злоумышленнику, посредством которых возможно получение охраняемых сведений. Причиной возникновения каналов утечки являются конструктивные и технологические несовершенства схемных решений либо эксплуатационный износ элементов. Все это позволяет взломщикам создавать действующие на определенных физических принципах преобразователи, образующие присущий этим принципам канал передачи информации— канал утечки.

Однако есть и достаточно примитивные пути несанкционированного доступа:

• хищение носителей информации и документальных отходов;

• инициативное сотрудничество;

• склонение к сотрудничеству со стороны взломщика;

• выпытывание;

• подслушивание;

• наблюдение и другие пути.

Вредоносные программы классифицируются следующим образом: Логические бомбы, как вытекает из названия, используются для искажения или уничтожения информации, реже с их помощью совершаются кража или мошенничество. Манипуляциями с логическими бомбами обычно занимаются чем-то недовольные служащие, собирающиеся покинуть данную организацию, но это могут быть и консультанты, служащие с определенными политическими убеждениями и т.п.

Реальный пример логической бомбы: программист, предвидя свое увольнение, вносит в программу расчета заработной платы определенные изменения, которые начинают действовать, когда его фамилия исчезнет из набора данных о персонале фирмы.

Троянский конь — программа, выполняющая в дополнение к основным, т. е. запроектированным и документированным действиям, действия дополнительные, не описанные в документации. Аналогия с древнегреческим троянским конем оправдана — и в том и в другом случае в не вызывающей подозрения оболочке таится угроза. Троянский конь представляет собой дополнительный блок команд, тем или иным образом вставленный в исходную безвредную программу, которая затем передается (дарится, продается, подменяется) пользователям ИС. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени, по команде извне и т.д.). Запустивший такую программу подвергает опасности как свои файлы, так и всю ИС в целом. Троянский конь действует обычно в рамках полномочий одного пользователя, но в интересах другого пользователя или вообще постороннего человека, личность которого установить порой невозможно.

Червь — программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. Червь использует механизмы поддержки сети для определения узла, который может быть заражен. За- тем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий. Наиболее известный представитель этого класса — вирус Морриса (червь Морриса), поразивший сеть Internet в 1988 г. Подходящей средой распространения червя является сеть, все пользователи которой считаются дружественными и доверяют друг другу, а защитные механизмы отсутствуют. Наилучший способ защиты от червя — принятие мер предосторожности против несанкционированного доступа к сети.

Захватчик паролей — это программы, специально предназначенные для воровства паролей. При попытке обращения пользователя к терминалу системы на экран выводится информация, необходимая для окончания сеанса работы. Пытаясь организовать вход, пользователь вводит имя и пароль, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке, а ввод и управление возвращаются к операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля возможен и другими способами. Для предотвращения этой угрозы перед входом в систему необходимо убедиться, что вы вводите имя и пароль именно системной программе ввода, а не какой-нибудь другой. Кроме того, необходимо неукоснительно придерживаться правил использования паролей и работы с системой. Большинство нарушений происходит не из-за хитроумных атак, а из-за элементарной небрежности. Соблюдение специально разработанных правил использования паролей — необходимое условие надежной защиты.

Нарушение информационного обслуживания — угроза, источником которой является сама ИТ. Задержка с предоставлением информационных ресурсов абоненту может привести к тяжелым для него последствиям. Отсутствие у пользователя своевременных данных, необходимых для принятия решения, может вызвать его нерациональные действия.

Незаконное использование привилегий. Любая защищенная система содержит средства, используемые в чрезвычайных ситуациях, или средства которые способны функционировать с нарушением существующей политики безопасности. Например, на случай внезапной проверки пользователь должен иметь возможность доступа ко всем наборам системы. Обычно эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющими специальные функции.

Строгое соблюдение правил управления системой защиты, соблюдение принципа минимума привилегий позволяет избежать таких нарушений.

2.2 Вирус – источник угрозы информации

Вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а, скажем, при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Разновидности вирусов устроены так, что при запуске зараженной программы вирус остается резидентно, т.е. до перезагрузки DOS, компьютера и время от времени заражает программы и выполняет вредные действия на компьютере.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющих в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Следует заметить, что тексты программ и документов, информационные файлы без данных, таблицы табличных процессоров и другие аналогичные файлы не могут быть заражены вирусом, он может их только испортить.

В настоящее время известно более 87800 вирусов, число которых непрерывно растет. Известны случаи, когда создавались учебные пособия, помогающие в написании вирусов.

Основные виды вирусов: загрузочные, файловые, файлово-загрузочные. Наиболее опасный вид вирусов - полиморфные. Из истории компьютерной вирусологии ясно, что любая оригинальная компьютерная разработка заставляет создателей антивирусов приспосабливаться к новым технологиям, постоянно усовершенствовать антивирусные программы.

Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны - с отсутствием средств защиты у операционной системы.

Основные пути проникновения вирусов - съемные диски и компьютерные сети. Чтобы этого не случилось, соблюдайте меры по защите. Также для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов следствием не вполне ясного понимания предмета.

Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но, и могут вообще с ним не совпадать!

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-с) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (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.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые квазивирусные или "троянские" программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Глава 3. Способы защиты информации

3.1 Блок законов Российской Федерации о защите информации

Право граждан на информацию установлено Конституцией РФ, в соответствии с которой каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. В то же время с помощью блока специальных законов регулируется информационная безопасность государства, общества и личности. Среди этих законов:

* Закон "О средствах массовой информации" от 27.12.91 г. N 2124-I;
* Закон "О Федеральных органах правительственной связи и информации" от 19.02.92 N 4524-1;
* Закон "О правовой охране программ для электронных вычислительных машин и баз данных" от 23.09.92 года №3523-1;
* Закон "О правовой охране топологий интегральных микросхем" от 23.09.92 г. N 3526-I;
* Закон "О государственной тайне" от 21 июля 1993 г. N 5485-1;
* Закон "Об обязательном экземпляре документов" от 29.12.94 г. N 77-ФЗ;
* Закон "Об информации, информатизации и защите информации" от 20.02.95 года N 24-ФЗ;
* Закон "О внешней разведке" от 10.01.96 г. N 5-ФЗ;
* Закон "Об участии в международном информационном обмене" от 5.06.1996 г. N 85-ФЗ;
* Закон "О Государственной автоматизированной системе Российской Федерации "Выборы" N 20-ФЗ от 10 января 2003 г.

3.2 Закон "О правовой охране программ для электронных вычислительных машин и баз данных"

Правовая охрана программ для ЭВМ и баз данных впервые в полном объеме введена в Российской Федерации Законом "О правовой охране программ для электронных вычислительных машин и баз данных", который вступил в силу с 20 октября 1992 года. В п. 4 постановления о введении Закона в действие предусматривался переходный режим, когда до 1 января 1994 года использование в учебных, научно-исследовательских и личных целях без извлечения прибыли допускалось без согласия авторов и правообладателей. С 20 октября 1992 года в Российской Федерации охраняются как программы для ЭВМ и базы данных, созданные после этой даты, так и программы для ЭВМ и базы данных, созданные ранее, но использование которых продолжается после 20 октября 1992 года (п. 3). Соответственно, правовая охрана программам для ЭВМ и базам данных, созданных российскими авторами, предоставляется в зарубежных странах на тех же условиях тоже после 20 октября 1992 года. При этом необходимо, чтобы эти произведения были выпущены в свет.

В первой главе Закона сформулированы основные понятия, применяемые в данной области. Они включают определения обоих объектов охраны, условия признания авторского права, сроки охраны и сферы действия Закона. В ст. 1 особо выделены понятия адаптации, модификации и декомпилирования программы для ЭВМ или базы данных. С помощью этих понятий разграничиваются действия, которые можно и нельзя осуществлять без согласия автора (правообладателя). Не менее важны понятия, относящиеся к использованию программы для ЭВМ или базы данных, к их воспроизведению, распространению, выпуску в свет и иные действия по введению в хозяйственный оборот.

В главе II содержатся нормы, регулирующие исключительные авторские права. В статьях 8-12 этой главы четко разграничены личные и имущественные права автора, определен порядок передачи имущественных прав, в том числе и на программы для ЭВМ и базы данных, созданные в порядке выполнения служебных обязанностей (по заданию нанимателя). Специальная статья (13), посвященная праву на регистрацию программы для ЭВМ и базы данных, устанавливает требования к регистрации данных объектов в Российском агентстве по правовой охране программ для ЭВМ, баз данных и топологий интегральных микросхем (РосАПО).

В главе III конкретизированы особенности использования программы для ЭВМ и базы данных по договору с правообладателем, их свободного воспроизведения и адаптации, условия свободной перепродажи отдельных экземпляров.

В главе IV приведены нормы, обеспечивающие защиту прав автора (правообладателя) программы для ЭВМ или базы данных.

Таким образом, из основного закона о правовой охране программ для ЭВМ и баз данных следует, что, как минимум, должны быть изданы три подзаконных документа. К ним относятся "Правила составления, подачи и рассмотрения заявок на официальную регистрацию программ для электронных вычислительных машин и баз данных" (рег. N 181 в Минюсте России от 17.03.93), "Правила регистрации договоров на программы для электронных вычислительных машин, базы данных и топологии интегральных микросхем" (рег. N 183 в Минюсте России от 17.03.93) и "Положение о регистрационных сборах за официальную регистрацию программ для электронных вычислительных машин, баз данных и топологий интегральных микросхем". Положение было первоначально утверждено постановлением Совета Министров - Правительства Российской Федерации от 12 августа 1993 года N 793, а затем в него были внесены отдельные изменения и уточнен размер регистрационных сборов постановлением Правительства Российской Федерации от 23 апреля 1994 года N 382.

### 3.3 Комплексный подход к обеспечению информационной безопасности

Информация является одним из объектов гражданского права том числе и прав собственности, владения, пользования. Собственник информационных ресурсов, технологий и систем – субъект с правом владения, пользования и распределения указанных объектов. Владельцем ресурсов, технологий и систем является субъект с полномочиями владения и пользования указанными объектами. Под пользователем понимается субъект обращающийся к информационной системе за получением нужной информации и пользующегося ею.

К защищаемой относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, выдвигаемыми собственником информации.

Под утечкой информации понимают неконтролируемое распространение защищенной информации путем ее разглашения, несанкционированного доступа и получение разведчиками. Несанкционированный доступ - получение защищенной информации заинтересованным субъектом с нарушением правилом доступа к ней.

Несанкционированное воздействие на защищенную информацию это воздействие с нарушением правил ее изменения( например подменяя электронных документов). Под непреднамеренным воздействием на защищенную информацию понимается воздействие на нее из-за ошибок пользователя, сбой техники, или программных средств, природных явлений и других непреднамеренных воздействий( например уничтожение документа на накопителе на жестком диске).

Целью защиты информации является предотвращение нанесения ущерба пользователю, владельцу или собственнику. Под эффективностью защиты информации понимается степень соответствия результатов защиты поставленной цели. Объектом защиты может быть информация, ее носитель, информационный процесс, в отношении которого необходимо производить защиту в соответствии с поставленными целями.

Конфиденциальность информации – это известность ее содержания только имеющим, соответствующие полномочия субъект.

Шифрование информации это преобразование информации, в результате, которого содержание информации становится непонятным для субъекта, не имеющего соответствующего доступа. Результат шифрования называется шифротекстом.

Под угрозой информационной безопасности в компьютерной системе понимают события или действия которые могут вызвать изменения функционирования КС, связанные с нарушением защищенности информации обрабатываемой в ней.

Уязвимость информации – это возможность возникновения на каком либо этапе жизненного цикла КС такого ее состояния при котором создастся условия для реальной угрозы безопасности в ней

Атака это действие предпринимаемое нарушителем, в поиске и использовании той или иной уязвимости. Угрозы могу быть разделены на угрозы независящие от деятельности человека и искусственный угрозы, связанные с деятельностью человека.

Искусственные угрозы в свою очередь делятся на непреднамеренные (ошибки в проектировании, ошибки в работе программных средств) и преднамеренные (несанкционированный доступ, несанкционированные действия).

Результатом реализации угроз может быть утечка, искажение или утрата информации.

## 3.4 Использование программных и программно-аппаратных средств обеспечения безопасности информации

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав КС и выполняющие (как самостоятельно, так и при помощи программных средств) некоторые функции по обеспечению безопасности информации.

К основным аппаратным средствам защиты информации относятся:

* Устройства ввода идентифицирующий пользователя информации;
* Устройства шифрования информации;
* Устройства для воспрепятствования несанкционированному включению рабочих станций серверов.

Под программными средствами информационной безопасности понимают специальные программные средства, включаемые в состав программного обеспечения КС исключительно для выполнения защитах функций.

К основным программным средствам защиты информации относятся:

* Программы идентификации, аутентификации пользователей КС;
* Программы разграничения доступа пользователей к ресурсам КС;
* Программы от несанкционированного доступа, копирования изменения и использования.

К преимуществам программных средств защиты информации относятся:

* простота тиражирования;
* Гибкость (возможность настройки на различные условия применения);
* Простота применения;
* Практически неограниченные возможности их развития.

К недостаткам программных средств относятся:

* снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирования программ защиты;
* Более низкая производительность;
* Пристыкованность многих программных средств.

Глава 4. Основные методы защиты информации

##

## 4.1 Использование Криптографических методов

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

С широким распространением письменности криптография стала формироваться как самостоятельная наука. Первые криптосистемы встречаются уже в начале нашей эры. Так, Цезарь в своей переписке использовал уже более менее систематический шифр, получивший его имя.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos - тайный, logos - наука). Криптология разделяется на два направления - криптографию и криптоанализ. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов криптоанализа - исследование возможности расшифровывания информации без знания ключей.

Современная криптография включает в себя четыре крупных раздела:

Симметричные криптосистемы.

Криптосистемы с открытым ключом.

Системы электронной подписи.

Управление ключами.

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Как бы ни были сложны и надежны криптографические системы - их слабое мест при практической реализации - проблема распределения ключей. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены системы с открытым ключом.

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщение возможно только с использованием закрытого ключа, который известен только самому адресату.

4.2 Методы защиты информации в Internet

Сегодня самая актуальная для Internet тема - проблема защиты информации. Сеть стремительно развивается в глобальных масштабах, и все большее распространение получают системы внутренних сетей (intranet, интрасети). Появление на рынке новой огромной ниши послужило стимулом как для пользователей, так и для поставщиков сетевых услуг к поиску путей повышения безопасности передачи информации через Internet.

Проблема безопасности в Internet подразделяется на две категории: общая безопасность и вопросы надежности финансовых операций. Успешное разрешение проблем в сфере финансовой деятельности могло бы открыть перед Internet необозримые перспективы по предоставлению услуг для бизнеса. В борьбу за решение этой проблемы включились такие гиганты в области использовани кредитных карточек, как MasterCard и Visa, а также лидеры компьютерной индустрии Microsoft и Netscape. Все это касается "денежных" дел; наша же статья посвящена проблеме общей безопасности.

Задача исследований в этой области - решение проблемы конфиденциальности.

Кроме конфиденциальности пользователей также волнует вопрос гарантий, с кем они сейчас "беседуют". Им необходима уверенность, что сервер Internet, с которым у них сейчас сеанс связи, действительно является тем, за кого себя выдает; будь то сервер World-Wide Web, FTP, IRC или любой другой. Не составляет особого труда имитировать (то ли в шутку, то ли с преступными намерениями) незащищенный сервер и попытаться собрать всю информацию о вас. И, конечно же, поставщики сетевых услуг также хотели бы быть уверенными, что лица, обращающиеся к ним за определенными ресурсами Internet, например, электронной почтой и услугами IRC, действительно те, за кого себя выдают.

## 4.3 Метод парольной защиты

Законность запроса пользователя определяется по паролю, представляющему собой, как правило, строку знаков. Метод паролей считается достаточно слабым, так как пароль может стать объектом хищения, перехвата, перебора, угадывания. Однако простота метода стимулирует поиск путей его усиления.

Для повышения эффективности парольной защиты рекомендуется:

1. выбирать пароль длиной более 6 символов, избегая распространенных, легко угадываемых слов, имен, дат и т.п.;
2. использовать специальные символы;
3. пароли, хранящиеся на сервере, шифровать при помощи односторонней функции;
4. файл паролей размещать в особо защищаемой области ЗУ ЭВМ, закрытой для чтения пользователями;
5. комментарии файла паролей следует хранить отдельно от файла;
6. периодически менять пароли;
7. предусмотреть возможность насильственной смены паролей со стороны системы через определенный промежуток времени;
8. использовать несколько пользовательских паролей: собственно пароль, персональный идентификатор, пароль для блокировки/разблокировки аппаратуры при кратковременном отсутствии и т.п.

В качестве более сложных парольных методов используется случайная выборка символов пароля и одноразовое использование паролей. В первом случае пользователю (устройству) выделяется достаточно длинный пароль, причем каждый раз для опознавания используется часть пароля, выбираемая случайно. При одноразовом использовании пароля пользователю выделяется не один, а большое количество паролей, каждый из которых используется по списку или по случайной выборке один раз.

## 4.4 Административные методы защиты

Проблема защиты информации решается введением контроля доступа и разграничением полномочий пользователя.

Распространённым средством ограничения доступа (или ограничения полномочий) является система паролей. Однако оно ненадёжно. Опытные хакеры могут взломать эту защиту, "подсмотреть" чужой пароль или войти в систему путём перебора возможных паролей, так как очень часто для них используются имена, фамилии или даты рождения пользователей. Более надёжное решение состоит в организации контроля доступа в помещения или к конкретному ПК в ЛВС с помощью идентификационных пластиковых карточек различных видов.

Использование пластиковых карточек с магнитной полосой для этих целей вряд ли целесообразно, поскольку, её можно легко подделать. Более высокую степень надёжности обеспечивают пластиковые карточки с встроенной микросхемой – так называемые микропроцессорные карточки (МП – карточки, smart – card). Их надёжность обусловлена в первую очередь невозможностью копирования или подделки кустарным способом. Кроме того, при производстве карточек в каждую микросхему заносится уникальный код, который невозможно продублировать. При выдаче карточки пользователю на неё наносится один или несколько паролей, известных только её владельцу. Для некоторых видов МП – карточек попытка несанкционированного использования заканчивается её автоматическим "закрытием". Чтобы восстановить работоспособность такой карточки, её необходимо предъявить в соответствующую инстанцию.

Установка специального считывающего устройства МП – карточек возможна не только на входе в помещения, где расположены компьютеры, но и непосредственно на рабочих станциях и серверах сети.

4.5 Оценка эффективности систем защиты программного обеспечения

Системы защиты ПО широко распространены и находятся в постоянном развитии, благодаря расширению рынка ПО и телекоммуникационных технологий. Необходимость использования систем защиты (СЗ) ПО обусловлена рядом проблем, среди которых следует выделить: незаконное использование алгоритмов, являющихся интеллектуальной собственностью автора, при написании аналогов продукта (промышленный шпионаж); несанкционированное использование ПО (кража и копирование); несанкционированная модификация ПО с целью внедрения программных злоупотреблений; незаконное распространение и сбыт ПО (пиратство).

Системы защиты ПО по методу установки можно подразделить на системы, устанавливаемые на скомпилированные модули ПО; системы, встраиваемые в исходный код ПО до компиляции; и комбинированные.

Системы первого типа наиболее удобны для производителя ПО, так как легко можно защитить уже полностью готовое и оттестированное ПО (обычно процесс установки защиты максимально автоматизирован и сводится к указанию имени защищаемого файла и нажатию "Enter"), а потому и наиболее популярны. В то же время стойкость этих систем достаточно низка (в зависимости от принципа действия СЗ), так как для обхода защиты достаточно определить точку завершения работы "конверта" защиты и передачи управления защищенной программе, а затем принудительно ее сохранить в незащищенном виде.

Системы второго типа неудобны для производителя ПО, так как возникает необходимость обучать персонал работе с программным интерфейсом (API) системы защиты с вытекающими отсюда денежными и временными затратами. Кроме того, усложняется процесс тестирования П.О и снижается его надежность, так как кроме самого ПО ошибки может содержать API системы защиты или процедуры, его использующие. Но такие системы являются более стойкими к атакам, потому что здесь исчезает четкая граница между системой защиты и как таковым ПО.

Для защиты ПО используется ряд методов, таких как:

* Алгоритмы запутывания - используются хаотические переходы в разные части кода, внедрение ложных процедур - "пустышек", холостые циклы, искажение количества реальных параметров процедур ПО, разброс участков кода по разным областям ОЗУ и т.п.
* Алгоритмы мутации - создаются таблицы соответствия операндов - синонимов и замена их друг на друга при каждом запуске программы по определенной схеме или случайным образом, случайные изменения структуры программы.
* Алгоритмы компрессии данных - программа упаковывается, а затем распаковывается по мере выполнения.
* Алгоритмы шифрования данных - программа шифруется, а затем расшифровывается по мере выполнения.
* Вычисление сложных математических выражений в процессе отработки механизма защиты - элементы логики защиты зависят от результата вычисления значения какой-либо формулы или группы формул.
* Методы затруднения дизассемблирования - используются различные приемы, направленные на предотвращение дизассемблирования в пакетном режиме.
* Методы затруднения отладки - используются различные приемы, направленные на усложнение отладки программы.
* Эмуляция процессоров и операционных систем - создается виртуальный процессор и/или операционная система (не обязательно реально существующие) и программа-переводчик из системы команд IBM в систему команд созданного процессора или ОС, после такого перевода ПО может выполняться только при помощи эмулятора, что резко затрудняет исследование алгоритма ПО.

Заключение

В данной работе было проработано большое количество литературы и информации по выявлению источников угрозы информации и определению способов защиты от них.

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в нее изменений неуполномоченными лицами, и сохранение тайны переписки в электронной связи. Разумеется, во всех цивилизованных странах на безопасности граждан стоят законы, но в вычислительной технике правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, и надежность работы компьютерных систем во многом опирается на меры самозащиты.

Статистика показывает, что 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 комплексные средства защиты.

Список литературы

1. Баричев С.В. Криптография без секретов. – М., 1998. – с. 21-22.
2. Богатов Д.Ф., Богатов Ф.Г. Основы информатики и математики для юристов. В 2-х томах: краткий курс в таблицах, схемах и примерах. Учебник. - М.: Приор, 2000.- с.144, с. 166.
3. Информатика и математика для юристов: Учебное пособие для вузов (Гриф МО РФ) / Под ред. проф. Х.А.Андриашина, проф. С.Я.Казанцева – М.:Юнити-Дана, 2002.- с. 463.
4. Козырев А.А. Информатика: Учебник для вузов. СПб: издательство Михайлова В.А., 2002.- с. 511.

Крылов В.В. Информационные компьютерные преступления. – М., 1997

1. Левин В.К. Защита информации в информационно-вычислительных cистемах и сетях. Программирование. - 1994. - N5. - с. 5-16.
2. Мельников В.И. Защита информации в компьютерных системах. – М.: Финансы и статистика, Электронинформ, 1997. – с. 123 – 128.
3. Мостовой Д.Ю. Современные технологии борьбы с вирусами // Мир ПК.
4. Симонович С.В. и др. Информатика: Базовый курс. – СПб.: Питер –2002.
5. Турецкий В.Я. Математика и информатика.– 3-е изд., испр. и доп. – М.: Инфра-М, 2000.- с. 560.
6. ФЗ РФ "О персональных данных" от 27 июля 2006 года, №152-ФЗ
7. ФЗ РФ "О государственной тайне" от 21 июля 1993 года, № 5485-1 (в ред. ФЗ от 06.10.97 № 131-ФЗ)
8. ФЗ РФ "О коммерческой тайне" от 29 июля 2004 года N 98-ФЗ
9. ФЗ РФ "Об информации, информационных технологиях и о защите информации от 27 июля 2006 года N 149-ФЗ
10. Хореев П.В. Методы и средства защиты информации в компьютерных системах. – М.: издательский центр "Академия", 2005. – с. 205.