МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

М.Ю. НЕСТЕРЕНКО, С.И. СОРМОВ, Ю.В ПОЛИЩУК, Т.А. ЧЕРНЫХ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Рекомендовано Ученым советом государственного образовательного учреждения высшего профессионального образования «Оренбургский государственный университет» в качестве учебного пособия для студентов специальности 010503 – «Математическое обеспечение и администрирование информационных систем»

Оренбург 2009

УДК 004.239.056 (075)
ББК 65.011
Н56

Рецензент
доктор технических наук, профессор А.И. Сердюк

Нестеренко, М.Ю.
Н56 **Информационная безопасность в информационно-вычислительных системах: учебное пособие/С.И. Сормов, Ю.В. Полищук, Т.А. Черных – Оренбург: ГОУ ОГУ, 2009. – 104с.**

ISBN

В настоящем пособии рассмотрены проблемы уязвимости информации в современных системах обработки данных, классифицируются угрозы безопасности информации. Основное внимание уделяется проблемам опознавания пользователя, криптографическим методам защиты информации, методам защиты от компьютерных вирусов, защите от утечки информации по техническим каналам, организационно-правовому обеспечению безопасности информации.

Учебное пособие предназначено для студентов математического факультета, специализирующихся в области компьютерной безопасности, а также студентам факультета информационных технологий для изучения дисциплины «Информационная безопасность».

ББК 65.011

ISBN

Содержание

Введение

Информационная безопасность – сравнительно молодая, быстро развивающаяся область информационных технологий. Словосочетание информационная безопасность в разных контекстах может иметь различный смысл. Под информационной безопасностью будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Основное внимание сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке она закодирована, кто или что является ее источником, и какое психологическое воздействие она оказывает на людей.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

С методологической точки зрения правильный подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Информационная безопасность – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход. Для решения данной задачи используются меры законодательного, административного и программно-технического уровня.

В определении информационная безопасность - перед существительным «ущерб» стоит прилагательное «неприемлемый». Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Данное Учебное пособие предназначено для студентов математического факультета, специализирующихся в области компьютерной безопасности, а также студентам факультета информационных технологий для изучения дисциплины «Информационная безопасность».

1 Понятия, положения защиты информации в информационно-вычислительных системах

1.1 Предмет и объект защиты информации

Вопросы информационной безопасности занимают особое место и в связи с возрастающей ролью в жизни общества требуют к себе все большего внимания. Успех практически любой деятельности в немалой степени зависит от умения распоряжаться такой ценностью, как информация.

В законе РФ «Об информации, информатизации и защите информации» определено:

- «информационные ресурсы являются объектами собственности граждан, организаций, общественных объединений, государства»;
- «информация – сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), отраженные на материальных носителях, используемые в целях получения знаний и практических решений».

Информация имеет ряд особенностей:

- не материальна;
- хранится и передается с помощью материальных носителей;
- любой материальный объект содержит информацию о самом себе либо о другом объекте.

Ценность информации определяется степенью ее полезности для владельца.

Законом РФ «Об информации, информатизации и защите информации» гарантируется право собственника информации на ее использование и защиту от доступа к ней других лиц (организаций). Если доступ к информации ограничен, то такая информация называется конфиденциальной. Конфиденциальная информация может содержать государственную или коммерческую тайну.

Конфиденциальность информации – субъективно определяемая (приписываемая) характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию втайне от субъектов, не имеющих полномочий доступа к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты их законных интересов от других субъектов информационных отношений.

Государственную тайну могут содержать сведения, принадлежащие государству (государственному учреждению). В соответствии с законом «О государственной тайне» сведениям, представляющим ценность для государства, может быть присвоена одна из трех возможных степеней (гриф) секретности: «особая важность», «совершенно секретно » и «секретно». Для менее важной

информации в государственных учреждениях существует гриф «для служебного пользования».

Коммерческую тайну могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и т.д. Для обозначения ценности конфиденциальной коммерческой информации используют три категории: «коммерческая тайна – строго конфиденциально (строгий учет)», «коммерческая тайна – конфиденциально», «коммерческая тайна».

Достоверность информации определяется достаточной для владельца точностью отражать объекты и процессы окружающего мира в определенных временных и пространственных рамках. Информация, искаженно представляющая действительность, может нанести владельцу значительный материальный и моральный ущерб. Если информация искажена умышлено, то ее называют дезинформацией.

Предметом защиты является информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах. Особенностями данного вида информации являются:

- двоичное представление информации внутри системы, независимо от физической сущности носителей исходной информации;
- высокая степень автоматизации обработки и передачи информации;
- концентрации большого количества информации.

Объектом защиты информации является компьютерная система или автоматизированная система обработки информации.

Информационная система – это организационно-упорядоченная совокупность информационных ресурсов, технических средств, технологий и персонала, реализующих информационные процессы в традиционном или автоматизированном режиме для удовлетворения информационных потребностей пользователей.

Информационная безопасность АСОИ – состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой, ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Информационная безопасность достигается проведением соответствующего уровня политики информационной безопасности.

Под политикой информационной безопасности понимают совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АСОИ от заданного множества угроз безопасности.

Система защиты информации – совокупность правовых норм, организационных мер и мероприятий, технических, программных и криптографических средств и методов, обеспечивающих защищенность информации в системе в соответствии с принятой политикой безопасности.

1.2 Понятие угрозы безопасности

Под угрозой обычно понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим – либо интересам. В дальнейшем изложении, под угрозой информационной безопасности автоматизированной системы (АС) будем понимать возможность реализации воздействия на информацию, обрабатываемую АС, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

Типичными угрозами в АС являются:

- сбой в работе одной из компонент АС – сбой из-за ошибок при проектировании или ошибок оборудования или программ может привести к отказу в обслуживании или компрометации безопасности. Выход из строя брандмауэра или ложные отказы в авторизации серверами аутентификации являются примерами сбоев, которые оказывают влияние на безопасность;
- сканирование информации – неавторизованный просмотр критической информации злоумышленниками или авторизованными пользователями может происходить, используя различные механизмы – электронное письмо с неверным адресатом, распечатка принтера, неправильно сконфигурированные списки управления доступом, совместное использование несколькими людьми одного идентификатора и т.д.;
- использование информации не по назначению, использование информации для целей, отличных от авторизованных, может привести к отказу в обслуживании, излишним затратам, потере репутации. Виновниками этого могут быть как внутренние, так и внешние пользователи;
- неавторизованное удаление, модификация или раскрытие информации – специальное искажение информационных ценностей, которое может привести к потере целостности или конфиденциальности информации;
- проникновение – атака неавторизованных людей или систем, которая может привести к отказу в обслуживании или значительным затратам на восстановление после инцидента;
- маскарад – попытки замаскироваться под авторизованного пользователя для кражи сервисов или информации, или для инициации финансовых транзакций, которые приведут к финансовым потерям или проблемам для организации.

Наличие угрозы необязательно означает, что она нанесет вред. Чтобы стать риском, угроза должна использовать уязвимое место в средствах обеспечения безопасности системы и система должна быть видима из внешнего мира.

Видимость системы – это мера как интереса злоумышленников к этой системе, так и количества информации, доступной для общего пользования в этой системе.

Так как многие угрозы, основанные на глобальных сетях, являются вероятностными по своей природе, уровень видимости организации напрямую определяет вероятность того, что враждебные агенты будут пытаться нанести вред с помощью той или иной угрозы. В Интернете любопытные студенты, подростки-вандалы, криминальные элементы, промышленные шпионы могут являться носителями угрозы. По мере того как использование глобальных сетей для электронной коммерции и критических задач увеличивается, число атак криминальных элементов и шпионов будет увеличиваться.

Существует три разновидности угроз.

1. Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка».

2. Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

Целостность информации – существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Чаще субъектов интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т.е. ее не искаженности.

3. Угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую, для того чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих

автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

1.3 Классификация угроз информационной безопасности

Классификация всех возможных угроз информационной безопасности АС может быть проведена по ряду базовых признаков.

1. По природе возникновения.

Естественные угрозы – угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы – угрозы информационной безопасности АС, вызванные деятельностью человека.

2. По степени преднамеренности проявления.

Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала. Угрозы, не связанные с преднамеренными действиями злоумышленников и реализуемые в случайные моменты времени, называют случайными или непреднамеренными.

Реализация угроз этого класса приводит к наибольшим потерям информации (до 80 % ущерба). При этом может происходить уничтожение, нарушение целостности, доступности и конфиденциальности информации, например:

- проявление ошибок программно-аппаратных средств АС;
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

Угрозы преднамеренного действия, например:

- традиционный или универсальный шпионаж и диверсии (подслушивание, визуальное наблюдение; хищение документов и машинных носителей, хищение программ и атрибутов системы защиты, подкуп и шантаж сотрудников, сбор и анализ отходов машинных носителей, поджоги, взрывы);
- несанкционированный доступ к информации (реализуется в случае отсутствия системы разграничения доступа (СРД), сбоями или отказами технических средств), ошибками в СРД, фальсификацией полномочий);

- побочные электромагнитные излучения и наводки (ПЭМИН);

- несанкционированная модификация структур (алгоритмической, программной, технической);

- информационные инфекции (вредительские программы).

3. По непосредственному источнику угроз.

Угрозы, непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение и т.п.).

Угрозы, источником которых является человек, например:

- внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

- вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

- угроза несанкционированного копирования секретных данных пользователем АС;

- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства, например:

- запуск технологических программ, способных при некомпетентном пользовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

- возникновение отказа в работе операционной системы.

Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства, например:

- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

- заражение компьютера вирусами с деструктивными функциями.

4. По положению источника угроз.

Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС, например:

- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

- дистанционная фото- и видеосъемка.

Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС, например:

- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.д.);

- применение подслушивающих устройств.

Угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам).

Угрозы, источник которых расположен в АС, например:

- проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации;

- некорректное использование ресурсов АС.

5. По степени зависимости от активности АС.

Угрозы, которые могут проявляться независимо от активности АС, например:

- вскрытие шифров криптозащиты информации;

- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем).

Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных (например, угрозы выполнения и распространения программных вирусов).

6. По степени воздействия на АС.

Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС, например: угроза копирования секретных данных.

Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС, например:

- внедрение аппаратных спецвложений, программных «закладок » и «вирусов» («троянских коней» и «жучков»), т.е. таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

- угроза умышленной модификации информации.

7. По этапам доступа пользователей или программ к ресурсам АС.

Угрозы, которые могут проявляться на этапе доступа к ресурсам АС (например, угрозы несанкционированного доступа в АС).

Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС (например, угрозы несанкционированного или некорректного использования ресурсов АС).

8. По способу доступа к ресурсам АС.

Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС. Например:

- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.

Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС, например:

- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
- угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС.

9. По текущему месту расположения информации, хранимой и обрабатываемой в АС.

Угрозы доступа к информации на внешних запоминающих устройства (например, угроза несанкционированного копирования секретной информации с жесткого диска).

Угрозы доступа к информации в оперативной памяти, например:

- чтение остаточной информации из оперативной памяти;
- чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных АС и систем программирования;
- угроза доступа к системной области оперативной памяти со сторон прикладных программ.

Угрозы доступа к информации, циркулирующей в линиях связи, например:

- незаконное подключение к линиям связи с целью работы «между строк » с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений;

- перехват всего потока данных с целью дальнейшего анализа не в реальном масштабе времени.

Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере, например, угроза записи отображаемой информации на скрытую видеокамеру.

Возможности осуществления вредительских воздействий в большой степени зависят от статуса злоумышленника по отношению к АС.

Злоумышленником может быть:

- разработчик АС (владеет наиболее полной информацией о программных и аппаратных средствах АС и имеет возможность внедрения «закладок» на этапах создания и модернизации систем, но не получает доступа на эксплуатируемые объекты АС);

- сотрудник из числа обслуживающего персонала (наиболее опасный класс – работники службы безопасности информации, далее идут системные и прикладные программисты, инженерно-технический персонал);

- пользователь (имеет общее представление о структуре АС и механизмах ее защиты, но может осуществлять сбор информации методами традиционного шпионажа);

- постороннее лицо (может осуществлять дистанционные методы шпионажа и диверсионную деятельность).

1.4. Методы реализации угроз информационной безопасности

К основным направлениям реализации злоумышленником информационных угроз относятся:

- непосредственное обращение к объектам доступа;

- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;

- внедрение в технические средства АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС.

К числу основных методов реализации угроз информационной безопасности АС относятся:

- определение злоумышленником типа и параметров носителей информации;

- получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;

- получение злоумышленником детальной информации о функциях, выполняемых АС;

- получение злоумышленником данных о системах защиты;

- определение способа представления информации;

- определение злоумышленником содержания данных, обрабатываемых в АС, на качественном уровне (мониторинг дешифрования сообщений);

- хищение (копирование) машинных носителей информации, имеющих конфиденциальные данные;

- хищение (копирование) носителей информации;

- использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН) – конфиденциальные данные перехватываются злоумышленником путем изменения информативных сигналов из электромагнитного излучения и наводок по цепям питания средств вычислительной техники, входящей в АС;

- уничтожение средств ВТ и носителей информации;

- несанкционированный доступ пользователя к ресурсам АС путем преодоления систем защиты с использованием спецсредств, приемов, методов;

- несанкционированное превышение пользователем своих полномочий;

- несанкционированное копирование программного обеспечения;

- перехват данных, передаваемых по каналам связи;

- визуальное наблюдение – конфиденциальные данные считываются с экранов терминалов, распечаток в процессе их печати и т.п.;

- раскрытие представления информации (дешифрование данных);

- раскрытие содержания информации на семантическом уровне к смысловой составляющей информации, хранящейся в АС;

- уничтожение машинных носителей информации;

- внесение пользователем несанкционированных изменений программно-аппаратные компоненты АС и обрабатываемых данных;

- установка и использование нештатного аппаратного и/или программного обеспечения;

- заражение программными вирусами;

- внесение искажений в представление данных, уничтожение на уровне представления, искажение информации при передаче по линиям связи;

- внедрение дезинформации;

- выведение из строя машинных носителей информации без уничтожения информации (выведение из строя электронных блоков жестких дисков и т.п.);

- проявление ошибок проектирования и разработки аппаратных программных компонентов АС;

- обход (отключение) механизмов защиты – загрузка злоумышленником нештатной операционной системы с дискеты, использование режимов программно-аппаратных компонент АС и т.п.

- искажение соответствия синтаксических и семантических конструкций языка – установление новых значений слов, выражений и т.п.;

- запрет на использование информации – имеющаяся информация по каким-либо причинам не может быть использована.

1.5 Причины, виды и каналы утечки информации

Основными причинами утечки информации являются:

- несоблюдение персоналом норм, требований, правил эксплуатации АС;
- ошибки в проектировании АС и систем защиты АС;
- ведение противостоящей стороной технической и агентурной разведок.

Несоблюдение персоналом норм, требований, правил эксплуатации АС может быть как умышленным, так и непреднамеренным. От ведения противостоящей стороной агентурной разведки этот случай отличает то, что в данном случае лицом, совершающим несанкционированные действия, двигают личные побудительные мотивы. Причины утечки информации достаточно тесно связаны с видами утечки информации. Существует три вида утечки информации: разглашение, несанкционированный доступ к информации, получение защищаемой информации разведками.

Под разглашением информации понимается несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации.

Под несанкционированным доступом понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. При этом заинтересованным субъектом, осуществляющим несанкционированный доступ к информации, может быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Получение защищаемой информации разведками может осуществиться с помощью технических средств (техническая разведка) или агентурными методами (агентурная разведка).

Канал утечки информации – совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может располагаться в пределах контролируемой зоны, охватывающей или вне ее.

Применительно к АС выделяют несколько каналов утечки информации.

1. Электромагнитный канал. Причиной его возникновения является электромагнитное поле, связанное с протеканием электрического тока в аппаратных компонентах АС. Электромагнитное поле может индуцировать токи в близко расположенных проводных линиях (наводки).

2. Акустический (виброакустический) канал – связан с распространением звуковых волн в воздухе или упругих колебаний в других средах, возникающих при работе устройств отображения информации АС.

3. Визуальный канал – связан с возможностью визуального наблюдения злоумышленником за работой устройств отображения информации без

проникновения в помещения, где расположены компоненты системы. В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т.п.

4. Информационный канал – связан с доступом (непосредственным и телекоммуникационным) к элементам АС, к носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также с подключением к линиям связи.

1.6 Уязвимость и последствия

Организации по разному уязвимы к риску. Политики безопасности должны отражать уязвимость конкретной организации к различным типам инцидентов с безопасностью и делать приоритетными инвестиции в области наибольшей уязвимости.

Имеется два фактора, определяющих уязвимость организации. Первый фактор – последствия инцидента с безопасностью. Почти все организации уязвимы к финансовым потерям – устранение последствий инцидентов с безопасностью может потребовать значительных вложений, даже если пострадали некритические сервисы.

Одним из важных шагов при определении возможных последствий является ведение реестра информационных ценностей. Хотя это и кажется простым, поддержание точного списка систем, сетей, компьютеров и баз данных, использующихся в организации, является сложной задачей. Организации должны объединить этот список с результатами работ по классификации данных, в ходе которых информация классифицируется по степени важности для выполнения организацией своих задач. Более серьезные последствия возникают, когда нарушается внутренняя работа организации, что приводит к убыткам из-за упущенных возможностей, потерь рабочего времени и работ по восстановлению работы. Самые серьезные последствия – это невозможность системы выполнять свои внешние функции. Последствия инцидента с безопасностью напрямую вызывают нарушения работы служб.

1.7. Политика безопасности

Информация в системе, поддержанная информационной технологией, является критическим ресурсом, который позволяет использующим его организациям выполнять свои функции. При этом система будет выполнять эти функции эффективно только при осуществлении надлежащего контроля за информацией, чтобы гарантировать, что она защищена от опасностей типа нежелательного или несанкционированного распространения, изменения или потери. Анализ возможных угроз и анализ рисков помогает выбору мер безопасности, которые должны быть осуществлены, чтобы уменьшить риск до

приемлемого уровня. Эти меры безопасности можно обеспечить через соответствующие комбинации технологий, реализующих функции системы, и/или через внешние меры.

Особенностью понятия «защищенность» является его тесная связь с понятиями «злоумышленник» или «угрозы» (понятие, обезличивающее причину вывода системы из защищенного состояния злоумышленником). При рассмотрении понятия «злоумышленник» практически всегда выделяется объект его воздействия – часть системы, на которую направлены те или иные его действия.

Обычно выделяют три компоненты, связанные с нарушением безопасности системы: злоумышленник – внешний по отношению к системе источник нарушения свойства безопасности, объект атаки – часть, принадлежащая системе, на которую направлены те или иные воздействия «злоумышленника», канал воздействия – среда переноса злоумышленного воздействия.

Политика безопасности – это совокупность норм, правил и практических рекомендаций, регламентирующие работу средств защиты от заданного множества угроз безопасности.

Политика безопасности включает:

- множество возможных операций субъектов над объектами;
- для каждой пары «субъект – объект» множество разрешенных операций, из множества возможных операций.

Политика безопасности строится на основе анализа рисков системы, которые признаются реальными для информационной системы организации. Когда риски проанализированы, и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

1.8. Модели управления доступом

Основой политики безопасности являются модели управления доступом. Существуют следующие основные модели управления доступом: дискреционная, мандатная и ролевая.

Основой дискреционной модели является дискреционное управление доступом (Discretionary Access Control – DAC), которое определяется двумя свойствами:

- все субъекты и объекты должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

К достоинствам дискреционной политики безопасности можно отнести относительно простую реализацию соответствующих механизмов защиты. Этим обусловлен тот факт, что большинство распространенных в настоящее время автоматизированных систем обеспечивают выполнение положений именно

данной политики безопасности. К недостаткам относится статичность модели. Это означает, что данная политика безопасности не учитывает динамику изменений состояния АС, не накладывает ограничений на состояния системы. Кроме этого, при использовании дискреционной модели управления доступом возникает вопрос определения правил распространения прав доступа и анализа их влияния на безопасность АС, как результат - проблема троянских коней.

Для реализации модели управление доступом используется понятие монитор безопасности – средство, реализующее правила безопасности.

В общем случае при использовании данной модели управления доступом перед монитором безопасности объектов, который при санкционировании доступа субъекта к объекту руководствуется некоторым набором правил, стоит алгоритмически неразрешимая задача: проверить приведут ли его действия к нарушению безопасности или нет.

В терминах модели состояние системы характеризуется тройкой (S, O, M), где S – набор субъектов, O – набор объектов (в O могут быть включены и субъекты), M – матрица доступа. Для примера рассмотрим простейшую систему, состоящую из двух субъектов и двух объектов.

Допустим рассмотрение операций доступа: чтение, запись, выполнение и создание.

При этом предположим, что в системе реализовано дискреционное управление доступом, заданное матрицей M, где r — обозначение операции чтения (read), w — записи (write), e — исполнения (execute), c — создания (create).

В то же время имеются модели АС, реализующих дискреционную политику безопасности (например, модель Take – Grant), которые предоставляют алгоритмы проверки безопасности.

Основным недостатком дискреционной модели является проблема троянских коней – отсутствие контроля передачи прав от субъекта субъекту и, как следствие, возможность несанкционированной передачи прав.

Основу мандатной (обязательной) модели составляет мандатное управление доступом (Mandatory Access Control – MAC), которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- задан линейно упорядоченный набор меток секретности;
- каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации – его уровень секретности в АС;
- каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в АС – максимальное значение метки секретности объектов, к которым субъект имеет доступ; метка секретности субъекта называется его уровнем доступа.

Основная цель мандатной политики безопасности – предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа, т.е. противодействие возникновению в АС информационных каналов сверху вниз.

Средства MAC не позволят пользователю случайно или преднамеренно сделать информацию доступной для лиц, которые не должны обладать ею.

Обязательный контроль доступа управляет доступом на основе классификации объектов и субъектов системы. Каждому субъекту и объекту системы назначается некоторый уровень безопасности (УБ). Уровень безопасности объекта, как правило, описывает важность этого объекта и возможный ущерб, который может быть причинен при разглашении информации содержащейся в объекте. Уровень безопасности субъекта является уровнем доверия к нему. В простейшем случае все уровни безопасности являются членами некоторой иерархии. Например: Совершенно Секретно (СС), Секретно (С), Конфиденциально (К) и Рассекречено (Р), при этом верно следующее: СС > С > К > Р, т.е. каждый уровень включает сам себя и все уровни находящиеся ниже в иерархии.

Доступ субъекта к объекту предоставляется если выполнено некоторое условие отношения (которое зависит от типа доступа) между уровнями безопасности объекта и субъекта. В частности, должны выполняться следующие условия:

- Доступ на чтение дается если УБ субъекта включает в себя УБ объекта.
- Доступ на запись дается если УБ субъекта включается в УБ объекта.

Выполнение этих условий, гарантирует, что данные высокоуровневых объектов (например Совершенно Секретно) не попадут в низкоуровневые объекта (например Рассекреченный) смотрите рисунок 1.1.

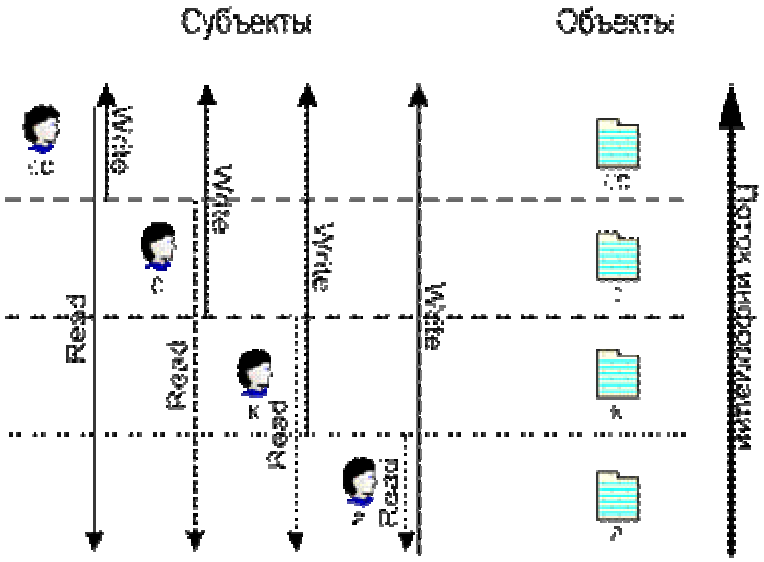

Рисунок 1.1 - Управление потоками информации для обеспечения безопасности данных.

В этой модели важно различать понятия пользователь и субъект. Уровни безопасности назначаются субъектам. А пользователи могут выступать от имени субъекта в тот или иной момент. При этом в различных ситуациях один пользователь может выступать от имени различных субъектов. При этом важно,

чтобы в каждый конкретный момент, пользователь выступал от имени только одного субъекта. Это обеспечивает невозможность передачи информации от высокого уровня к более низкому.

В описанной выше модели существует два неочевидных момента, которые ставят под вопрос непротиворечивость модели.

1. Пользователь нижнего уровня имеет право записывать в объекты всех верхних уровней. Таким образом он может переписать существующий объект своим собственным, что равносильно удалению. Этот недостаток может быть устранен путем запрета записи на более верхние уровни. При такой схеме правила будут выглядеть так:
   - Доступ на чтение дается если УБ субъекта включает в себя УБ объекта.
   - Доступ на запись дается если УБ субъекта равняется УБ объекта.
2. Из диаграммы видно, что пользователи с более высоки уровнем доверия не могут изменять объекты с более низким уровнем безопасности. Эта проблема разрешается тем, что пользователь при доступе к различным документам может выступать от имени субъектов с различными уровнями доверия. Т.е. пользователь с уровнем доверия «С» может выступать от имени субъектов с уровнем доверия «С», «К» и «Р».

В 2001 г. Национальный институт стандартов и технологий США предложил проект стандарта ролевого управления доступом. Ролевое разграничение доступа (РРД) представляет собой развитие политики дискреционного разграничения доступа; при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли. РРД является составляющей многих современных систем и применяется в системах защиты СУБД, сетевых ОС.

Задание ролей позволяет определить более четкие и понятные для пользователей системы правила разграничения доступа, соответствующих их должностным полномочиям и обязанностям.

Роль является совокупностью прав доступа на объекты системы. Вместе с тем РРД не является частным случаем дискреционного разграничения доступа, так как правила РРД определяют порядок предоставления прав доступа субъектам системы в зависимости от сессии его работы и от имеющихся или отсутствующих у него ролей в каждый момент времени, что является характерным для систем мандатного разграничения доступа. В то же время правила РРД являются более гибкими, чем правила мандатного разграничения доступа, построенные на основе жестко определенной решетки (шкалы) ценности информации. Суть ролевого разграничения доступа состоит в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах.

Ролевое управление доступом оперирует следующими основными понятиями:

- пользователь (человек, интеллектуальный автономный агент и т.п.);
- сеанс работы пользователя;
- роль (определяется в соответствии с организационной структурой);
- объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);
- операция (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п., для таблиц СУБД – вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными);
- право доступа (разрешение выполнять определенные операции над определенными объектами).

Ролям приписываются пользователи и права доступа; можно считать, что они именуют отношения "многие ко многим " между пользователями и правами. Роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям.

1.9 Контрольные вопросы

1. Охарактеризуйте информацию и ее свойства.
2. Что является предметом и объектом защиты информации?
3. Чем определяется ценность информации? Приведите классификацию конфиденциальной информаций.
4. Охарактеризуйте свойства достоверности и своевременности информации.
5. Что такое политика безопасности?
6. Назовите основные типы политики безопасности.
7. Назовите факторы определяющие уязвимость организаций.
8. Приведите пример простейшей системы, реализующую дискреционную модель управления доступом.
9. В чем состоят недостатки дискреционной модели?
10. Сформулируйте основные принципы мандатного управления доступом.
11. Что такое роль в ролевой модели?

2. Криптографическая защита информации

2.1. Основные понятия криптографии

С распространением письменности в человеческом обществе появилась потребность в обмене письмами и сообщениями, что вызвало необходимость сокрытия содержимого письменных сообщений от посторонних. Методы сокрытия содержимого письменных сообщений можно разделить на три группы. К первой группе относятся методы маскировки или стеганографии, которые осуществляют сокрытие самого факта наличия сообщения; вторую группу составляют различные методы тайнописи или криптографии (от греческих слов ktyptos – тайный и grapho – пишу); методы третьей группы ориентированы на создание специальных технических устройств, засекречивания информации.

Практически одновременно с криптографией стал развиваться и криптоанализ – наука о раскрытии шифров (ключей) по шифртексту.

Вторая мировая война дала новый толчок развитию криптографии и криптоанализа, что было вызвано применением технических средств связи и боевого управления. Для разработки новых шифров и работы в качестве криптоаналитиков привлекались ведущие ученые. В годы Второй мировой войны был разработан ряд механических устройств для шифрования сообщений.

В 1949 г. была опубликована статья Клода Шеннона «Теория связи в секретных системах», которая подвела научную базу под криптографию и криптоанализ. С этого времени стали говорить о КРИПТОЛОГИИ (от греческого kryptos – тайный и logos – сообщение) – науке о преобразовании информации для обеспечения ее секретности. Этап развития криптографии и криптоанализа до 1949 г. стали называть донаучной криптологией.

Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи.

Защита данных с помощью шифрования – одно из возможных решений проблемы безопасности. Зашифрованные данные становятся доступными только тем, кто знает, как их расшифровать, и поэтому похищение зашифрованных данных абсолютно бессмысленно для несанкционированных пользователей.

Коды и шифры использовались задолго до появления ЭВМ. С теоретической точки зрения не существует четкого различия между кодами и шифрами. Однако в современной практике различие между ними является достаточно четким. Коды оперируют лингвистическими элементами, разделяя шифруемый текст на такие смысловые элементы, как слова и слоги. В шифре всегда различают два элемента: алгоритм и ключ.

Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно большого текста.

Определим ряд терминов, используемых в криптологии.

Под шифром понимается совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма.

Гаммирование – процесс наложения по определенному закону гаммы шифра на открытые данные.

Гамма шифра – псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для зашифрования открытых данных и расшифрования зашифрованных данных.

Зашифрованием данных называется процесс преобразования открытых данных в зашифрованные с помощью шифра, а расшифрованием данных – процесс преобразования закрытых данных в открытые с помощью шифра.

Дешифрованием называется процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.

Имитозащита – защита от навязывания ложных данных. Для обеспечения имитозащиты к зашифрованным данным добавляется имитовставка, представляющая собой последовательность данных фиксированной длины, полученную по определенному правилу из открытых данных и ключа.

Криптографическая защита – это защита данных с помощью криптографического преобразования, под которым понимается преобразование данных шифрованием и (или) выработкой имитовставки.

Синхропосылка – исходные открытые параметры алгоритма криптографического преобразования.

Уравнение зашифрования (расшифрования) – соотношение, описывающее процесс образования зашифрованных (открытых) данных из открытых (зашифрованных) данных в результате преобразований, заданных алгоритмом криптографического преобразования.

Современные методы шифрования должны отвечать следующим требованиям:

1. Стойкость шифра, противостоящая криптоанализу должна быть такой, чтобы вскрытие шифра могло быть осуществлено только путем решения задачи полного перебора ключей.
2. Криптостойкость обеспечивается не секретностью алгоритма, а секретностью ключа.
3. Шифртекст не должен существенно превосходить по объему исходную

информацию.

4. Ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации.

5. Время шифрования не должно быть большим.

6. Стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

В настоящее время известно большое число методов криптографического закрытия информации. Классификация методов шифрования (криптоалгоритмов) может быть осуществлена по следующим признакам:

- по типу ключей: симметричные и асимметричные криптоалгоритмы;
- по размеру блока информации: потоковые и блочные шифры;
- по характеру воздействий, производимых над данными: метод замены (перестановки), метод подстановки; аналитические методы, аддитивные методы (гаммирование), комбинированные методы.

Кодирование может быть смысловое, символьное, комбинированное.

Закрытие информации другими способами может достигаться с помощью стеганографии, сжатия/расширения, рассечения/разнесения.

2.2 Симметричные криптографические методы шифрования

В данных методах один и тот же ключ (хранящийся в секрете) используется и для шифровки, и для расшифровки сообщений. Существуют весьма эффективные методы симметричного шифрования. Существует и стандарт на подобные методы – ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Для определенности будем вести речь о защите сообщений, хотя события могут развиваться не только в пространстве, но и во времени, когда шифруются и расшифровываются никуда не перемещающиеся файлы показанные на рисунке 2.1.

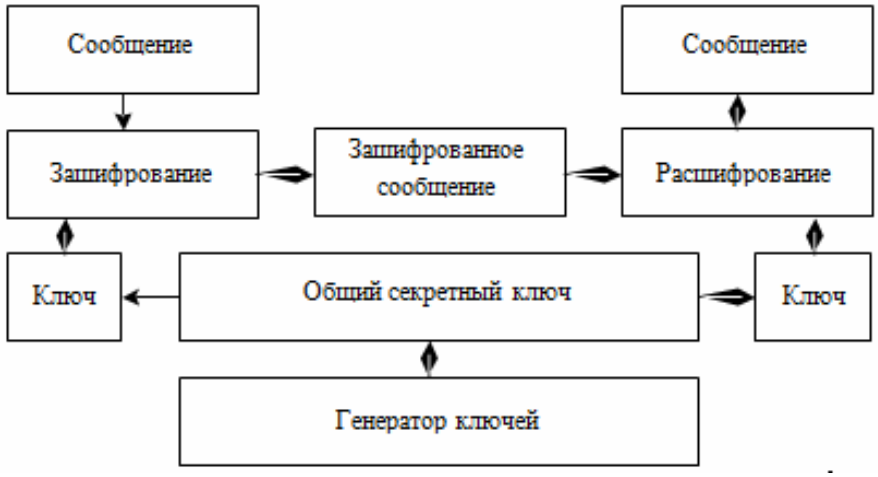

Рисунок 2.1- Использование симметричного метода шифрования.

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной

стороны, это ставит новую проблему рассылки ключей. С другой стороны, получатель на основании наличия шифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать и сам.

2.2.1 Методы замены

Шифрование методом замены (подстановки) основано на алгебраической операции, называемой подстановкой. Подстановкой называется взаимно-однозначное отображение некоторого конечного множества *M* на себя. Число *N* элементов этого множества называется степенью подстановки. Природа множества M роли не играет, поэтому можно считать, что *M = {1, 2,..., N}*.

Если при данной подстановке *S* число *j* переходит в *Ij*, то подстановка обозначается символом *S*:

$$S = \begin{bmatrix} 1 & 2 & & n \\ I_1 & I_2 & & I_n \end{bmatrix}$$

В этой записи числа 1, 2, ..., n можно произвольным образом переставлять, соответственно переставляя числа $I_1, I_2, ..., I_n$. Результат последовательного выполнения двух подстановок S_1 и S_2 одной и той же степени также является подстановкой, которая называется произведением подстановок S_1 и S_2 и обозначается S_1S_2.

Пусть *S* – произвольная подстановка степени *n*. Если для некоторого *j* число *Ij* отлично от j, то говорят, что подстановка *S* действительно перемещает число *j*; в противном случае – подстановка *S* оставляет число *j* на месте.

Количество *m* чисел, действительно перемещаемых подстановкой *S*, называется длиной цикла подстановки.

Подстановка *S* называется транспозицией, если существует пара (j_1, j_2) различных элементов из M, удовлетворяющих условиям:

$Ij_1 = j_2$, $Ij_2 = j_2$, $Ij = j$ для каждого $j \quad \{M\backslash\{j_1, j_2\}\}$. Любая подстановка разлагается в произведение транспозиций.

В качестве примера рассмотрим моноалфавитный тип замены.

Таблица 2.1 - Коды букв русского алфавита.

Буква	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	–
Код	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

При моноалфавитной замене каждой букве алфавита открытого текста ставится в соответствие одна буква шифртекста из этого же алфавита.

Пример. Открытый текст: «ШИФРОВАНИЕ_ЗАМЕНОЙ». Подстановка задана таблице 2.1.

Таблица 2.2 - Подстановка.

ИТ	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	–
ШТ	–	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Е	Д	Г	В	Б	А

ИТ – алфавит исходного текста; ШТ – алфавит шифртекста.

Шифртекст: «ИШМРТЮ_УШЫАЩ_ФЫУТЧ».

Основным недостатком рассмотренного метода является сохранение статистических свойств открытого текста (частота повторения букв) в шифртексте.

2.2.2 Методы перестановки

При использовании для шифрования информации методов перестановки символы открытого текста переставляются в соответствии с некоторыми правилами.

Пример. Открытый текст: «ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ». Ключ (правило перестановки): группы из 8 букв с порядковыми номерами 1, 2,..., 8 переставить в порядок 3-8-1-5-2-7-6-4.

Шифр текст: «ФНШОИАВР_СИЕЕЕРПННТВАОКО».

Можно использовать и усложненную перестановку. Для этого открытый текст записывается в матрицу по определенному ключу k1. Шифртекст образуется при считывании из этой матрицы по ключу k2.

Пример. Открытый текст: «ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ». Матрица из четырех столбцов. Ключи: *k1 {5-3-1-2-4-6}; k2 {4-2-3-1}*. Запись по строкам производится в соответствии с ключом k1. Чтение по столбцам в соответствии с ключом *k2* (рисунок 2.2).

1	И	Е	_	П
2	Е	Р	Е	С
3	О	В	А	Н
4	Т	А	Н	О
5	Ш	И	Ф	Р
6	В	К	О	Й
k_1/k_2	1	2	3	4

Рисунок 2.2 - Шифрование перестановкой.

Шифр текст: «ПСНОРЙЕРВАИК_ЕАНФОИЕОТШВ».

Наиболее сложные перестановки осуществляются по гамильтоновым путям, которых в графе может быть несколько.

В 1991 г. В.М. Кузьмич предложил схему перестановки, основанной на кубике Рубика. Согласно этой схеме открытый текст записывается в ячейки граней куба по строкам (рисунок 2.3). После осуществления заданного числа заданных поворотов слоев куба считывание шифртекста осуществляется по

столбикам. Сложность расшифрования в этом случае определяется количеством ячеек на гранях куба и сложностью выполненных поворотов слоев. Перестановка, основанная на кубике Рубика, получила название объемной (многомерной) перестановки.

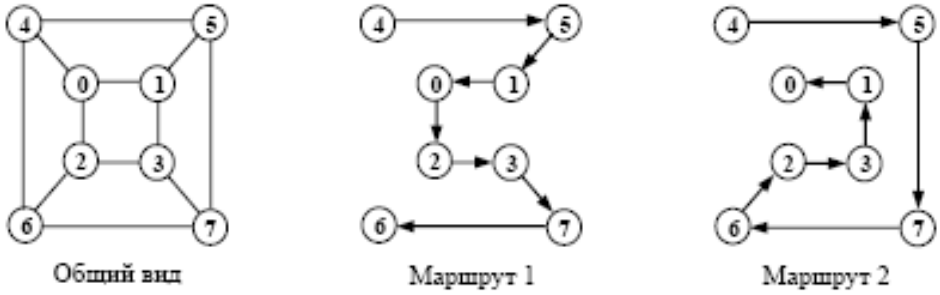

Рисунок 2.3 - Гамильтоновы пути на графе

В 1992–1994 г.г. идея применения объемной перестановки для шифрования открытого текста получила дальнейшее развитие. Усовершенствованная схема перестановок по принципу кубика Рубика, в которой наряду с открытым текстом перестановке подвергаются и функциональные элементы самого алгоритма шифрования, легла в основу секретной системы «Рубикон». В качестве прообразов пространственных многомерных структур, на основании объемных преобразований которых осуществляются перестановки, в системе «Рубикон» используются трехмерные куб и тэтраэдр. Другой особенностью системы «Рубикон» является генерация уникальной версии алгоритма и ключа криптографических преобразований на основании некоторого секретного параметра (пароля). Это обеспечивает как дополнительные трудности для криптоанализа перехваченных сообщений нарушителем (неопределенность примененного алгоритма), так и возможность априорного задания требуемой криптостойкости. Криптостойкость данной системы определяется длиной ключа, криптостойкостью отдельных функциональных элементов алгоритма криптографических преобразований, а также количеством таких преобразований.

Использование уникальных алгоритма и ключа шифрования для каждого пользователя системы соответствует положению теории К. Шеннона о том, что абсолютно стойкий шифр может быть получен только при использовании "ленты однократного применения", т.е. уникальных параметров при каждом осуществлении шифрования.

2.2.3 Методы аналитических преобразований

Шифрование методами аналитических преобразований основано на понятии односторонней функции. Будем говорить, что функция $y = f(x)$ является односторонней, если она за сравнительно небольшое число операций преобразует элемент открытого текста X в элемент шифртекста Y для всех значений X из области определения, а обратная операция (вычисление $X = F^{-1}(Y)$ при известном шифртексте) является вычислительно трудоемкой.

В качестве односторонней функции можно использовать следующие преобразования: умножение матриц; решение задачи об укладке ранца; вычисление значения полинома по модулю; экспоненциальные преобразования и др.

Метод умножения матриц использует преобразование вида $Y = CX$, где $Y = ||y1, y2,..., yn||T$; $C = ||Cij||$; $X = ||x1, x2,..., xn||$.

2.2.4 Гаммирование

Различают два случая: метод конечной гаммы и метод бесконечной гаммы. В качестве конечной гаммы может использоваться фраза, а в качестве бесконечной – последовательность, вырабатываемая датчиком псевдослучайных чисел.

Принцип зашифрования заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел (ПСЧ) и наложении полученной гаммы на открытые данные обратимым образом (например, при использовании логической операции «исключающее ИЛИ»).

Процесс расшифрования данных сводится к повторной генерации гаммы шифра при известном ключе и наложению такой гаммы на зашифрованные данные. Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, когда гамма шифра не содержит повторяющихся битовых последовательностей. По сути дела гамма шифра должна изменяться случайным образом для каждого шифруемого слова.

Фактически если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

Чтобы получить линейные последовательности элементов гаммы, длина которых превышает размер шифруемых данных, используются датчики ПСЧ. На основе теории групп было разработано несколько типов таких датчиков. В настоящее время наиболее доступными и эффективными являются конгруэнтные генераторы ПСЧ.

Они вырабатывают последовательности псевдослучайных чисел T(i), описываемые соотношением $T(i+1) = (A*T(i) + C) \bmod M$, где A и C – константы; $T(0)$ – исходная величина, выбранная в качестве порождающего числа.

Для шифрования данных с помощью датчика ПСЧ может быть выбран ключ любого размера. Например, пусть ключ состоит из набора чисел X(j) размерностью b, где $j = 1, 2,...., N$. Тогда создаваемую гамму шифра G можно представить как объединение непересекающихся множеств $H(j)$: $G = H(1) \cup H(2) \cup ... \cup H(N)$, где $H(j)$ – множество соответствующих j-му сегменту данных и полученных на основе порождающего числа Y(j), определенного как функция от $X(j)$ (например, ПСЧ, полученное на основе $X(j)$).

Разумеется, возможны и другие, более изощренные варианты выбора порождающих чисел для гаммы шифра. Более того, гамму шифра необязательно рассматривать как объединение непересекающихся множеств. Например, гамма шифра может быть представлена в виде *G = H(1) (+) H(2) (+) ... (+) H(N)*, где символ (+) обозначает операцию «Исключающее ИЛИ».

Шифрование с помощью датчика ПСЧ является довольно распространенным криптографическим методом, а качество шифра определяется не только и не столько характеристиками датчика, сколько алгоритмом получения гаммы. Хорошие результаты дает метод гаммирования с обратной связью, который заключается в том, что для получения сегмента гаммы используется контрольная сумма определенного участка шифруемых данных.

2.2.5 Комбинированные методы

Шифрование комбинированными методами основывается на результатах, полученных К. Шенноном. Наиболее часто применяются такие комбинации, как подстановка и гамма, перестановка и гамма, подстановка и перестановка, гамма и гамма. При составлении комбинированных шифров необходимо проявлять осторожность, так как неправильный выбор составлявших шифров может привести к исходному открытому тексту.

В качестве примера можно привести шифр, предложенный Д. Френдбергом, который комбинирует многоалфавитную подстановку с генератором ПСЧ. Особенность данного алгоритма состоит в том, что при большом объеме шифртекста частотные характеристики символов шифртекста близки к равномерному распределению независимо от содержания открытого текста.

Комбинация методов подстановки и перестановки была применена в 1974 г. Фирмой IBM при разработке системы ЛЮЦИФЕР.

Система ЛЮЦИФЕР строится на базе блоков подстановки (S-блоков) и блоков перестановки (P-блоков). Блок подстановки включает линейные и нелинейные преобразования.

Первый преобразователь S-блока осуществляет развертку двоичного числа из *n* разрядов в число по основанию 2^n. Второй преобразователь осуществляет свертку этого числа.

Блок перестановки осуществляет преобразование n разрядного входного числа в *n* разрядное число.

Входные данные (открытый текст) последовательно проходят через чередующиеся слои 32-разрядных P-блоков и 8-разрядных S-блоков.

Реализация шифрования данных в системе ЛЮЦИФЕР программными средствами показала низкую производительность, поэтому P и S-блоки были реализованы аппаратно, что позволило достичь скорости шифрования до 100 Кбайт/с. Опыт, полученный при разработке и эксплуатации системы, дал возможность создать стандарт шифрования данных DES.

DES (Data Encryption Standard) является одним из наиболее распространенных криптографических стандартов на шифрование данных, применяемых в США. Первоначально метод, лежащий в основе данного стандарта, был разработан фирмой IBM для своих целей. Он был проверен Агентством Национальной Безопасности США, которое не обнаружило в нем статистических или математических изъянов. Это означало, что дешифрование данных, защищенных с помощью DES, не могло быть выполнено статистическими (например, с помощью частотного словаря) или математическими («прокручиванием» в обратном направлении) методами.

После этого метод фирмы IBM был принят в качестве федерального стандарта.

Стандарт DES используется федеральными департаментами и агентствами для защиты всех достаточно важных данных в компьютерах (исключая некоторые данные, методы защиты которых определяются специальными актами). Его применяют многие негосударственные институты, в том числе большинство банков и служб обращения денег.

Оговоренный в стандарте алгоритм криптографической защиты данных опубликован для того, чтобы большинство пользователей могли использовать проверенный и апробированный алгоритм с хорошей криптостойкостью. Однако, с одной стороны, публикация алгоритма нежелательна, поскольку может привести к попыткам дешифрования закрытой информации, но, с другой стороны, это не столь существенно поскольку стандартный алгоритм шифрования данных должен обладать такими характеристиками, чтобы его опубликование не сказалось на его криптостойкости.

DES имеет блоки по 64 бит и основан на 16 кратной перестановке данных, также для шифрования использует ключ в 56 бит. Существует несколько режимов DES: электронная кодовая книга (ECB), сцепление блоков шифра (CBC), обратная связь по шифртексту CFB, обратная связь по выходу OFB. 56 бит – это 8 семибитовых ASCII символов, т.е. ключ не может быть больше чем 8 букв. Если вдобавок использовать только буквы и цифры, то количество возможных вариантов будет существенно меньше максимально возможных 256.

ГОСТ 28147–89 – отечественный стандарт на шифрование данных. В нашей стране установлен единый алгоритм криптографического преобразования данных для систем обработки информации в сетях ЭВМ, отдельных вычислительных комплексах и ЭВМ, который определяется указанным ГОСТом.

Этот алгоритм криптографического преобразования данных предназначен для аппаратной или программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничения на степень секретности защищаемой информации.

2.3 Ассиметричные методы шифрования

Наиболее перспективными системами криптографической защиты данных являются системы, основанные на асимметричных методах шифрования. В таких системах для зашифрования данных используется один ключ, а для расшифрования другой. Первый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью известного ключа невозможно. Для расшифрования данных получатель зашифрованной информации использует второй ключ, который является секретным. Разумеется, ключ расшифрования не может быть определен из ключа зашифрования.

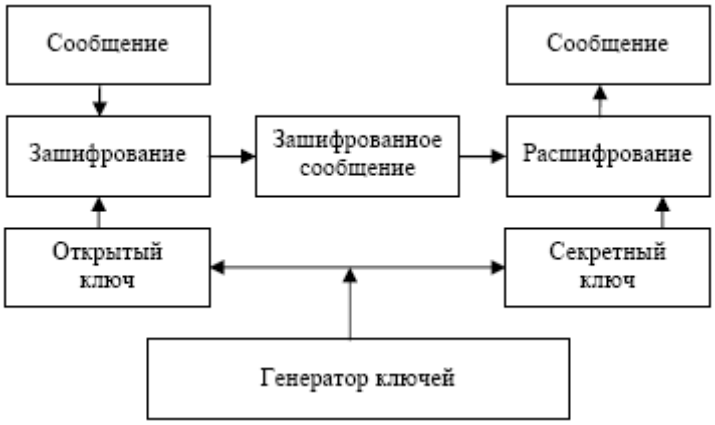

Рисунок 2.4 - Использование асимметричного метода шифрования.

Применение таких шифров стало возможным благодаря К. Шеннону, предложившему строить шифр таким способом, чтобы его раскрытие было эквивалентно решению математической задачи, требующей выполнения объемов вычислений, превосходящих возможности современных ЭВМ (например, операции с большими простыми числами и их произведениями).

Принцип применения асимметричного шифрования показан на рисунке 2.4.

2.3.1. Алгоритм RSA

В настоящее время наиболее развитым методом криптографической защиты информации с известным ключом является RSA, названный так по начальным буквам фамилий ее изобретателей (Rivest, Shamir и Adleman). Перед тем как приступить к изложению концепции метода RSA, необходимо определить некоторые термины.

Под простым числом будем понимать такое число, которое делится только на 1 и на само себя. Взаимно простыми числами будем называть такие числа, которые не имеют ни одного общего делителя, кроме 1.

Под результатом операции *i mod j* будем считать остаток от целочисленного деления *i* на *j*. Чтобы использовать алгоритм RSA, надо сначала сгенерировать открытый и секретный ключи, выполнив следующие шаги.

Выберем два очень больших простых числа p и q.

Определим n как результат умножения p на q $(n = pq)$.

Выберем большое случайное число, которое назовем d. Это число должно быть взаимно простым с m результатом умножения $(p - 1)$ $(q - 1)$.

Определим такое число e, для которого является истинным следующее соотношение $(e\ d)\ mod\ (m) = 1$.

Открытым ключом будут числа e и n, а секретным ключом – числа d и n.

Теперь, чтобы зашифровать данные по известному ключу $\{e, n\}$, необходимо сделать следующее:

− разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде числа $M(i) = 0, 1, \ldots, n - 1$;

− зашифровать текст, рассматриваемый как последовательность чисел $M(i)$ по формуле $C(i) = (M(i)^e)\ mod\ n$.

Чтобы расшифровать данные, используя секретный ключ $\{d, n\}$, необходимо выполнить следующие вычисления: $M(i) = (C(i)^d)\ mod\ n$. В результате получится множество чисел $M(i)$, которые представляют собой исходный текст.

Пример. Применим метод *RSA* для шифрования сообщения «ГАЗ». Для простоты будем использовать очень маленькие числа (на практике используются намного большие числа длиной не менее 512 бит).

Выберем $p = 3$ и $q = 11$.

Определим $n = 3 \quad 11 = 33$.

Найдем $(p - 1)$ $(q - 1) = 20$. Следовательно, в качестве d выберем любое число, которое является взаимно простым с 20, например $d = 3$.

Выберем число e. В качестве такого числа может быть взято число, для которого удовлетворяется соотношение $(e \times 3) \bmod 20 = 1$. Это соотношение может быть решено, например перебором чисел от 0 до 19. В данном случае e=7.

Представим шифруемое сообщение как последовательность целых чисел в диапазоне 0…32. Пусть буква *А* изображается числом 1, буква Г – числом 4, а буква З – числом 9.

Тогда сообщение можно представить в виде последовательности чисел 4 1 9. Зашифруем сообщение, используя ключ {7, 33}:

$C_1 = (4^7) \bmod 33 = 16384 \bmod 33 = 16$,

$C_2 = (1^7) \bmod 33 = 1 \bmod 33 = 1$,

$C_3 = (9^7) \bmod 33 = 4782969 \bmod 33 = 15$.

Шифртекст: «16 1 15».

Попытаемся расшифровать сообщение {16, 1, 15}, полученное в результате зашифрования по известному ключу, на основе секретного ключа {3, 33}:

$M_1 = (16^3) \bmod 33 = 4096 \bmod 33 = 4$,

$M_2 = (1^3) \bmod 33 = 1 \bmod 33 = 1$,

$M_3 = (15^3) \bmod 33 = 3375 \bmod 33 = 9$.

Таким образом, в результате расшифрования сообщения получено исходное сообщение «ГАЗ».

Криптостойкость алгоритма *RSA* основывается на предположении, что исключительно трудно определить секретный ключ по известному, поскольку для этого необходимо решить задачу о существовании делителей целого числа.

2.3.2 Электронная цифровая подпись

В основе криптографического контроля целостности лежат два понятия: хэш-функция; электронная цифровая подпись (ЭЦП).

Хэш-функция – это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых должна быть проверена, хэш-функция и ранее вычисленный результат ее применения к исходным данным (дайджест). Хэш-функцию обозначим через *h*, исходные данные – через *T*, проверяемые данные – через *T'*. Контроль целостности данных сводится к проверке равенства *h(T) = h(T')*. Если оно выполняется, считается, что *T = T'*. Совпадение дайджестов для различных данных называется коллизией. В принципе коллизии возможны (так как мощность множества дайджестов меньше множества хэшируемых данных), однако, исходя из определения хэш-функции, специально организовать коллизию за приемлемое время невозможно.

Асимметричные методы позволяют реализовать так называемую электронную цифровую подпись, или электронное заверение сообщения. Идея состоит в том, что отправитель посылает два экземпляра сообщения – открытое и дешифрованное его секретным ключом (естественно, дешифровка незашифрованного сообщения на самом деле есть форма шифрования). Получатель может зашифровать с помощью открытого ключа отправителя дешифрованный экземпляр и сравнить с открытым. Если они совпадут, личность и подпись отправителя можно считать установленными.

Пусть *E(T)* обозначает результат шифрования текста *T* с помощью открытого ключа, а *D(T)* – результат дешифровки текста *T* с помощью секретного ключа. Чтобы асимметричный метод мог применяться для реализации электронной подписи, необходимо выполнение тождества *E(D(T)) = D(E(T)) = T*.

На рисунке 2.5 показана процедура эффективной генерации электронной подписи, состоящая в шифровании преобразованием *D* дайджеста *h(T),* а проверка эффективно сгенерированной электронной подписи может быть реализована способом, изображенным на рисунке 2.6.

Из равенства *E(S') = h(T)* следует, *S'= D(h(T'))*. Следовательно, ЭЦП защищает целостность сообщения, удостоверяет личность отправителя и служит основой неотказуемости.

Два российских стандарта, «Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» и «Функция хэширования», объединенные общим заголовком «Информационная

технология. Криптографическая защита информации», регламентируют вычисление дайджеста и реализацию электронной подписи.

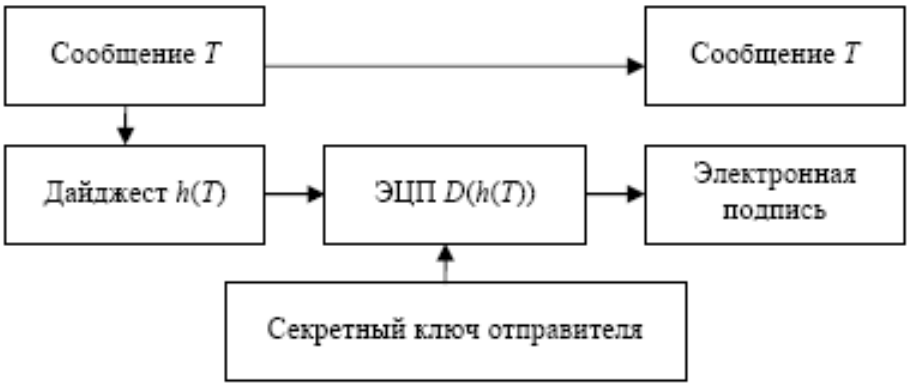

Рисунок 2.5 - Выработка электронной цифровой подписи.

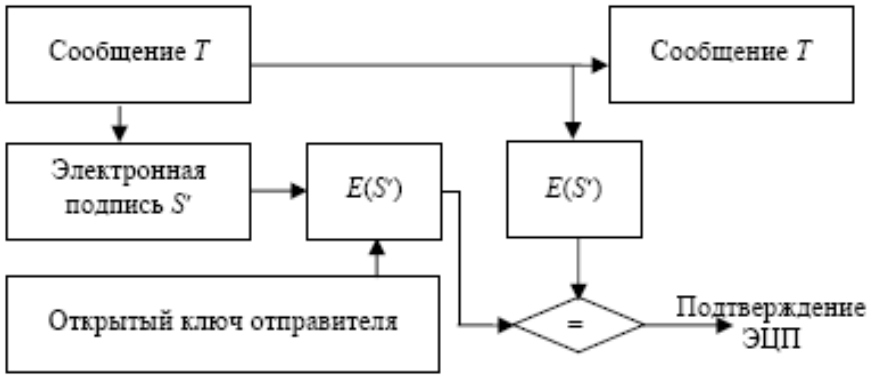

Рисунок 2.6 - Проверка электронной цифровой подписи.

В сентябре 2001 г. утвержден, а с 1 июля 2002 г. вступил в силу новый стандарт ЭЦП – ГОСТ Р 34.10–2001.

Для контроля целостности последовательности сообщений (т.е. защиты от кражи, дублирования и переупорядочения сообщений) применяют временные штампы и нумерацию элементов последовательности, при этом штампы и номера включают в подписываемый текст.

Обратим внимание на то, что при использовании асимметричных методов шифрования (в частности ЭЦП) необходимо иметь гарантию подлинности пары (имя, открытый ключ) адресата. Для решения этой задачи вводятся понятия цифрового сертификата и сертификационного центра. Сертификационный центр – это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей, заверяющий подлинность пары имя, открытый ключ адресата своей подписью.

Отметим, что услуги, характерные для асимметричного шифрования, можно реализовать и с помощью симметричных методов, если имеется надежная третья сторона, знающая секретные ключи своих клиентов.

2.4. Прочие методы шифрования

Широкое применение персональных ЭВМ (ПЭВМ) сделало актуальной задачу защиты хранящихся данных (файлов). Для защиты файлов могут быть применены рассмотренные методы шифрования и кодирования.

Специфика применения ПЭВМ позволяет реализовать дополнительные методы кодирования для надежного закрытия содержимого файлов. Примером такого кодирования является метод рассечения-разнесения, в соответствии с которым содержимое одного файла разбивается на блоки, которые разносятся по нескольким файлам. Каждый такой файл не несет никакой информации, а сбор данных в единое целое осуществляется простой программой.

Одной из важных проблем при использовании ПЭВМ является проблема хранения больших массивов данных. Для этой цели применяют различные методы сжатия данных (сжатие рассматривается как метод кодирования). Методы сжатия данных осуществляют такое преобразование повторяющихся символов и строк символов, которое позволяет использовать для хранения данных меньший объем памяти. Методы сжатия можно разделить на два класса: статические и динамические (адаптивные). Методы статического сжатия данных эффективны, когда частоты появления символов изменяются незначительно. Методы динамического сжатия адаптивно отслеживают неравномерности частот появления символов с сохранением последовательности изменений вероятностей появления символов. Адаптивные методы сжатия могут динамично реагировать на изменения в открытом тексте, происходящие по мере кодирования. Первые такие методы являлись модификацией кодов Хаффмена и использовали счетчики для хранения текущих частот появления каждого символа. При таких методах наиболее часто встречающиеся символы сдвигаются ближе к корню дерева и, следовательно, получают более короткие кодовые слова.

Кодирование Лемпеля-Зива использует синтаксический метод для динамического источника. Этот метод осуществляет синтаксический анализ символьных потоков, которые не превышают заданной длины, и строит таблицу отображения этих потоков в кодированные слова фиксированной длины. Длина кодового слова зависит от размера таблицы, используемой для хранения кодового отображения поток-слово. При кодировании по методу Лемпеля-Зива-Уэлча таблица инициализируется символьным множеством и содержит вместо потоков заданной длины пары (кодовое слово, символ) фиксированной длины. Таблица строится на основе синтаксического анализа самого длинного опознанного в таблице потока и использовании последующего символа для формирования нового входа в таблицу. Это позволяет уменьшить размеры таблицы.

В последнее время широкое распространение получили методы сжатия на основе расширяющихся деревьев. Префиксный код переменной длины в этих методах строится на основе положения символов в дереве. Для получения оптимальных кодов дерево балансируется.

Несомненно, криптография должна стать обязательным компонентом защиты всех сколько-нибудь развитых систем. К сожалению, этому мешает огромное количество самых разных барьеров.

2.5 Контрольные вопросы

1. Для чего предназначена криптография?
2. Что такое шифр?
3. Что такое гаммирование?
4. Назовите основные симметричные криптографические методы шифрования.
5. Что такое комбинированные методы шифрования?
6. В чем принципиальное различие ассиметричной системы от симметричной?

3. Информационная безопасность операционных систем

Операционная система (ОС) есть специально организованная совокупность программ, которая управляет ресурсами системы (ЭВМ, вычислительной системы, других компонентов ИВС) с целью наиболее эффективного их использования и обеспечивает интерфейс пользователя с ресурсами.

Операционные системы, подобно аппаратуре ЭВМ, на пути своего развития прошли несколько поколений.

ОС первого поколения были направлены на ускорение и упрощение перехода с одной задачи пользователя на другую задачу (другого пользователя), что поставило проблему обеспечения безопасности данных, принадлежащих разным задачам.

Второе поколение ОС характеризовалось наращиванием программных средств обеспечения операций ввода-вывода и стандартизацией обработки прерываний. Надежное обеспечение безопасности данных в целом осталось нерешенной проблемой.

К концу 60-х гг. XX в. начал осуществляться переход к мультипроцессорной организации средств ВТ, поэтому проблемы распределения ресурсов и их защиты стали более острыми и трудноразрешимыми. Решение этих проблем привело к соответствующей организации ОС и широкому применению аппаратных средств защиты (защита памяти, аппаратный контроль, диагностика и т.п.).

Основной тенденцией развития вычислительной техники была и остается идея максимальной доступности ее для пользователей, что входит в противоречие с требованием обеспечения безопасности данных.

Под механизмами защиты ОС будем понимать все средства и механизмы защиты данных, функционирующие в составе ОС. Операционные системы, в составе которых функционируют средства и механизмы защиты данных, часто называют защищенными системами.

Под безопасностью ОС будем понимать такое состояние ОС, при котором невозможно случайное или преднамеренное нарушение функционирования ОС, а также нарушение безопасности находящихся под управлением ОС ресурсов системы. Укажем следующие особенности ОС, которые позволяют выделить вопросы обеспечения безопасности ОС в особую категорию:

− управление всеми ресурсами системы;

− наличие встроенных механизмов, которые прямо или косвенно влияют на безопасность программ и данных, работающих в среде ОС;

− обеспечение интерфейса пользователя с ресурсами системы;

− размеры и сложность ОС.

Большинство ОС обладают дефектами с точки зрения обеспечения безопасности данных в системе, что обусловлено выполнением задачи обеспечения максимальной доступности системы для пользователя.

Рассмотрим типовые функциональные дефекты ОС, которые могут привести к созданию каналов утечки данных.

1. Идентификация. Каждому ресурсу в системе должно быть присвоено уникальное имя – идентификатор. Во многих системах пользователи не имеют возможности удостовериться в том, что используемые ими ресурсы действительно принадлежат системе.

2. Пароли. Большинство пользователей выбирают простейшие пароли, которые легко подобрать или угадать.

3. Список паролей. Хранение списка паролей в незашифрованном виде дает возможность его компрометации с последующим НСД к данным.

4. Пороговые значения. Для предотвращения попыток несанкционированного входа в систему с помощью подбора пароля необходимо ограничить число таких попыток, что в некоторых ОС не предусмотрено.

5. Подразумеваемое доверие. Во многих случаях программы ОС считают, что другие программы работают правильно.

6. Общая память. При использовании общей памяти не всегда после выполнения программ очищаются участки оперативной памяти (ОП).

7. Разрыв связи. В случае разрыва связи ОС должна немедленно закончить сеанс работы с пользователем или повторно установить подлинность субъекта.

8. Передача параметров по ссылке, а не по значению (при передаче параметров по ссылке возможно сохранение параметров в ОП после проверки их корректности, нарушитель может изменить эти данные до их использования).

9. Система может содержать много элементов (например, программ), имеющих различные привилегии.

Основной проблемой обеспечения безопасности ОС является проблема создания механизмов контроля доступа к ресурсам системы. Процедура контроля доступа заключается в проверке соответствия запроса субъекта предоставленным ему правам доступа к ресурсам. Кроме того, ОС содержит вспомогательные средства защиты, такие как средства мониторинга, профилактического контроля и аудита. В совокупности механизмы контроля доступа и вспомогательные средства защиты образуют механизмы управления доступом.

Средства профилактического контроля необходимы для отстранения пользователя от непосредственного выполнения критичных с точки зрения безопасности данных операций и передачи этих операций под контроль ОС. Для обеспечения безопасности данных работа с ресурсами системы осуществляется с помощью специальных программ ОС, доступ к которым ограничен.

Средства мониторинга осуществляют постоянное ведение регистрационного журнала, в который заносятся записи обо всех событиях в системе. В ОС могут применяться средства сигнализации о НСД, которые используются при обнаружении нарушения безопасности данных или попыток нарушения.

3.1 Безопасность в Windows NT

Операционная система Windows NT всегда обладала прекрасными и широко применимыми на практике возможностями защиты. Однократная регистрация в домене Windows NT предоставляет пользователям доступ к ресурсам всей корпоративной сети.

Полноценный набор инструментов Windows NT Server облегчает администраторам управление системой защиты и ее поддержку. Например, администратор может контролировать круг пользователей, имеющих права доступа к сетевым ресурсам: файлам, каталогам, серверам, принтерам и приложениям. Учетными записями пользователей и правами для каждого ресурса можно управлять централизованно.

С помощью простых графических инструментов администратор задает принадлежность к группам, допустимое время работы, срок действия и другие параметры учетной записи. Администратор получает возможность аудита всех событий, связанных с защитой доступа пользователей к файлам, каталогам, принтерам и иным ресурсам. Система также способна блокировать учетную запись пользователя, если число неудачных попыток регистрации превышает заранее определенное. Администраторы вправе устанавливать срок действия паролей, принуждать пользователей к периодической смене паролей и выбору паролей, затрудняющих несанкционированный доступ.

С точки зрения пользователя системы защита Windows NT Server полноценна и несложна в обращении. Простая процедура регистрации обеспечивает доступ к соответствующим ресурсам. Для пользователя невидимы такие процессы, как шифрование пароля на системном уровне. Пользователь сам определяет права доступа к тем ресурсам, которыми владеет. Например, чтобы разрешить совместное использование своего документа, он указывает, кто и как может с ним работать. Разумеется, доступ к ресурсам предприятия контролируется только администраторами с соответствующими полномочиями.

Более глубокий уровень безопасности – то, как Windows NT Server защищает данные, находящиеся в физической памяти компьютера. Доступ к ним предоставляется только имеющим на это право программам. Если данные больше не содержатся на диске, система предотвращает несанкционированный доступ к той области диска, где они содержались. При такой системе защиты никакая программа не «подсмотрит» в виртуальной памяти машины информацию, с которой оперирует в данный момент другое приложение.

Удаленный доступ через открытые сети и связь предприятий через Интернет стимулируют постоянное и быстрое развитие технологий безопасности. В качестве примера можно выделить сертификаты открытых ключей и динамические пароли. Перечислим функции безопасности Windows NT:

− информация о доменных правилах безопасности и учетная информация хранятся в каталоге Active Directory (служба каталогов Active Directory обеспечивает тиражирование и доступность учетной информации на многих контроллерах домена, а также позволяет удаленное администрирование);

− в Active Directory поддерживается иерархичное пространство имен пользователей, групп и учетных записей машин (учетные записи могут быть сгруппированы по организационным единицам);

− административные права на создание и управление группами учетных записей пользователей могут быть делегированы на уровень организационных

единиц (возможно установление дифференцированных прав доступа к отдельным свойствам пользовательских объектов);

− тиражирование Active Directory позволяет изменять учетную информацию на любом контроллере домена, а не только на первичном (копии Active Directory, хранящиеся на других контроллерах домена, обновляются и синхронизируются автоматически);

− доменная модель использует Active Directory для поддержки многоуровневого дерева доменов (управление доверительными отношениями между доменами упрощено в пределах всего дерева доменов);

− в систему безопасности включены механизмы аутентификации, такие как Kerberos v5 и TLS (Transport Layer Security), базирующиеся на стандартах безопасности Интернета;

− протоколы защищенных каналов (SSL 3.0/TLS) обеспечивают поддержку надежной аутентификации клиента (осуществляется сопоставление мандатов пользователей в форме сертификатов открытых ключей с существующими учетными записями Windows NT);

− дополнительно к регистрации посредством ввода пароля может поддерживаться аутентификация с использованием смарт-карт.

Внешние пользователи, не имеющие учетных записей Windows NT, могут быть аутентифицированы с помощью сертификатов открытых ключей и соотнесены с существующей учетной записью. Права доступа, назначенные для этой учетной записи, определяют права внешних пользователей на доступ к ресурсам.

В распоряжении пользователей простые средства управления парами закрытых (открытых) ключей и сертификатами, используемыми для доступа к ресурсам системы.

Технология шифрования встроена в операционную систему и позволяет использовать цифровые подписи для идентификации потоков.

Протокол аутентификации Kerberos определяет взаимодействие между клиентом и сетевым сервисом аутентификации, известным как KDC (Key Distribution Center). В Windows NT KDC используется как сервис аутентификации на всех контроллерах домена. Домен Windows NT эквивалентен области Kerberos, но к ней обращаются как к домену. Клиент Kerberos реализован в виде ПФБ (поставщика функций безопасности) Windows NT. Сервер Kerberos (KDC) интегрирован с существующими службами безопасности Windows NT, исполняемыми на контроллере домена. Для хранения информации о пользователях и группах он использует службу каталогов Active Directory.

Протокол Kerberos усиливает существующие функции безопасности Windows NT и добавляет новые:

− повышенная скорость аутентификации при установлении начального соединения (сервер приложений не обращается к контроллеру домена для аутентификации клиента);

− делегирование аутентификации в многоярусных архитектурах клиент-сервер (при подключении клиента к серверу, последний имперсонирует (олицетворяет) клиента в этой системе, но если серверу для завершения транзакции нужно выполнить сетевое подключение к другому серверу, протокол Kerberos позволяет делегировать аутентификацию первого сервера и подключиться ко второму от имени клиента);

− транзитивные доверительные отношения для междудоменной аутентификации (т.е. пользователь может быть аутентифицирован в любом месте дерева доменов) упрощают управление доменами в больших сетях с несколькими доменами.

Основы Kerberos. Протокол Kerberos является протоколом аутентификации с совместным секретом – и пользователю, и KDC известен пароль (KDC – зашифрованный пароль). Kerberos определяет серию обменов между клиентами, KDC и серверами для получения билетов Kerberos. Когда клиент начинает регистрацию в Windows NT, поставщик функций безопасности Kerberos получает начальный билет Kerberos TGT (Ticket grantticket), основанный на зашифрованном представлении пароля. Windows NT хранит TGT в кэше билетов на рабочей станции, связанной с контекстом регистрации пользователя. При попытке клиентской программы обратиться к сетевой службе проверяется кэш билетов: есть ли в нем верный билет для текущего сеанса работы с сервером. Если такого билета нет, на KDC посылается запрос с TGT для получения сеансового билета, разрешающего доступ к серверу.

Сеансовый билет добавляется в кэш и может впоследствии быть использован повторно для доступа к тому же самому серверу в течение времени действия билета. Время действия билета устанавливается доменными правилами и обычно равно восьми часам. Если время действия билета истекает в процессе сеанса, то поставщик функций безопасности Kerberos возвращает соответствующую ошибку, что позволяет клиенту и серверу обновить билет, создать новый сеансовый ключ и возобновить подключение. Сеансовый билет Kerberos предъявляется удаленной службе в сообщении о начале подключения. Части сеансового билета зашифрованы секретным ключом, используемым совместно службой и KDC. Сервер может быстро аутентифицировать клиента, проверив его сеансовый билет и не обращаясь к сервису аутентификации, так как на сервере в КЭШе хранится копия секретного ключа. Соединение при этом происходит гораздо быстрее. Сеансовые билеты Kerberos содержат уникальный сеансовый ключ, созданный KDC для симметричного шифрования информации об аутентификации, а также данных, передаваемых от клиента к серверу. В модели Kerberos KDC используется в качестве интерактивной доверенной стороны, генерирующей сеансовый ключ.

Протокол Kerberos полностью интегрирован с системой безопасности и контроля доступа Windows NT. Начальная регистрация в Windows NT обеспечивается процедурой WinLogon, использующей ПФБ Kerberos для получения начального билета TGT. Протокол Kerberos версии 5 реализован в

различных системах и используется для единообразия аутентификации в распределенной сети. Под взаимодействием Kerberos подразумевается общий протокол, позволяющий учетным записям аутентифицированных пользователей, хранящимся в одной базе осуществлять доступ ко всем сервисам в гетерогенной среде.

Взаимодействие Kerberos основывается на следующих характеристиках:

− общий протокол аутентификации пользователя или сервиса по основному имени при сетевом подключении;

− возможность определения доверительных отношений между областями Kerberos и создания ссылочных запросов билетов между областями;

− поддержка форматов маркера безопасности Kerberos версии 5 для установления контекста и обмена сообщениями.

Поддержка Kerberos открытых ключей.

В Windows NT также реализованы расширения протокола Kerberos, поддерживающие дополнительно к аутентификации с совместно используемым секретным ключом аутентификацию, основанную на парах открытого (закрытого) ключа. Поддержка открытых ключей позволяет клиентам запрашивать начальный ключ TGT с помощью закрытого ключа, в то время как KDC проверяет запрос с помощью открытого ключа, полученного из сертификата X.509 (хранится в пользовательском объекте в каталоге Active Directory), Сертификат пользователя может быть выдан как сторонним уполномоченным сертификации (Certification Authority), так и Microsoft Certificate Server, входящим в Windows NT. После начальной аутентификации закрытым ключом используются стандартные протоколы Kerberos для получения сеансовых билетов на доступ к сетевым службам,

Модель безопасности Windows NT обеспечивает однородный и унифицированный механизм контроля за доступом к ресурсам домена на основе членства в группах. Компоненты безопасности Windows NT доверяют хранимой в каталоге информации о защите.

Например, сервис аутентификации Windows NT хранит зашифрованные пароли пользователей в безопасной части каталога объектов пользователя. По умолчанию операционная система «считает», что правила безопасности защищены и не могут быть изменены кем-либо несанкционированно. Общая политика безопасности домена также хранится в каталоге Active Directory.

Делегирование административных полномочий – гибкий инструмент ограничения административной деятельности рамками части домена. Этот метод позволяет предоставить отдельным сотрудникам возможность управления пользователями или группами в заданных пределах и, в то же время, не дает им прав на управление учетными записями, относящимися к другим подразделениям.

Существует три способа делегирования административных полномочий:

- на изменение свойств определенного контейнера, например, LocalDomainPolicies самого домена;

- на создание и удаление дочерних объектов определенного типа (пользователи, группы, принтеры и пр.) внутри OU;

- на обновление определенных свойств некоторых дочерних объектов внутри OU (например, право устанавливать пароль для объектов типа User).

Делегировать полномочия просто. Достаточно выбрать лицо, которому будут делегированы полномочия, и указать, какие именно полномочия передаются. Интерфейс программы администрирования Active Directory позволяет без затруднений просматривать информацию о делегировании, определенную для контейнеров. Наследование прав доступа означает, что информация об управлении доступом, определенная в высших слоях контейнеров в каталоге, распространяется ниже – на вложенные контейнеры и объекты-листья.

Существуют две модели наследования прав доступа: динамическая и статическая. При динамическом наследовании права определяются путем оценки разрешений на доступ, назначенных непосредственно для объекта, а также для всех родительских объектов в каталоге. Это позволяет эффективно управлять доступом к части дерева каталога, внося изменения в контейнер, влияющий на все вложенные контейнеры и объекты-листья. Обратная сторона такой гибкости – недостаточно высокая производительность из-за времени определения эффективных прав доступа при запросе пользователя.

В Windows NT реализована статическая форма наследования прав доступа, иногда также называемая наследованием в момент создания. Информация об управлении доступом к контейнеру распространяется на все вложенные объекты контейнера. При создании нового объекта наследуемые права сливаются с правами доступа, назначаемыми по умолчанию. Любые изменения наследуемых прав доступа, выполняемые в дальнейшем на высших уровнях дерева, должны распространяться на все дочерние объекты. Новые наследуемые права доступа распространяются на объекты Active Directory в соответствии с тем, как эти новые права определены. Статическая модель наследования позволяет увеличить производительность.

Элементы безопасности системы. Далее будут рассмотрены вопросы реализации политики безопасности: управлению учетными записями пользователей и групп, исполнению и делегированию административных функций.

Учетные записи пользователей и групп. Любой пользователь Windows NT характеризуется определенной учетной записью. Под учетной записью понимается совокупность прав и дополнительных параметров, ассоциированных с определенным пользователем.

Кроме того, пользователь принадлежит к одной или нескольким группам. Принадлежность к группе позволяет быстро и эффективно назначать права доступа и полномочия.

К встроенным учетным записям пользователей относятся:

- Guest – учетная запись, фиксирующая минимальные привилегии гостя;

- Administrator – встроенная учетная запись для пользователей, наделенных максимальными привилегиями;

- Krbtgt – встроенная учетная запись, используемая при начальной аутентификации Kerberos.

Кроме них имеются скрытые встроенные учетные записи:

- System – учетная запись, используемая операционной системой;

- Creator owner – создатель (файла или каталога).

Перечислим встроенные группы:

- локальные (Account operators; Administrators; Backup operators; Guests; Print operators; Replicator; Server operators; Users);

- глобальные (Domain guests – гости домена; Domain Users – пользователи домена; Domain Admins – администраторы домена).

Помимо этих встроенных групп имеется еще ряд специальных групп:

- Everyone – в эту группу по умолчанию включаются вообще все пользователи в системе;

- Authenticated users – в эту группу включаются только аутентифицированные пользователи домена;

- Self – сам объект.

Для просмотра и модификации свойств учетной записи достаточно щелкнуть имя пользователя или группы и на экране появится диалоговое окно User Properties:

• General – общее описание пользователя;

• Address – домашний и рабочий адрес пользователя;

• Account – обязательные параметры учетной записи;

• Telephone/notes – необязательные параметры;

• Organization – дополнительные необязательные сведения;

• Membership – обязательная информация о принадлежности пользователя к группам;

• Dial-in – параметры удаленного доступа;

• Object – идентификационные сведения о пользовательском объекте;

• Security – информация о защите объекта.

Локальная политика безопасности – регламентирует правила безопасности на локальном компьютере. С ее помощью можно распределить административные роли, конкретизировать привилегии пользователей, назначить правила аудита.

По умолчанию поддерживаются следующие области безопасности:

- политика безопасности – задание различных атрибутов безопасности на локальном и доменном уровнях; так же охватывает некоторые установки на машинном уровне;

- управление группами с ограничениями – позволяет управлять членством в группах, которые, по мнению администратора, «чувствительны» с точки зрения безопасности системы;

- управление правами и привилегиями – позволяет редактировать список пользователей и их специфических прав и привилегий;

- деревья объектов – включают три области защиты: объекты каталога Active Directory, ключи реестра, локальную файловую систему; для каждого объекта в дереве шаблоны безопасности позволяют конфигурировать и анализировать характеристики дескрипторов защиты, включая владельцев объекта, списки контроля доступа и параметры аудита;

- системные службы (сетевые или локальные) – построенные соответствующим образом дают возможность независимым производителям программного обеспечения расширять редактор конфигураций безопасности для устранения специфических проблем.

Для конфигурирования параметров безопасности системы используются шаблоны.

Реестр – это дерево объектов. Доступ к каждому объекту в дереве должен быть регламентирован. Выбрав в окне обзорного просмотра ветвь, соответствующую шаблону Custom, щелкните папку Registry. В правой части окна появится список ветвей реестра, доступ к которым можно ограничивать. В шаблоне, поставляемом с редактором, приведена ветвь MACHINE\HARDWARE, которую надо истолковывать как HKEY_LOCAL_MACHINE\Hardware. Чтобы добавить к дереву новые ветви, их надо в явном виде прописать в шаблоне с помощью любого текстового редактора. Для разграничения доступа к выбранной ветви реестра дважды щелкните ее имя и укажите нужный тип доступа и имя соответствующей учетной записи. Изменения будут занесены в шаблон.

3.2 Безопасность в UNIX

Операционная система UNIX относится к категории многопользовательских многопрограммных ОС (операционная система), работающих в режиме разделения времени. Богатые возможности, заложенные в ОС UNIX, сделали ее наиболее популярной в мире. ОС UNIX поддерживается практически на всех типах ЭВМ.

Организация работ в ОС UNIX основана на понятии последовательного процесса как единицы работы, управления и потребления ресурсов. Взаимодействие процессов внутри ядра (процесс вызывает ядро как подпрограмму) происходит по принципу сопрограмм. Последовательность вычислений внутри процесса строго выдерживается: процесс, в частности, не может активизировать ввод–вывод и продолжать вычисление параллельно с ним. В этом случае требуется создать параллельный процесс.

Резидентная часть ОС называется ядром. Ядро ОС UNIX состоит из двух основных частей: управления процессами и управления устройствами. Управление процессами резервирует ресурсы, определяет последовательность выполнения процессов и принимает запросы на обслуживание. Управление устройствами контролирует передачу данных между ОП и периферийными устройствами.

В любой момент времени выполняется либо программа пользователя (процесс), либо команда ОС. В каждый момент времени лишь один пользовательский процесс активен, а все остальные приостановлены. Ядро ОС UNIX служит для удовлетворения потребностей процессов.

Процесс – это программа на этапе выполнения. В некоторый момент времени программе могут соответствовать один или несколько процессов, или не соответствовать ни одного. Считается, что процесс является объектом, учтенным в специальной таблице ядра системы. Наиболее важная информация о процессе хранится в двух местах: в таблице процессов и в таблице пользователя, называемой также контекстом процесса. Таблица процессов всегда находится в памяти и содержит на каждый процесс по одному элементу, в котором отражается состояние процесса: адрес в памяти или адрес своппинга, размер, идентификаторы процесса и запустившего его пользователя. Таблица пользователя существует для каждого активного процесса и к ней могут непосредственно адресоваться только программы ядра (ядро резервирует по одному контексту на каждый активный процесс). В этой таблице содержится информация, требуемая во время выполнения процесса: идентификационные номера пользователя и группы, предназначенные для определения привилегий доступа к файлам, ссылки на системную таблицу файлов для всех открытых процессом файлов, указатель на индексный дескриптор текущего каталога в таблице индексных дескрипторов и список реакций на различные ситуации. Если процесс приостанавливается, контекст становится недоступным и не модифицируемым.

Каталоги файловой системы ОС UNIX «спрятаны» от пользователей и защищены механизмами ОС. Скрытой частью файловой организации в ОС UNIX является индексный дескриптор файла, который описывает расположение файла, его длину, метод доступа к файлу, даты, связанные с историей создания файла, идентификатор владельца и т.д.

Работа с таблицами является привилегией ядра, что обеспечивает сохранность и безопасность системы. Структура данных ядра ОС, обеспечивающих доступ к файлам, приведена на рисунке 3.1.

При взаимодействии с ОС UNIX пользователь может обращаться к большому числу информационных объектов или файлов, объединенных в каталоги. Файловая система ОС UNIX имеет иерархическую структуру.

В ОС UNIX используется четыре типа файлов: обычные, специальные, каталоги, а в некоторых версиях ОС и FIFO-файлы (First In – First Out). Обычные файлы содержат данные пользователей. Специальные файлы предназначены для организации взаимодействия с устройствами ввода–вывода. Доступ к любому устройству реализуется как обслуживание запроса к специальному (дисковому) файлу. Каталоги используются системой для поддержания файловой структуры. Особенность каталогов состоит в том, что пользователь может читать их содержимое, но выполнять записи в каталоги (изменять структуру каталогов) может только ОС. В ОС UNIX, организуются именованные программные каналы,

являющиеся соединительным средством между стандартным выводом одной программы и стандартным вводом другой. Схема типичной файловой системы ОС UNIX приведена на рисунке 3.2.

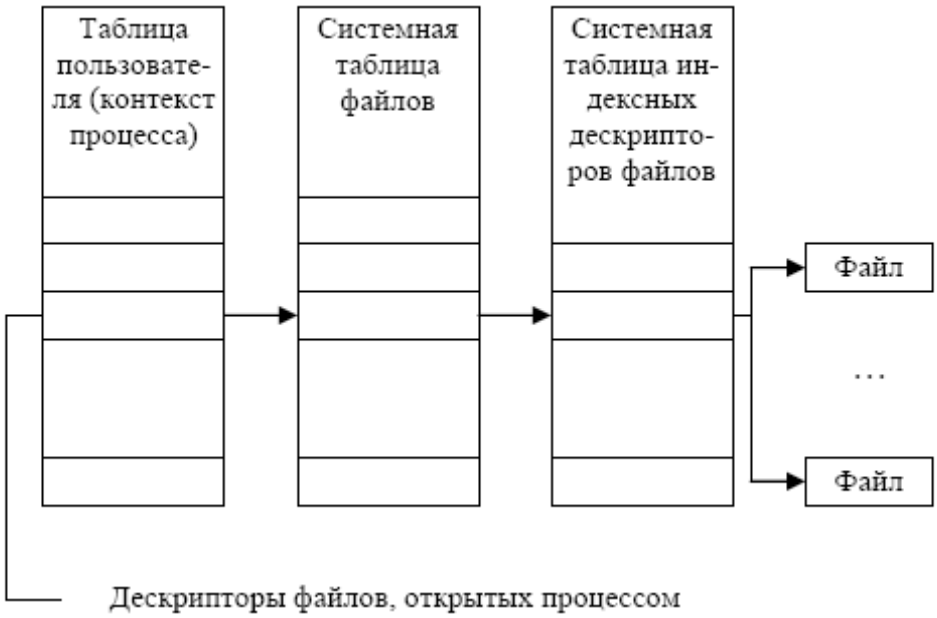

Рисунок 3.1 - Структура данных ядра ОС UNIX.

Рассмотрим основные механизмы защиты данных, реализованные в ОС UNIX.

При включении пользователя в число абонентов ему выдается регистрационное имя (идентификатор) для входа в систему и пароль, который служит для подтверждения идентификатора пользователя. В отдельных версиях ОС UNIX, помимо идентификатора и пароля, требуется ввод номера телефона, с которого выполняется подключение к системе. Администратор системы и пользователь могут изменить пароль командой passwd. При вводе этой команды ОС запрашивает ввод текущего пароля, а затем требует ввести новый пароль. Если предложенный пароль не удовлетворяет требования системы, то запрос на ввод пароля может быть повторен. Если предложенный пароль удовлетворителен, ОС просит ввести его снова с тем, чтобы убедиться в корректности ввода пароля.

Пользователи, которым разрешен вход в систему, перечислены в учетном файле пользователей /etc/passwd. Этот текстовый файл содержит следующие данные: имя пользователя, зашифрованный пароль, идентификатор пользователя, идентификатор группы, начальный текущий каталог и имя исполняемого файла, используемого в качестве интерпретатора команд. Пароль шифруется, как правило, с использованием DES-алгоритма.

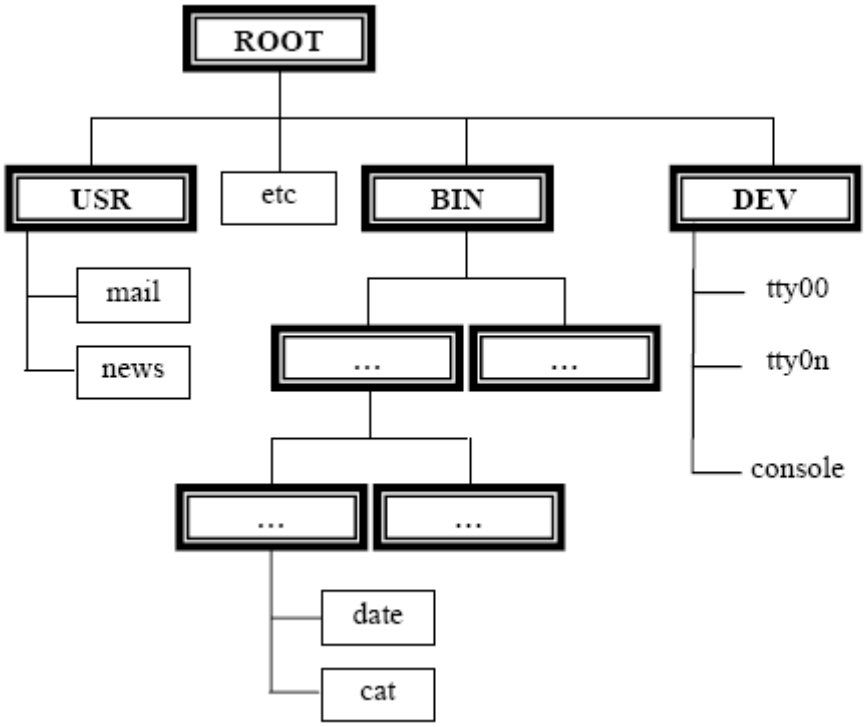

Рисунок 3.2 - Схема файловой системы ОС UNIX.

Операционная система UNIX поддерживает для любого файла комплекс характеристик, определяющих санкционированность доступа, тип файла, его размер и точное местоположение на диске. При каждом обращении к файлу система проверяет право пользоваться им. Операционная система UNIX допускает выполнение трех типов операций над файлами: чтение, запись и выполнение. Чтение файла означает, что доступно его содержимое, а запись – что возможны изменения содержимого файла. Выполнение приводит либо к загрузке файла в ОП либо к выполнению содержащихся в файле команд системного монитора Shell. Разрешение на выполнение каталога означает, что в нем допустим поиск с целью формирования полного имени на пути к файлу. Любой из файлов в ОС UNIX имеет определенного владельца и привязан к некоторой группе. Файл наследует их от процесса, создавшего файл. Пользователь и группа, идентификаторы которых связаны с файлом, считаются его владельцами.

Идентификаторы пользователя и группы, связанные с процессом, определяют его права при доступе к файлам. По отношению к конкретному файлу все процессы делятся на три категории:

- владелец файла (процессы, имевшие идентификатор пользователя, совпадающий с идентификатором владельца файла);
- члены группы владельца файла (процессы, имеющие идентификатор группы, совпадающий с идентификатором группы, которой принадлежит файл);
- прочие (процессы, не попавшие в первые две категории).

Владелец файла обладает одними привилегиями на доступ к нему, члены группы, в которую входит файл – другими, все остальные пользователи – третьими. Каждый файл содержит код защиты, который присваивается файлу при его создании. Код защиты располагается в индексном дескрипторе файла и

содержит десять символов, причем первый символ определяет тип файла, а последующие девять – право на доступ к нему. Три вида операций (чтение, запись и выполнение) и три категории (уровни привилегий на доступ: владельцев, групп и прочих пользователей) дают в совокупности девять возможных вариантов разрешений или запретов на доступ к файлу. Первые три символа определяют возможности чтения (*r),* записи *(w)* и выполнения *(e)* на уровне владельца, следующие три – на уровне группы, в которую входит владелец, и последние три – на уровне остальных пользователей. Наличие символов *r, w* и *e* указывает на соответствующее разрешение.

Если процесс требует доступа к файлу, то сначала определяется категория, в которую по отношению к этому файлу он попадает. Затем из кода защиты выбираются те три символа, которые соответствуют данной категории, и выполняется проверка: разрешен ли процессу требуемый доступ. Если доступ не разрешен, системный вызов, посредством которого процесс сделал запрос на доступ, отвергается ядром ОС.

По соглашению, принятому в ОС UNIX, привилегированный пользователь имеет идентификатор, равный нулю. Процесс, с которым связан нулевой идентификатор пользователя, считается привилегированным. Независимо от кода защиты файла привилегированный процесс имеет право доступа к файлу для чтения и записи. Если в коде защиты хотя бы одной категории пользователей (процессов) есть разрешение на выполнение файла, привилегированный процесс тоже имеет право выполнять этот файл.

С помощью специальных команд владелец файла (и привилегированный пользователь) может изменять распределение привилегий. Команда Change mode позволяет изменить код защиты, команда Change owner меняет право на владение файлом, а команда Change group – принадлежность к той или иной группе. Пользователь может изменять режимы доступа только для тех файлов, которыми он владеет.

Для защиты хранимых данных в составе ОС UNIX имеется утилита crypt, которая читает данные со стандартного ввода, шифрует их и направляет на стандартный вывод. Шифрование применяется при необходимости предоставления абсолютного права владения файлом.

Операционная система UNIX поддерживает три основных набора утилит копирования: программы volcopy/labelit, dump/restor и cpio. Программа volcopy целиком переписывает файловую систему, проверяя с помощью программы labelit соответствие меток требуемых томов. Программа dump обеспечивает копирование лишь тех файлов, которые были записаны позднее определенной даты (защита накоплением). Программа restor может анализировать данные, созданные программой dump, и восстанавливать отдельные файлы или всю файловую систему полностью. Программа cpio предназначена для создания одного большого файла, содержащего образ всей файловой системы или какой-либо ее части.

Для восстановления поврежденной, например, в результате сбоев в работе аппаратуры файловой системы используются программы fsck и fsdb.

За сохранность файловой системы, адаптацию программного обеспечения к конкретным условиям эксплуатации, периодическое копирование пользовательских файлов, восстановление потерянных данных и другие операции ответственность возложена на администратора системы.

В составе утилит ОС UNIX находится утилита cron, которая предоставляет возможность запускать пользовательские программы в определенные моменты (промежутки) времени и, соответственно, ввести временные параметры для ограничения доступа пользователей.

Для управления доступом в ОС UNIX также применяется разрешение установки идентификатора владельца. Такое разрешение дает возможность получить привилегии владельца файла на время выполнения соответствующей программы. Владелец файлов может установить такой режим, в котором другие пользователи имеют возможность назначать собственные идентификаторы режима.

Доступ, основанный на полномочиях, использует соответствие меток. Для этого вводятся метки объектов (файлов) и субъектов (процессов), а также понятия доминанты и равенства меток (для выражения отношения между метками). Создаваемый файл наследует метку от создавшего его процесса. Вводятся соотношения, определяющие права процессов по отношению к файлам.

Интерфейс дискреционной модели доступа существенно детализирует имеющиеся механизмы защиты ОС UNIX. Вводимые средства можно разделить на следующие группы:

− работа со списками доступа при дискреционной защите;

− проверка права доступа;

− управление доступом на основе полномочий;

− работа привилегированных пользователей.

В рамках проекта Posix создан интерфейс системного администратора. Указанный интерфейс определяет объекты и множества действий, которые можно выполнить над объектами. В качестве классов субъектов и объектов предложены пользователь, группа пользователей, устройство, файловая система, процесс, очередь, вход в очередь, машина, система, администратор, программное обеспечение и др. Определены атрибуты таких классов, операции над классами и события, которые могут с ними происходить.

3.3. Безопасность в NOVELL NETWARE

Авторизация доступа к данным сети. В NetWare реализованы три уровня защиты данных (рисунок 3.3).

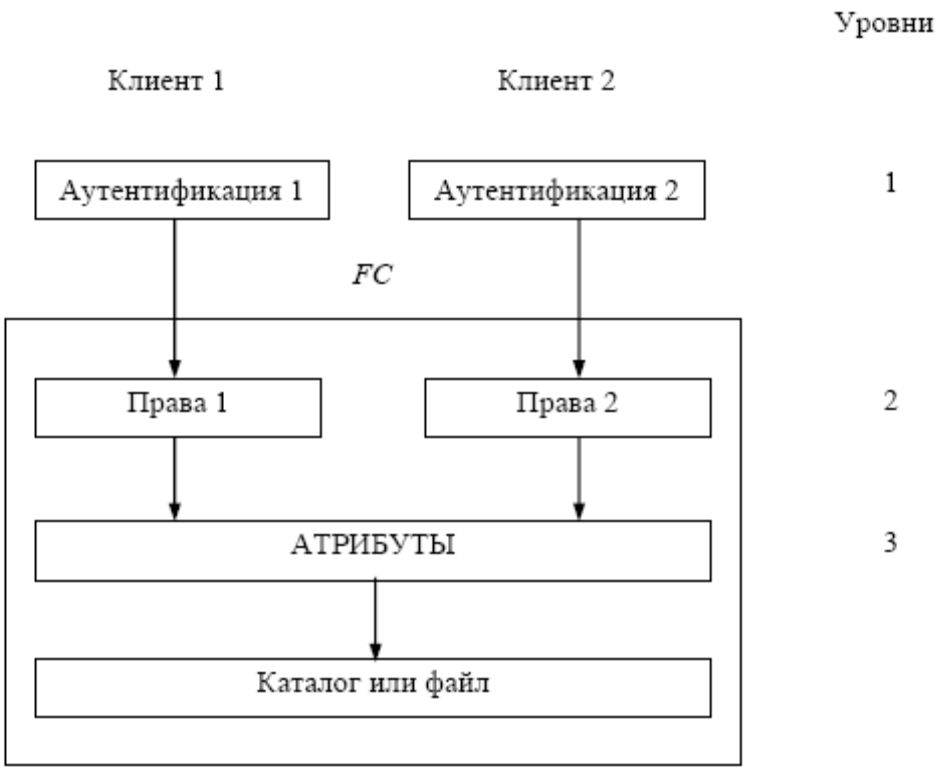

Рисунок 3.3 - Уровни защиты данных в NetWare.

Здесь под аутентификацией понимается:

− процесс подтверждения подлинности клиента при его подключении к сети;

− процесс установления подлинности пакетов, передаваемых между сервером и рабочей станцией.

Права по отношению к файлу (каталогу) определяют, какие операции пользователь может выполнить с файлом (каталогом). Администратор может для каждого клиента сети определить права по отношению к любому сетевому файлу или каталогу.

Атрибуты определяют некоторые системные свойства файлов (каталогов). Они могут быть назначены администратором для любого сетевого файла или каталога. Например, чтобы записать данные в файл, клиент должен:

− знать свой идентификатор и пароль для подключения к сети;

− иметь право записи данных в этот файл;

− файл должен иметь атрибут, разрешающий запись данных.

Следует отметить, что атрибуты файла (каталога) имеют более высокий приоритет, чем права пользователей по отношению к этому файлу.

Аутентификация пользователей при подключении к сети. Подключение к сети выполняется с помощью утилиты LOGIN.EXE. Эта программа передает на сервер идентификатор, введенный пользователем.

По этому идентификатору NetWare выполняет поиск соответствующего объекта пользователя в системной базе данных сетевых ресурсов. Если в базе данных хранится значение пароля для этого клиента, то NetWare посылает на рабочую станцию зашифрованный с помощью пароля открытый ключ

(симметричное шифрование). На рабочей станции этот ключ расшифровывается с помощью пароля, введенного пользователем, и используется для получения подписи запроса (пакета) к серверу о продолжении работы.

Сервер расшифровывает эту подпись с помощью закрытого ключа (асимметричное шифрование), проверяет ее и посылает подтверждение на рабочую станцию. В дальнейшем каждый пакет сообщения снабжается подписью, получаемой в результате кодирования открытом ключом контрольной суммы содержимого пакета и случайного числа Nonce. Это число генерируется для каждого сеанса. Поэтому подписи пакетов не повторяются для разных сеансов, даже если пользователь выполняет те же самые действия пакеты могут подписываться и рабочими станциями, и файловым сервером.

Для инициирования включения подписи в пакеты администратор может задать один из следующих уровней:

0 – сервер не подписывает пакет;

1 – сервер подписывает пакет, если этого требует клиент (уровень на станции больше или равен 2);

2 – сервер подписывает пакет, если клиент также способен это сделать (уровень на станции больше или равен 1);

3 – сервер подписывает пакет и требует этого от всех клиентов (иначе подключение к сети невозможно).

Права пользователей по отношению к каталогам и файлам. Права, которые могут быть предоставлены пользователю (или группе пользователей) по отношению к каталогу или файлу, перечислены в таблице 3.1.

Права и фильтры (маски) наследуемых прав назначаются администратором сети с помощью утилит NetWare. Но назначение прав для каждого пользователя по отношению ко всем требуемым файлам и каталогам – это утомительная задача. В NetWare предлагается механизм наследования прав. Прежде всего, введем некоторые определения.

Опекун (Trustees) – это пользователь (группа пользователей, другой объект), которому администратор с помощью утилиты (например, FILER) явно назначает права по отношению к какому-либо файлу или каталогу. Такие права называются опекунскими назначениями.

Фильтр наследуемых прав (IRF – Inherited Right Filter) – это свойство файла (каталога), определяющее, какие права данный файл (каталог) может унаследовать от родительского каталога. Фильтр назначается администратором с помощью утилиты (например, FILER).

Наследуемые права – права, передаваемые (распространяемые) от родительского каталога.

Эффективные права – права, которыми пользователь реально обладает по отношению к файлу или каталогу.

Права доступа к объектам NDS и их свойствам. Системная база данных сетевых ресурсов (СБДСР) представляет собой совокупность объектов, их свойств и значений этих свойств. В NetWare 4.x эта база данных называется NDS (NetWare

Directory Services), а в NetWare 3.x – Bindery. Объекты NDS связаны между собой в иерархическую структуру, которую часто называют деревом NDS. На верхних уровнях дерева (ближе к корню [Root]) описываются логические ресурсы, которые принято называть контейнерными объектами. На самом нижнем (листьевом) уровне располагаются описания физических ресурсов, которые называют оконечными объектами.

Таблица 3.1 - Список возможных прав по отношению к каталогу или файлу.

Право	Обозначение	Описание
Supervisor	*S*	Предоставляет все права по отношению к каталогу или файлу, включая возможность назначения этого права другим пользователям. Не блокируется фильтром наследуемых прав IRF. Это право не может быть удалено ниже по дереву каталогов
Read	*R*	Чтение существующего файла (просмотр содержимого текстового файла, просмотр записей в файле базы данных и т.д.)
Write	*W*	Запись в существующий файл (добавление, удаление частей текста, редактирование записей базы данных)
Create	*C*	Создание в каталоге новых файлов (и запись в них) и подкаталогов. На уровне файла позволяет восстанавливать файл, если он был ошибочно удален
Erase	*E*	Удаление существующих файлов и каталогов
Modify	*M*	Изменение имен и атрибутов (файлов и каталогов), но не содержимого файлов
File Scan	*F*	Просмотр в каталоге имен файлов и подкаталогов. По отношению к файлу – возможность видеть структуру каталогов от корневого уровня до этого файла (путь доступа)
AccessControl	*A*	Возможность предоставлять другим пользователям все права, кроме Supervisor. Возможность изменять фильтр наследуемых прав IRF

В качестве контейнерных объектов используются объекты типа [Root] (корень), C (страна), O (организация), OU (организационная единица). Оконечные объекты – это User (пользователь), Group (группа), NetWare Server (сервер NetWare), Volume (том файлового сервера), Directories (директория тома) и т.д. Оконечные объекты имеют единое обозначение – CN.

В NetWare 4.x разработан механизм защиты дерева NDS. Этот механизм очень похож на механизм защиты файловой системы, который был рассмотрен ранее. Чтобы облегчить понимание этого механизма, оконечный объект можно интерпретировать как файл, а контейнерный объект – как каталог, в котором могут быть созданы другие контейнерные объекты (как бы подкаталоги) и оконечные объекты (как бы файлы). На рисунке 3.4 представлена схема дерева NDS, где символами [Root], C, O, OU обозначены контейнерные объекты, а символами CN – оконечные объекты.

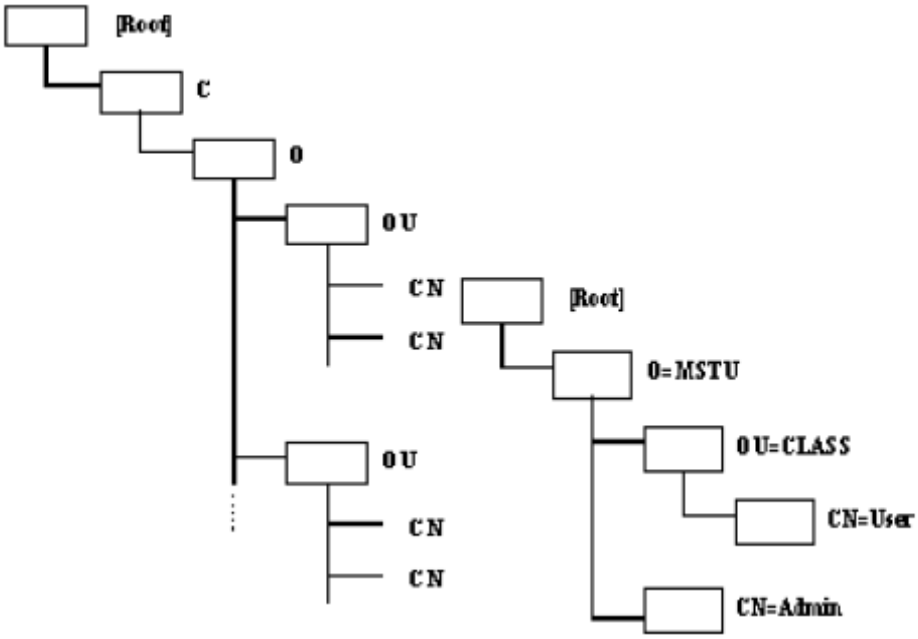

Рисунок 3.4 - Схема дерева NDS.

В отличие от файловой системы здесь права по отношению к какому-либо объекту можно предоставить любому контейнерному или оконечному объекту дерева NDS. В частности, допустимо рекурсивное назначение прав объекта по отношению к этому же объекту.

Права, которые могут быть предоставлены объекту по отношению к другому или тому же самому объекту, перечислены в таблице 3.2.

Таблица 3.2 - Список возможных прав по отношению к объекту.

Право	Обозначение	Описание
Supervisor	*S*	Гарантирует все привилегии по отношению к объекту и его свойствам. В отличие от файловой системы это право может быть блокировано фильтром наследуемых прав IRF, который может быть назначен для каждого объекта
Browse	*B*	Обеспечивает просмотр объекта в дереве NDS
Create	*C*	Это право может быть назначено только по отношению к контейнерному объекту (контейнеру). Позволяет создавать объекты в данном и во всех дочерних контейнерах
Delete	*D*	Позволяет удалять объект из дерева NDS
Rename	*R*	Позволяет изменять имя объекта

Администратор сети может для каждого объекта в дереве NDS определить значения свойств этого объекта. Для объекта User – это имя Login, требования к паролю, пароль пользователя, пользовательский сценарий подключения и т.д.

3.4 Контрольные вопросы

1. Дайте определение операционной системы.
2. Назовите основные типовые функциональные дефекты операционных систем.

3. Перечислите функции безопасности операционной системы Windows NT.

4. Назовите три способа делегирования административных полномочий в операционной системе Windows NT.

5. Как устроена организация работ в операционной системе UNIX.

6. Назовите основные механизмы защиты данных, реализованные в операционной системе UNIX.

7. Что понимается под аутентификацией в операционной системе NOVELL NETWARE?

8. Назовите права пользователей по отношению к каталогам и файлам в операционной системе NOVELL NETWARE.

4. Защита информации в компьютерных сетях

Межсетевой экран (МЭ) или брандмауэр (Firewall) – это средство защиты, которое можно использовать для управления доступом между надежной сетью и менее надежной.

Межсетевой экран – это не одна компонента, а стратегия защиты ресурсов организации, доступных из глобальной сети.

Основная функция МЭ – централизация управления доступом. Если удаленные пользователи могут получить доступ к внутренним сетям в обход МЭ, его эффективность близка к нулю. МЭ обычно используются для защиты сегментов локальной сети организации.

Межсетевые экраны обеспечивают несколько типов защиты:

− блокирование нежелательного трафика;

− перенаправление входного трафика только к надежным внутренним системам;

− сокрытие уязвимых систем, которые нельзя обезопасить от атак из глобальной сети другим способом;

− протоколирование трафика в и из внутренней сети;

− сокрытие информации (имен систем, топологии сети, типов сетевых устройств и внутренних идентификаторов пользователей, от внешней сети;

− обеспечение более надежной аутентификации, чем та, которую представляют стандартные приложения.

Как и для любого средства защиты, нужны определенные компромиссы между удобством работы и безопасностью. Прозрачность – это видимость МЭ как внутренним пользователям, так и внешним, осуществляющим взаимодействие через МЭ, который прозрачен для пользователей, если он не мешает им получить доступ к сети. Обычно МЭ конфигурируются так, чтобы быть прозрачными для внутренних пользователей сети (посылающим пакеты наружу), и, с другой стороны, МЭ конфигурируется так, чтобы быть непрозрачным для внешних пользователей, пытающихся получить доступ к внутренней сети извне. Это обычно обеспечивает высокий уровень безопасности и не мешает внутренним пользователям.

4.1 Методы установления подлинности в компьютерных сетях

Для того чтобы установить подлинность субъектов и объектов системы, все субъекты и объекты, зарегистрированные в системе, должны иметь уникальные имена-идентификаторы. Когда какой-либо субъект обращается к ресурсам системы, необходимо установить его подлинность, опознать его (процесс авторизации или аутентификации).

Установление подлинности субъекта (объекта) заключается в подтверждении того, что обратившийся субъект (вызываемый объект) является

именно тем, которому разрешено участвовать в данном процессе (выполнять действия).

В зависимости от сложности установления подлинности различают три основные группы операций: простое, усложненное и особое установление подлинности.

Простое установление подлинности сводится к сравнению предъявленного кода (характеристики) с эталонным кодом, который хранится в памяти устройства, выполняющего установление подлинности.

Усложненное установление подлинности требует от пользователя ввода дополнительной информации и осуществляется в режиме диалога.

Особое установление подлинности, кроме использования методов простого и усложненного установления подлинности, использует специальную совокупность опознавательных характеристик, которая выбирается для обеспечения надежного установления подлинности.

Для установления подлинности субъектов используются различные опознавательные характеристики.

В литературе описаны устройства установления подлинности субъектов в реальном масштабе времени по почерку, голосу и отпечаткам пальцев.

Установление подлинности по почерку производится, например, с помощью специальной ручки-датчика. При этом используются методы сопоставления контуров, анализа специфических штрихов и гистограмм.

При установлении подлинности по голосу используются следующие параметры: тембр, высота звука, акцент, интонация, сила звука и скорость речи, основано на спектральных методах и не зависит от содержания речи.

Установление подлинности по отпечаткам пальцев производится путем сличения предъявленных отпечатков пальцев с эталонными. Устройство использует методы сопоставления бинарных образов и проекций для характерных точек и направлений штрихов отпечатков пальцев.

Некоторые производители реализуют системы установления подлинности на базе пластиковых карт, на которые кодовая информация записывается и считывается лазерноголографическими методами. Такие карты могут использоваться в двух режимах: ключа и персонального идентификационного кода (ПИК). В режиме ключа карта служит для открывания специальных голографических электронно-механических замков, устанавливаемых на защищаемых объектах. В режиме ПИК карта используется для ограничения доступа к терминалам вычислительной системы и хранящимся в ней данным. Для этого на карту заносится ПИК пользователя, занимающий от 64 до 256 бит.

Методы паролирования требуют, чтобы пользователь ввел строку символов (пароль) для сравнения с эталонным паролем, хранящимся в памяти. При соответствии пароля эталонному пользователю разрешена работа с системой.

Метод простого пароля состоит во вводе пользователем одного пароля с клавиатуры. Метод выборки символов состоит в запросе системой определенных символов пароля, выбираемых случайным образом. Метод выборки символов не

позволяет нарушителю определить значение пароля по однократному наблюдению вводимых пользователем символов.

Метод паролей однократного использования предполагает наличие списка из N паролей, хранящегося в системе. При каждом обращении к системе пользователь вводит очередной пароль, который после окончания работы вычеркивается системой из списка. Основным недостатком рассмотренного метода является неоднозначность пароля.

Метод групп паролей основывается на том, что система для каждого пользователя может потребовать пароли из двух групп. Группы могут включать пароли, которые являются:

− ответами на общие для всех пользователей вопросы, например, имя, адрес, номер телефона и т.п.;

− ответами на вопросы, которые устанавливаются администратором системы при регистрации персонально для каждого пользователя для работы с системой, например, любимый цвет, девичья фамилия матери и т.п.

При каждом обращении пользователя система случайно выбирает по нескольку вопросов из каждой группы.

Метод функционального преобразования предполагает, что пользователю при регистрации для работы в системе сообщается некоторое преобразование, которое он может выполнить в уме. Для усложнения вскрытия пароля в методе функционального преобразования в качестве аргументов могут использоваться числа месяца, часы суток или их комбинации.

При работе с паролями должны соблюдаться следующие правила:

− пароли должны храниться в памяти только в зашифрованном виде;

− символы пароля при вводе их пользователем не должны появляться в явном виде;

− пароли должны периодически меняться;

− пароли не должны быть простыми.

Для проверки сложности паролей обычно используют специальные контроллеры паролей, которые позволяет проверить уязвимость паролей. Контроллер осуществляет попытки взлома пароля по следующей методике.

1. Проверка использования в качестве пароля входного имени пользователя, его инициалов и их комбинаций.

2. Проверка использования в качестве пароля слов из различных словарей (60 000 слов): мужские и женские имена (16 000 имен); названия стран и городов; имена персонажей мультфильмов, кинофильмов, научно – фантастических произведений и т.п.; спортивные термины (названия команд, имена спортсменов, спортивный жаргон и т.п.); числа (цифрами и прописью, например, 2000, TWELVE); строки букв и цифр (например, AA, AAA, AAAA и т.д.); библейские имена и названия; биологические термины; жаргонные слова и ругательства; последовательности символов в порядке их расположения на клавиатуре (например, QWERTY, ASDF, ZXCVBN и т.д.); имена компьютеров (из файла

/etc/hostc в ОС UNIX); персонажи и места действия из произведений Шекспира; часто употребляемые иностранные слова; названия астероидов.

3. Проверка различных перестановок слов из п. 2, включая: замену первой буквы на прописную; замену всех букв на прописные; инверсию всего слова; замену буквы О на цифру 0 и наоборот (цифру 1 на букву 1 и т.д.); превращение слов во множественное число.

Всего по пункту 3 контроллер осуществляет проверку на совпадение приблизительно с одним миллионом слов.

4. Проверка различных перестановок слов из п. 2, не рассмотренных в п. 3: замена одной строчной буквы на прописную (около 400 000 слов); замена двух строчных букв на прописные (около 1 500 000 слов); замена трех строчных букв на прописные и т.д.

5. Для иностранных пользователей проверка слов на языке пользователя.

6. Проверка пар слов.

Проведенные эксперименты показали, что данный контроллер позволил определить 10 % паролей из пяти символов, 35 % паролей из шести символов, 25 % паролей из семи символов и 23 % паролей из восьми символов.

Приведенные примеры позволяют сформулировать следующие способы снижения уязвимости паролей:

− не использовать в качестве пароля слова, проверяемые контроллером Кляйна;

− проверять пароли перед их использованием контроллерами паролей;

− часто менять пароли;

− при формировании пароля использовать знаки препинания и различные регистры;

− использовать не осмысленные слова, а наборы букв (например, первых букв какой-нибудь известной пользователю фразы).

Из примеров, приведенных при рассмотрении контроллера паролей, видно, что важнейшими характеристиками пароля являются его длина и период смены (или период жизни). Естественно, что чем больше длина пароля, тем больше усилий придется приложить нарушителю для его определения. Чем больше период жизни пароля, тем более вероятно его раскрытие.

Для случая, когда пользователь вводит пароль через удаленный терминал, можно применить формулу Андерсена: $4{,}32 * 104\ (vT)/(NP) < = As$, где v – скорость передачи данных через линию связи (в символах/мин); T – период времени, в течение которого могут быть предприняты попытки отгадывания пароля (в месяцах при работе 24 ч/сутки); N – число символов в каждом передаваемом сообщении при попытке получить доступ к системе; P – вероятность подбора нарушителем правильного пароля; A – число символов в алфавите, из которого составляется пароль; S – длина пароля (в символах).

Также одной из возможных стратегий действий нарушителя в ИВС является подключение к каналу связи. В этом случае нарушитель может имитировать механизм установления подлинности, что позволит ему получить пароль

пользователя и доступ к его данным. Для предупреждения подобных действий нарушителя пользователь должен убедиться в подлинности системы, с которой он начинает работать. Одним из методов решения этой задачи является так называемая процедура «рукопожатия». Для осуществления процедуры «рукопожатия» выбирается нетривиальное преобразование вида $y = f(x, k)$, где x – аргумент; k – коэффициент. В качестве аргумента преобразования можно использовать элементы даты, времени и т.п. Преобразование y известно только пользователям и ЭВМ и должно сохраняться в тайне. Пользователь вместе с запросом на подключение к системе посылает выбранное им значение x. Получив значение x вместе с идентификатором пользователя, система вычисляет $y = f(x, k)$ и посылает его пользователю вместе с запросом о вводе пароля. Пользователь вычисляет или имеет вычисленное заранее значение y. Если значения y, полученные пользователем и системой, совпадают, то режим опознания системы заканчивается, и пользователь может вводить пароль. После подтверждения правильности пароля пользователя считается, что «рукопожатие» состоялось.

Аналогичным образом осуществляется установление подлинности ЭВМ ИВС при необходимости обмена данных между ними. Проверка подлинности взаимодействующих субъектов и объектов системы может производиться не только перед началом сеанса, но и в ходе него. Такие проверки могут осуществляться через определенные промежутки времени, после определенного количества переданных данных и т.п.

После положительного установления подлинности пользователя (и системы со стороны пользователя) система должна осуществлять постоянную проверку полномочий поступающих от субъектов запросов. Проверка полномочий заключается в определении соответствия запроса субъекта предоставленным ему правам доступа к ресурсам. Такую процедуру часто называют «контроль полномочий» или «контроль доступа». Проверка полномочий основывается на различных методах разграничения доступа, которые были рассмотрены ранее.

Также и регистрация (протоколирование) обращений к защищенным ресурсам системы позволяет должностному лицу, ответственному за информационную безопасность, следить за использованием ресурсов и оперативно принимать меры по перекрытию обнаруженных каналов утечки данных. Все обращения к ресурсам системы должны фиксироваться в регистрационном журнале.

В регистрационный журнал обычно заносятся следующие данные:

− обращения (доступы) к защищаемым ресурсам;

− отказы в доступе;

− изменения полномочий;

− случаи неиспользования пользователями разрешенных запросов;

− изменения содержания памяти ЭВМ, производимые пользователями;

− любые подозрительные действия.

В системе должна быть предусмотрена возможность выводить содержимое регистрационного журнала на экран терминала и печатающее устройство, причем

выводимую информацию необходимо сортировать по пользователям, терминалам, датам, идентификаторам заданий, элементам данных и т.п.

Следует отметить, что регистрационный журнал может быть также использован для решения следующих задач:

− настройка системы (по частоте обращений к различным ресурсам);

− помощь пользователям в случае их непреднамеренных ошибок;

− изменение полномочий пользователей (если пользователи часто совершают ошибки, либо вообще никогда не обращаются к некоторым ресурсам);

− возврат системы в исходное состояние для восстановления;

− психологическое воздействие на потенциальных нарушителей.

Приведенный перечень задач, для решения которых может быть использован регистрационный журнал, еще раз подтверждает необходимость комплексного применения всех средств и механизмов защиты для обеспечения безопасности данных.

Реагирование на несанкционированные действия включает в себя:

− сигнализацию о НСД;

− блокировку (отключение терминала, группы терминалов, элементов ИВС и т.п.);

− задержку в работе;

− отказ в запросе;

− имитацию выполнения запрещенного действия для определения места подключения нарушителя и характера его действий.

Реагирование на НСД может осуществляться автоматически и с участием должностного лица, ответственного за информационную безопасность.

4.2 Многоуровневая защита компьютерных сетей

4.2.1 Аутентификация

Межсетевые экраны (МЭ) на основе маршрутизаторов не обеспечивают аутентификации пользователей. МЭ, в состав которых входят прокси-сервера, обеспечивают следующие типы аутентификации.

Имя/пароль – это самый плохой вариант, так как эта информация может быть перехвачена в сети или получена путем подглядывания за ее вводом из-за спины и еще тысячей других способов.

Одноразовые пароли – используют программы или специальные устройства для генерации нового пароля для каждого сеанса. Это означает, что старые пароли не могут быть повторно использованы, если они были перехвачены в сети или украдены другим способом.

Электронные сертификаты – используют шифрование с открытыми ключами.

4.2.2 Маршрутизация и прокси-сервера

В политике безопасности должно быть отражено, может ли МЭ маршрутизировать пакеты или они должны передаваться прокси-серверам. Тривиальным случаем МЭ является маршрутизатор, который может выступать в роли устройства для фильтрации пакетов. Все, что он может – только маршрутизировать пакеты. А прикладные шлюзы, наоборот, не могут быть сконфигурированы для маршрутизации трафика между внутренним и внешним интерфейсами МЭ, так как это может привести к обходу средств защиты. Все соединения между внешними и внутренними хостами должны проходить через прикладные шлюзы (прокси-сервера).

Маршрутизация источника – это механизм маршрутизации, посредством которого путь к машине-получателю пакета определяется отправителем, а не промежуточными маршрутизаторами. Маршрутизация источника может быть использована для атаки на хост. Если атакующий знает, что ваш хост доверяет какому-нибудь другому хосту, то маршрутизация источника может быть использована для создания впечатления, что пакеты атакующего приходят от доверенного хоста. Поэтому из-за такой угрозы безопасности маршрутизаторы с фильтрацией пакетов обычно конфигурируются так, чтобы отвергать пакеты с опцией маршрутизации источника. Поэтому сайт, желающий избежать проблем с маршрутизацией источника, обычно разрабатывает политику, в которой их маршрутизация запрещена.

Фальсификация IP-адреса имеет место, когда атакующий маскирует свою машину под хост в сети объекта атаки (то есть пытается заставить систему защиты думать, что пакеты приходят от доверенной машины во внутренней сети). Политика в отношении маршрутизации пакетов должна быть четкой, чтобы можно было корректно построить обработку пакетов, если есть проблемы с безопасностью. Необходимо объединить аутентификацию на основе адреса отправителя с другими способами, чтобы защитить сеть от атак подобного рода.

4.2.3 Межсетевые экраны

Существует несколько различных реализаций сетевых экранов (брандмауэров), которые могут быть созданы разными путями. Далее будет приведена краткая характеристика нескольких архитектур брандмауэров и их применимость к средам с низким, средним и высоким рискам.

Межсетевые экраны с фильтрацией пакетов используют маршрутизаторы с правилами фильтрации пакетов для предоставления или запрещения доступа на основе адреса отправителя, адреса получателя и порта. Они обеспечивают минимальную безопасность за низкую цену, и это может оказаться приемлемым для среды с низким риском. Они являются быстрыми, гибкими и прозрачными. Правила фильтрации часто нелегко администрировать, но имеется ряд средств для упрощения задачи создания и поддержания правил.

Шлюзы с фильтрацией имеют свои недостатки, включая следующие:

- адреса и порты отправителя и получателя, содержащиеся в заголовке IP-пакета, единственная информация, доступная маршрутизатору при принятии решения: разрешать или запрещать доступ трафика во внутреннюю сеть;
- они не защищают от фальсификации IP- и DNS-адресов;
- атакующий получит доступ ко всем хостам во внутренней сети после того, как ему был предоставлен доступ МЭ;
- усиленная аутентификация пользователя не поддерживается некоторыми шлюзами с фильтрацией пакетов;
- практически отсутствуют средства протоколирования доступа к сети.

Прикладной шлюз использует программы (называемые прокси-серверами), запускаемые на МЭ. Эти прокси-сервера принимают запросы извне, анализируют их и передают безопасные запросы внутренним хостам, которые предоставляют соответствующие сервисы. Прикладные шлюзы могут обеспечивать такие функции, как аутентификация пользователей и протоколирование их действий.

Прикладной шлюз считается самым безопасным типом МЭ. При этом он имеет ряд преимуществ:

− может быть сконфигурирован как единственный хост, видимый из внешней сети, что потребует осуществлять все внешние соединения через него;

− использование прокси-серверов для различных сервисов предотвращает прямой доступ к этим сервисам, защищая от атак небезопасные или плохо сконфигурированные внутренние хосты;

− с помощью прикладных шлюзов может быть реализована усиленная аутентификация;

− прокси-сервера могут обеспечивать детальное протоколирование на прикладном уровне.

Межсетевые экраны прикладного уровня должны конфигурироваться так, чтобы весь выходящий трафик казался исходящим от МЭ. Таким образом будет запрещен прямой доступ ко внутренним сетям. Все входящие запросы различных сетевых сервисов, таких как Telnet, FTP, HTTP, RLOGIN, и т.д., независимо от того, какой внутренний хост запрашивается, должны проходить через соответствующий прокси-сервер на МЭ.

4.3 Контрольные вопросы

1. Что такое межсетевой экран?
2. Что такое процесс авторизации?
3. В чем заключается метод групп паролей?
4. В чем заключается метод простого пароля?
5. Приведите примеры действий, позволяющих снизить уязвимость паролей.
6. Дайте определение маршрутизации источника.
7. Каких видов бывают шлюзы?

5 Защита от компьютерных инфекций

5.1 Классификация компьютерных вирусов

Информационные инфекции специфически ориентированы и обладают определенными чертами: противоправны (незаконны), способны самовосстанавливаться и размножаться, а также имеют определенный инкубационный период – замедленное время начала действия. Информационные инфекции имеют злонамеренный характер: их действия могут иметь деструктивный результат (уничтожения набора данных), реже физическое уничтожение (резкое включение и выключение дисковода), сдерживающее действие (переполнение канала ввода-вывода, памяти), или просто видоизменяющее влияние на работу программ. Самовосстановление и размножение приводит к заражению других программ и распространению по линиям связи. Замедленное действие проявляется в том, что работа программы начинается на определенных условиях: дата, час, продолжительность, наступление события и т.д.

В зависимости от механизма действия информационные инфекции делятся на:

- вирус - представляет собой программу, которая обладает способностью размножаться и самовостановливаться;
- логические бомбы - представляют собой программы или их части, резидентно находящиеся в ИВС и запускаемые всякий раз, когда выполняются определенные условия;
- троянский конь – это программа, полученная путем явного изменения или добавления команд в программы пользователя и способные вмешиваться в процесс обработки информации;
- червь - представляет собой паразитный процесс, который потребляет (истощает) ресурсы системы и способен перемещаться в ИВС или сети и самовоспроизводить копии.

Вирусы можно разделить на классы по следующим основным признакам:

• среда обитания;
• операционная система (ОС);
• особенности алгоритма работы;
• деструктивные возможности.

В зависимости от среды обитания вирусы можно разделить на:

– файловые;
– загрузочные;
– макровирусы;
– сетевые.

Файловые вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники (вирусы-компаньоны), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний, например файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, имеют довольно сложный алгоритм работы и часто применяют оригинальные методы проникновения в систему и маскировки. Пример такого сочетания – сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Заражаемая операционная система является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких ОС – DOS, Windows 95/98/Me/NT/2000/XP, OS/2, UNIX и т. д. Макровирусы заражают файлы форматов Word, Excel, других приложений Microsoft Office. Загрузочные вирусы ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Среди особенностей алгоритма работы вирусов выделяются следующие:

- резидентность;
- использование «стелс» - алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения ОС к объектам заражения и внедряются в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.

Резидентными можно считать макровирусы, поскольку они также присутствуют в памяти компьютера в течение всего времени работы зараженного редактора. При этом роль ОС берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

Использование «стелс» - алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным «стелс» - алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов и затем «стелс» - вирусы либо временно лечат их, либо подставляют

вместо себя незараженные участки информации. В случае макровирусов наиболее популярный способ – запрет вызовов меню просмотра макросов.

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру обнаружения вируса. Полиморфик – вирусы (polymorphic) достаточно трудно поддаются обнаружению; они не имеют сигнатур, т.е. не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик – вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса на разных ключах и модификациями программы – расшифровщика.

Различные нестандартные приемы часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС, защитить от обнаружения свою резидентную копию (вирусы TPVO, Trout2), затруднить лечение от вируса (например, помешают свою копию в Flash-BIOS) и т.д.

По деструктивным возможностям вирусы можно разделить на:

- безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске при своем распространении);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами;
- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- очень опасные – в алгоритм их работы заведомо заложены деструктивные процедуры (вызывающие потерю программ, уничтожение данных, или способствующие быстрому износу движущихся частей механизмов).

Прочие вредные программы. К вредным программам помимо вирусов относятся также «троянские кони», «логические бомбы», intended-вирусы, конструкторы вирусов и полиморфик–генераторы.

Следует отметить также «злые шутки» (hoax). К ним относятся программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К «злым шуткам» относятся, например, программы, которые «пугают» пользователя сообщениями о форматировании диска, определяют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т.д.

Intended-вирусы. К таким вирусам относятся программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок.

К категории intended-вирусов также относятся вирусы, которые по приведенным выше причинам размножаются только один раз из «авторской» копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению.

Конструкторы вирусов – это утилита, предназначенная для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS,

Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.

Некоторые конструкторы снабжены стандартным оконным интерфейсом, позволяющим при помощи системы меню выбрать тип вируса, поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса, и т. п.

Прочие конструкторы не имеют интерфейса и считывают информацию о типе вируса из конфигурационного файла.

Полиморфные генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т.е. открытия, закрытия и записи в файлы, чтения и записи секторов и т.д.

Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Приведенное деление не свободно от недостатков, поскольку производится по единственному критерию – возможности обнаруживать вирус по коду расшифровщика при помощи стандартного приема вирусных масок.

Если произвести деление на уровни с точки зрения антивирусов, использующих системы автоматического расшифрования кода вируса (эмуляторы), то деление на уровни будет зависеть от сложности эмуляции кода вируса. Возможно, более объективным является деление, в котором помимо критерия вирусных масок участвуют и другие параметры:

- степень сложности полиморфик-кода (процент от всех инструкций процессора, которые могут встретиться в коде расшифровщика);
- использование антиэмуляторных приемов;
- постоянство алгоритма расшифровщика;
- постоянство длины расшифровщика.

5.2 Защита от компьютерных вирусов

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Различают следующие виды антивирусных программ:

− программы-детекторы;
− программы-доктора или фаги;
− программы-мониторы (ревизоры);
− программы фильтры;
− программы-вакцины или иммунизаторы.

Программы-детекторы (сканеры) осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в

оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам.

Во многих сканерах используются также алгоритмы эвристического сканирования, т.е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения («возможно, заражен» или «не заражен») для каждого проверяемого объекта.

К достоинствам сканеров относится их универсальность, к недостаткам – размеры антивирусных баз, которые сканерам приходится «таскать за собой», и относительно небольшая скорость поиска вирусов.

Программы-доктора или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известными полифагами являются программы Aidstest, Scan, Norton AntiViris и Doctor Web.

Программы-ревизоры (CRC-сканеры) относятся к самым надежным средствам защиты от вирусов. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие «антистелс» - алгоритмы, являются довольно сильным оружием против вирусов: практически 100 % вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут детектировать вирус в новых файлах, поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту «слабость» CRC-сканеров, заражают только вновь создаваемые файлы и остаются невидимыми для CRC-сканеров. К числу программ-ревизоров относится, например, известная в России программа ADinf фирмы «Диалог-наука».

Антивирусные мониторы – это резидентные программы, перехватывающие вирусоопасные ситуации и сообщающие об этом пользователю. К вирусоопасным

относятся вызовы на открытие для записи в выполняемые файлы запись в загрузочные секторы дисков или MBR винчестера, попытки программ остаться резидентно и т.д., т.е. вызовы, которые характерны для вирусов в моменты их размножения.

К достоинствам мониторов относится их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно «выползает неизвестно откуда». К недостаткам относятся существование путей обхода защиты монитора и большое количество ложных срабатываний.

Вакцины или иммунизаторы – это резидентные программы, предоставляющие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса. Первые обычно записываются в конец файлов (по принципу файлового вируса и при запуске файла каждый раз проверяют его на изменение. Недостаток у таких иммунизаторов всего один, но он летален: абсолютная неспособность сообщить о заражении «стелс» - вирусом. Поэтому такие иммунизаторы, как и мониторы, практически не используются в настоящее время.

Второй тип иммунизации защищает систему от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные. Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса, при запуске вирус натыкается на нее и считает, что система уже заражена.

Качество антивирусной программы определяется по следующим позициям, приведенным в порядке убывания их важности:

1. Надежность и удобство работы – отсутствие зависаний антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.

2. Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов документов/таблиц (MS Word, Excel, Office), упакованных и архивированных файлов. Отсутствие «ложных срабатываний». Возможность лечения зараженных объектов (для сканеров – периодичность появления новых версий, т.е. скорость настройки сканера на новые вирусы).

3. Существование версий антивируса под все популярные платформы (DOS, Windows 95/98/NT/Me/2000/XP, Novell NetWare, OS/2, Alpha, UNIX, Linux и т. д.), присутствие не только режима «сканирование по запросу», но и «налету».

5.3 Контрольные вопросы

1. Перечислите виды компьютерных вирусов.
2. Перечислите виды компьютерных вирусов опираясь на особенности их алгоритма работы

3. Назовите виды компьютерных вирусов по их деструктивным возможностям.
4. Что такое конструкторы вирусов?
5. Перечислите уровни полиморфизма.
6. Перечислите способы защиты от компьютерных вирусов.

6 Комплексный подход к защите информации

6.1 Классификация информационных объектов

Классификация по требуемой степени безотказности.

Безотказность, или надежность доступа к информации, является одной из категорий информационной безопасности. Предлагается следующая схема классификации информации на 4 уровня безотказности на рисунке 6.1.

Параметр	класс 0	класс 1	класс 2	класс 3
Максимально возможное непрерывное время отказа	1 неделя	1 сутки	1 час	1 час
В какое время отказа не может превышать указанное выше?	в рабочее	в рабочее	в рабочее	24 часа в сутки
Средняя вероятность доступности данных в произвольный момент времени	80%	95%	99.5%	99.9%
Среднее максимальное время отказа	1 день в неделю	2 часа в неделю	20 минут в неделю	12 минут в месяц

Рисунок 6.1 - Схема классификации информации
на 4 уровня безотказности.

Класс	Тип информации	Описание	Примеры
0	открытая информация	общедоступная информация	информационные брошюры, сведения публиковавшиеся в СМИ
1	внутренняя информация	информация, недоступная в открытом виде, но не несущая никакой опасности при ее раскрытии	финансовые отчеты и тестовая информация за давно прошедшие периоды, отчеты об обычных заседаниях и встречах, внутренний телефонный справочник фирмы
2	конфиденциальная информация	раскрытие информации ведет к значительным потерям на рынке	реальные финансовые данные, планы, проекты, полный набор сведений о клиентах, информация о бывших и нынешних проектах с нарушениями этических норм
3	секретная информация	раскрытие информации приведет к финансовой гибели компании	(зависит от ситуации)

Рисунок 6.2 - Схема классификации информации на 4 класса
по уровню ее конфиденциальности.

Классификация по уровню конфиденциальности.

Уровень конфиденциальности информации является одной из самых важных категорий, принимаемых в рассмотрение при создании определенной политики безопасности учреждения. Предлагается следующая схема классификации информации на 4 класса по уровню ее конфиденциальности представленная на рисунке 6.2.

Требования по работе с конфиденциальной информацией.

При работе с информацией 1-го класса конфиденциальности рекомендуется выполнение следующих требований:

- осведомление сотрудников о закрытости данной информации,
- общее ознакомление сотрудников с основными возможными методами атак на информацию,
- ограничение физического доступа
- полный набор документации по правилам выполнения операций с данной информацией.

При работе с информацией 2-го класса конфиденциальности к перечисленным выше требованиям добавляются следующие:

- расчет рисков атак на информацию,
- поддержания списка лиц, имеющих доступ к данной информации,
- по возможности выдача подобной информации по расписку (в т.ч. электронную),
- автоматическая система проверки целостности системы и ее средств безопасности,
- надежные схемы физической транспортировки,
- обязательное шифрование при передаче по линиям связи,
- схема бесперебойного питания ЭВМ.

При работе с информацией 3-го класса конфиденциальности ко всем перечисленным выше требованиям добавляются следующие:

- детальный план спасения либо надежного уничтожения информации в аварийных ситуациях (пожар, наводнение, взрыв),
- защита ЭВМ либо носителей информации от повреждения водой и высокой температурой,
- криптографическая проверка целостности информации.

6.2 Построение системы безопасности на основе политики ролей

Функции каждого человека, так или иначе связанного с конфиденциальной информацией на предприятии, можно классифицировать и в некотором приближении формализовать. Подобное общее описание функций оператора носит название роли. В зависимости от размеров предприятия некоторые из

перечисленных ниже ролей могут отсутствовать вообще, а некоторые могут совмещаться одним и тем же физическим лицом.

Специалист по информационной безопасности играет основную роль в разработке и поддержании политики безопасности предприятия. Он проводит расчет и перерасчет рисков, ответственен за поиск самой свежей информации об обнаруженных уязвимостях в используемом в фирме программном обеспечении и в целом в стандартных алгоритмах.

Владелец информации – лицо, непосредственно работающее с данной информацией, (не нужно путать с оператором). Зачастую только он в состоянии реально оценить класс обрабатываемой информации, а иногда и рассказать о нестандартных методах атак на нее (узкоспецифичных для этого вида данных). Владелец информации не должен участвовать в аудите системы безопасности.

Поставщик аппаратного и программного обеспечения. Обычно стороннее лицо, которое несет ответственность перед фирмой за поддержание должного уровня информационной безопасности в поставляемых им продуктов.

Разработчик системы и/или программного обеспечения играет основную роль в уровне безопасности разрабатываемой системы. На этапах планирования и разработки должен активно взаимодействовать со специалистами по информационной безопасности.

Линейный менеджер или менеджер отдела является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача – своевременно и качественно инструктировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за ее их выполнением на рабочих местах. Линейные менеджеры должны быть осведомлены о всей политике безопасности предприятия, но доводить до сведения подчиненных только те ее аспекты, которые непосредственно их касаются.

Операторы – лица, ответственные только за свои поступки. Они не принимают никаких решений и ни за кем не наблюдают. Они должны быть осведомлены о классе конфиденциальности информации, с которой они работают, и о том, какой ущерб будет нанесен фирме при ее раскрытии.

Аудиторы – внешние специалисты или фирмы, нанимаемые предприятием для периодической (довольно редкой) проверки организации и функционирования всей системы безопасности.

6.3 Создание политики информационной безопасности

Существуют две системы оценки текущей ситуации в области информационной безопасности на предприятии. Они получили образные названия "исследование снизу вверх" и "исследование сверху вниз". Первый метод достаточно прост, требует намного меньших капитальных вложений, но и обладает меньшими возможностями. Он основан на известной схеме : "Вы – злоумышленник. Ваши действия?". То есть служба информационной

безопасности, основываясь на данных о всех известных видах атак, пытается применить их на практике с целью проверки, а возможно ли такая атака со стороны реального злоумышленника.

Метод "сверху вниз" представляет собой, наоборот, детальный анализ всей существующей схемы хранения и обработки информации. Первым этапом этого метода является, как и всегда, определение, какие информационные объекты и потоки необходимо защищать. Далее следует изучение текущего состояния системы информационной безопасности с целью определения, какие из классических методик защиты информации уже реализованы, в каком объеме и на каком уровне. На третьем этап производится классификация всех информационных объектов на классы в соответствии с ее конфиденциальностью, требованиями к доступности и целостности (неизменности).

Далее проводится оценка ущерба при раскрытии или иных атак на каждый конкретный информационный объект. Этот этап носит название "вычисление рисков". В первом приближении риском называется произведение "возможного ущерба от атаки" на "вероятность такой атаки". Существует множество схем вычисления рисков, остановимся на одной из самых простых.

Ущерб от атаки может быть представлен неотрицательным числом в приблизительном соответствии с рисунком 6.3.

Величина ущерба	Описание
0	Раскрытие информации принесет ничтожный моральный и финансовый ущерб фирме
1	Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение фирмы на рынке не затронуты
2	Финансовые операции не ведутся в течение некоторого времени, за это время фирма терпит убытки, но ее положение на рынке и количество клиентов изменяются минимально
3	Значительные потери на рынке и в прибыли. От фирмы уходит ощутимая часть клиентов
4	Потери очень значительны, фирма на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы.
5	Фирма прекращает существование

Рисунок 6.3 - Ущерб от атаки.

Уровень появления атаки представляется неотрицательным числом в приблизительном соответствии с рисунком 6.4.

Уровень появления	Средняя частота появления
0	Данный вид атаки отсутствует
1	реже, чем раз в год
2	около 1 раза в год
3	около 1 раза в месяц
4	около 1 раза в неделю
5	практически ежедневно

Рисунок 6.4 - Уровень появления атаки.

Необходимо отметить, что классификацию ущерба, наносимого атакой, должен оценивать владелец информации, или работающий с нею персонал. А вот оценку вероятности появления атаки лучше доверять техническим сотрудникам фирмы.

Следующим этапом составляется таблица рисков предприятия представленная на рисунке 6.5.

Описание атаки	Ущерб	Уровень появления	Риск (=Ущерб * Уровень появления)
Спам (переполнение почтового ящика)	1	4	4
Копирование жесткого диска из центрального офиса	3	1	3
...	...	...	2
Итого:			9

Рисунок 6.5 - Риски предприятия.

На этапе анализа таблицы рисков задаются некоторым максимально допустимым риском, например значением 7. Сначала проверяется каждая строка таблицы на не превышение риска этого значения. Если такое превышение имеет место, значит, данная строка – это одна из первоочередных целей разработки политики безопасности. Затем производится сравнение удвоенного значения (в нашем случае 7*2=14) с интегральным риском (ячейка "Итого"). Если интегральный риск превышает допустимое значение, значит, в системе набирается множество мелких огрешностей в системе безопасности, которые в сумме не дадут предприятию эффективно работать. В этом случае из строк выбираются те, которые дают самый значительный вклад в значение

интегрального риска и производится попытка их уменьшить или устранить полностью.

На самом ответственном этапе производится собственно разработка политики безопасности предприятия, которая обеспечит надлежащие уровни как отдельных рисков, так и интегрального риска. При ее разработке необходимо, однако, учитывать объективные проблемы, которые могут встать на пути реализации политики безопасности. Такими проблемами могут стать законы страны и международного сообщества, внутренние требования корпорации, этические нормы общества.

После описания всех технических и административных мер, планируемых к реализации, производится расчет экономической стоимости данной программы. В том случае, когда финансовые вложения в программу безопасности являются неприемлемыми или просто экономически невыгодными по сравнению с потенциальным ущербом от атак, производится возврат на уровень, где мы задавались максимально допустимым риском 7 и увеличение его на один или два пункта.

Завершается разработка политики безопасности ее утверждением у руководства фирмы и детальным документированием. За этим должна следовать активная реализация всех указанных в плане компонентов. Перерасчет таблицы рисков и, как следствие, модификация политики безопасности фирмы чаще всего производится раз в два года.

6.4 Методы обеспечения безотказности

Методы поддержания безотказности являются смежной областью в схемах комплексной информационной безопасности предприятия. Основным методом в этой сфере является внесение избыточности. Она может реализовываться в системе на трех уровнях: уровне данных (или информации), уровне сервисов (или приложений) и уровне аппаратного обеспечения.

Внесение избыточности на уровне данных практикуется достаточно давно: это резервное копирование и помехоустойчивое кодирование. Резервное копирование выполняется обычно при хранении информации на современных запоминающих устройствах (поскольку для них в аварийной ситуации характерен выход из строя больших блоков данных целиком – трудновосстановимое с помощью помехоустойчивого кодирования повреждение). А вот использование кодов с обнаружением и некоторым потенциалом для исправления ошибок получило широкое применение в средствах телекоммуникации.

Внесение избыточности на уровне приложений используется гораздо реже. Однако, многие, особенно сетевые, службы изначально поддерживают возможность работы с резервным или вообще с неограниченным, заранее неизвестным количеством альтернативных служб. Введение такой возможности рекомендуется при разработке программного обеспечения, однако, сам процесс автоматического переключения на альтернативную службу должен

подтверждаться криптографическим обменом первоначальной (установочной) информацией. Это необходимо делать для того, чтобы злоумышленник не мог, выведя из строя реальный сервис, навязать Вашей программе свой сервис с фальсифицированной информацией.

Внесение избыточности на аппаратном уровне реализуется обычно в отношении периферийных устройств (накопители на гибких и жестких дисках, сетевые и видео- адаптеры, мониторы, устройства ввода информации от пользователя). Это связано с тем, что дублирование работы основных компонентов ЭВМ (процессора, ОЗУ) гораздо проще выполнить, установив просто полноценную дублирующую ЭВМ с теми же функциями. Для автоматического определения работоспособности ЭВМ в программное обеспечение встраиваются либо 1) проверка контрольных сумм информации, либо 2) тестовые примеры с заведомо известным результатом, запускаемые время от времени, либо 3) монтирование трех и более дублирующих устройств и сверка их выходных результаты по мажоритарному правилу (каких результатов больше – те и есть правильные, а машины, выдавшие не такие результаты, выведены из строя).

6.5 Контрольные вопросы

1. Перечислите классификацию информационных объектов.
2. Перечислите особенности ролей аудитор и оператор.
3. Какие бывают методы обеспечения безотказности?

7 Правовое регулирование в области безопасности информации

Конец 20-го и начало 21-го веков характеризуется стремительным развитием компьютерных и информационных технологий. В результате их применения в различных сферах жизни, человечество вступило в новую эру – эру информатизации. Ныне компьютер является необходимым средством практически во всех областях человеческой жизни. В результате зависимость человека и общества от компьютерных технологий постоянно растет. Компьютер становится необходимым инструментом не только в производстве и науке, но и в домашних условиях. Это так же является базой для возникновения нового рода преступлений – преступлений в сфере информационных технологий (ИТ). Это преступления тем или иным образом связанные с компьютером, ущемляющие права пользователя, распространение заведомо ложной и опасной информации, способной нанести вред различным ИС или государству. Таким образом, проблема правового обеспечения защиты информации становится актуальной для государства и общества в целом.

Ни для кого не секрет, что преступность осваивает новые технологии гораздо быстрее, чем правоохранительные органы. И некоторое время пользуется ими абсолютно безнаказанно, так как если возникает деяние, не предусмотренное законодательством, то преступлением его считать нельзя. Обычно между возникновением такого деяния и признанием его преступлением проходит слишком много времени, чтобы реакцию законодателей можно было назвать своевременной.

В связи с проблемами, рассмотренными выше, необходимо уделять значительно большее внимание ИТ - преступлениям. И разрабатывать законодательно-правовую базу для пресечения не только преступной деятельности по уже известным схемам, но и процесса создания новых видов преступлений.

7.1 Государственная политика РФ в области безопасности информационных технологий

В Российской Федерации позиция государства отражена в документе «Доктрина информационной безопасности Российской Федерации», утвержденном президентом 9 сентября 2000 года. Согласно тексту доктрины, она развивает концепцию национальной безопасности применительно к информационной сфере и служит основой для трех направлений: формирования государственной политики в области обеспечения информационной безопасности РФ; подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности РФ; и разработки целевых программ обеспечения информационной

безопасности РФ. Под информационной безопасностью РФ в этом документе понимается «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства». На уровне личности для этого необходимо обеспечить реализацию конституционных прав человека и гражданина в информационной сфере, на уровне общества требуется упрочение демократии, создание правового социального государства, достижение и поддержание общественного согласия, а на уровне государства — реализация всех его функций, а также развитие отечественной информационной инфраструктуры.

Этот подход получает развитие при формулировании четырех основных составляющих национальных интересов Российской Федерации в информационной сфере. Во-первых, «соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны».

Во-вторых, «информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам».

В-третьих, «развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов».

В-четвертых, «защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России».

В контексте «технической» информационной безопасности интерес представляет последняя, четвертая из перечисленных составляющих национальных интересов РФ в информационной сфере. Государственное регулирование, направленное на улучшение ситуации по данному направлению, строится по принципу устранения и сокращения традиционных угроз информационной безопасности. Методы соответствующего регулирования подразделяются на правовые, организационно-технические и экономические.

Правовые меры

К правовым мерам обеспечения информационной безопасности относится разработка специализированных нормативных правовых актов (законов,

постановлений и т.п.), а также нормативных методических документов (в первую очередь, стандартов обеспечения безопасности).

Базу правового обеспечения информационной безопасности составляют: закон «О государственной тайне», законодательство об архивном фонде РФ и архивах, федеральные законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», «О коммерческой тайне» и ряд других законов и законопроектов. Этими правовыми актами, в частности, определяются виды информации, которую можно относить к конфиденциальной, требования к организации информационной безопасности, критерии разграничения доступа к информации, условия ее отнесения к государственной, коммерческой или служебной тайне, а также условия распространения на информацию прав собственности.

Стандарты информационной безопасности, используемые в РФ, сейчас по большей части являются адаптированными стандартами ISO/МЭК. С их помощью на единой методологической основе регламентируются различные аспекты создания и использования средств и систем обеспечения информационной безопасности.

Для государственных учреждений соблюдение этих стандартов обязательно, для коммерческих организаций — носит рекомендательный характер. Тем не менее, указанные стандарты сейчас используются практически во всех крупных организациях, а также в средних и мелких, для которых политики информационной безопасности и системы защиты информации разрабатывались специализированным компаниям.

Организационно-технические меры

Среди организационно-технических методов обеспечения информационной безопасности следует выделить: усиление правоприменительной деятельности органов исполнительной власти; разработку, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств; выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем; сертификацию средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации; совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности.

Экономические методы

Экономические методы обеспечения информационной безопасности РФ включают в себя разработку программ обеспечения информационной безопасности РФ и определение порядка их финансирования; совершенствование системы финансирования работ, связанных с реализацией правовых

и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Принципиально государство может регулировать рынок информационной безопасности либо непосредственно на него воздействуя, либо влияя на него косвенным образом. Из перечисленных выше методов обеспечения информационной безопасности на уровне государства непосредственное влияние на рынок оказывают экономические (финансирование целевых программ) и организационно-технические (лицензирование деятельности и сертификация продуктов). Первые влияют на величину спроса на средства защиты информации на рынке, а вторые — на соответствующее предложение, ограничивая число участников рынка и ассортимент предлагаемых товаров и услуг.

Перечень видов деятельности, подлежащих обязательному лицензированию, приводится в федеральном законе «О лицензировании отдельных видов деятельности». Среди них: разработка, распространение и техническое обслуживание шифровальных средств; предоставление услуг в области шифрования информации; деятельность по выявлению электронных устройств, предназначенных для негласного получения информации; деятельность по разработке и производству средств защиты конфиденциальной информации и технической защите конфиденциальной информации; разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации; проведение работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и оказанием услуг по защите государственной тайны (указано в федеральном законе «О государственной тайне»).

Правовое обеспечение информационной безопасности оказывает на рынок косвенное воздействие, определяя структуру рынка и образ действий его участников.

Как правило, законодательство отстает от современной ситуации в сфере информационной безопасности (что особенно актуально для российского законодательства). В результате далеко не все предотвращаемые и нейтрализуемые доступными на рынке средствами защиты угрозы относятся к нарушающим закон. Такова нынешняя ситуация со «спамом», «клонированием» мобильных телефонов стандарта CDMA, пользованием услугами Интернет по чужим реквизитам, созданием и распространением «шпионского» и «рекламного» программного обеспечения.

С другой стороны, законодательство в сфере информационной безопасности в определенной мере регламентирует деятельность участников рынка, не позволяя, в частности, использовать для защиты информации вредоносное программное обеспечение и иным образом нарушать права других участников информационных отношений.

7.2 Защита прав и свобод в информационной сфере в условиях информатизации

Конституция РФ защищает от угроз информационной безопасности следующие информационные права и свободы:

"Статья 29 пункт 4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом".

"Статья 33 Граждане Российской Федерации имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления".

"Статья 29 пункт 1. Каждому гарантируется свобода мысли и слова".

"Статья 44 пункт 1. Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

Пункт 2. Каждый имеет право на участие в культурной жизни и пользование учреждениями культуры, на доступ к культурным ценностям".

"Статья 29 пункт 3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них".

Отдельные положения конституционных норм развиваются нормами Федерального закона "Об информации, информатизации и защите информации".

Статья 12. Реализация права на доступ к информации из информационных ресурсов.

Пункт 1. Пользователи - граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения - обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом...

Пункт 2. Владельцы информационных ресурсов обеспечивают пользователей (потребителей) информацией из информационных ресурсов на основе законодательства, уставов указанных органов и организаций, положений о них, а также договоров на услуги по информационному обеспечению...".

"Статья 24. Защита права на доступ к информации.

Пункт 1. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным судом.

Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

Пункт 2. Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях необоснованного отказа в предоставлении информации пользователям или в результате других нарушений прав пользователей.

Пункт 3. Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях".

Защита информационных прав и свобод обеспечивается нормами институтов интеллектуальной собственности, института документированной информации, УК РФ, КоАП РСФСР, ГК РФ. 228

Примеры норм УК РФ: клевета (ст. 129), оскорбление (ст. 130), нарушение неприкосновенности частной жизни (ст. 137), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138), отказ в предоставлении гражданину информации (ст. 140), нарушение авторских и смежных прав (ст. 146), отказ в предоставлении гражданину информации (ст. 140), нарушение изобретательских и патентных прав (ст. 147).

7.3 Правовая защита информации, информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц

Правовую основу информационной безопасности составляют следующие информационные конституционные нормы:

"Статья 29 пункт 4. Перечень сведений, составляющих государственную тайну, определяется федеральным законом".

Конституция РФ охраняет личную тайну, информацию о личности или персональные данные от вмешательства посторонних лиц.

"Статья 23 пункт 1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Пункт 2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений...".

При этом прямо запрещается, кому бы то ни было собирать информацию о любом гражданине без его на то согласия.

"Статья 24 пункт 1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются".

Конституцией РФ запрещается также получать иную информацию от любого гражданина без его добровольного на то согласия или убеждать его отказаться от предоставленной ранее информации.

Основной системообразующий набор норм, обеспечивающих защиту информации, информационных ресурсов, информационных систем от неправомерного вмешательства третьих лиц, развивающих содержание конституционных норм, содержится в Федеральном законе "Об информации, информатизации и защите информации".

"Статья 21. Защита информации.

Пункт 1. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
- в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;
- в отношении персональных данных - федеральным законом".

К конфиденциальной информации относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, составляющие тайну следствия и судопроизводства;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Пункт 2. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы, информационные технологии для формирования и использования информационных ресурсов, ограниченным доступом, руководствуются в своей деятельности законодательством РФ.

Пункт 3. Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяемом Правительством РФ.

Пункт 4. Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

Пункт 5. Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

Пункт 6. Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство РФ. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки".

Федеральным законом "Об информации, информатизации и защите информации" устанавливаются права и обязанности субъектов в области защиты информации.

"Статья 22. Права и обязанности субъектов в области защиты информации.

Пункт 1. Собственник документов, массива документов, информационных систем или уполномоченные им лица... устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.

Пункт 2. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

Пункт 3. Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Пункт 4. Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Пункт 5. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или)

информационных систем обо всех фактах нарушения режима защиты информации".

Законом предусматривается защита прав субъектов в сфере информационных процессов и информатизации.

"Статья 23. Защита прав субъектов в сфере информационных процессов и информатизации.

Пункт 1. Защита прав субъектов в сфере формирования информационных ресурсов, пользования информационными ресурсами, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба.

Пункт 2. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

Пункт 3. За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством РФ и субъектов Российской Федерации.

Для рассмотрения конфликтных ситуаций и защиты прав участников в сфере формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения могут создаваться временные и постоянные третейские суды.

Третейский суд рассматривает конфликты и споры сторон в порядке, установленном законодательством о третейских судах.

Пункт 4. Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения, возлагается на органы государственной власти, организации и граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров, ратифицированных Российской Федерацией".

Ответственность за правонарушения по этому направлению информационной безопасности регулируются нормами статей УК РФ: нарушение неприкосновенности частной жизни (ст. 137), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 138), незаконный экспорт технологий, научно-технической информации и услуг, сырья, материалов и оборудования, используемых при создании оружия массового поражения, вооружения и военной техники (ст. 189), неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

Примером нормы об ответственности в Кодексе РСФСР об административных правонарушениях является ст. 4014 "Умышленное уничтожение, повреждение печатных материалов, относящихся к выборам, референдуму".

В целом вопросы этого направления правового обеспечения информационной безопасности условно разделяются на защиту открытой информации и защиту информации ограниченного доступа.

Защита открытой информации осуществляется нормами института документированной информации (см. гл. 8).

Защита информации ограниченного доступа регулируется нормами: института государственной тайны (см. гл. 16), института коммерческой тайны (см. гл. 17), института персональных данных (см. гл. 18), а также нормами защиты других видов тайн.

7.4 Структура правового регулирования отношений в области информационной безопасности

Заключая рассмотрение правовых проблем информационной безопасности, отметим, что информационную безопасность можно рассматривать как аспект или ракурс изучения и формирования системы информационного права, подготовки и совершенствования норм и нормативных правовых актов этой отрасли. Используя результаты исследования в области информационной безопасности, законодатель и исследователь отрасли информационного права получают дополнительные возможности совершенствования средств и механизмов правовой защиты информационной безопасности в информационной сфере. Тем самым существенно повышаются качество и эффективность правового регулирования отношений в информационной сфере.

В этой связи структура правового регулирования отношений в области информационной безопасности как бы повторяет структуру самого информационного законодательства, акцентируя внимание на вопросах защищенности объектов правового регулирования, исходя из требований информационной безопасности. В итоге можно построить некоторую модель основных направлений защиты объектов информационной сферы и институтов информационного законодательства, с помощью нормативных предписаний которых решается проблема правового обеспечения защиты их информационной безопасности.

Основные направления защиты информационной сферы:

1. Защита интересов личности, общества, государства от воздействия вредной, опасной, недоброкачественной информации
2. Защита информации, информационных ресурсов и информационных систем от неправомерного воздействия посторонних лиц
3. Защита информационных прав и свобод

Правовое регулирование информационной безопасности формируется на базе информационных правоотношений, охватывающих все направления деятельности субъектов информационной сферы. Они охватывают все области информационной сферы, всех субъектов и объектов правоотношений.

Объекты правоотношений в области информационной безопасности - это духовность, нравственность и интеллектуальность личности и общества, права и свободы личности в информационной сфере; демократический строй, знания и духовные ценности общества; конституционный строй, суверенитет и территориальная целостность государства.

Субъектами правоотношений в области информационной безопасности выступают личность, государство, органы законодательной, исполнительной и судебных властей, система обеспечения безопасности, Совет Безопасности РФ, граждане.

Поведение субъектов в данной области определяются предписаниями законов и других нормативных правовых актов в порядке осуществления их прав и обязанностей, направленных на обеспечение защищенности объектов правоотношений.

Права и обязанности субъектов задаются нормами законов и иных нормативных правовых актов, устанавливающих правила поведения субъектов в порядке защиты объектов правоотношений, контроля и надзора за обеспечением информационной безопасности. Здесь же вводятся ограничения информационных прав и свобод в порядке защиты интересов граждан, общества, государства. При формировании норм права, установления прав и обязанностей применяются методы конституционного, административного и гражданского права.

Ответственность за правонарушения в информационной сфере устанавливается в порядке: защиты нравственности и духовности личности, общества, государства от воздействия недоброкачественной, ложной информации и дезинформации; защиты личности в условиях информатизации; защиты информации и информационных ресурсов от несанкционированного доступа (гражданско-правовая, административно-правовая, уголовно-правовая ответственность). Особенности установления ответственности за правонарушения в среде трансграничных информационных сетей, в том числе в Интернет основываются на особенностях и юридических свойствах информации, информационных технологий и средств их обеспечения.

Правовые механизмы защиты жизненно важных интересов личности, общества, государства должны разрабатываться и внедряться в каждой из областей информационной сферы.

1. Область поиска, получения и потребления информации.

Объекты правоотношений: духовность и нравственность гражданина, общества, государства (от воздействия недостоверной, ложной, вредной информации); информационные права и свободы человека и гражданина (право на получение и использование информации); честь и достоинство гражданина (в

связи с созданием и распространением недостоверной информации или несанкционированным распространением личной информации о нем).

Субъекты правоотношений: человек и гражданин, потребитель информации, редакция.

2. Область создания (производство) исходной и производной информации.

Объекты правоотношений: информация как интеллектуальная собственность; документированная информация как интеллектуальная и вещная собственность.

Субъекты правоотношений: человек и гражданин, авторы, пользователи исключительных прав, издатели, потребители информации, органы государственной власти и местного самоуправления, органы и системы обеспечения защиты объектов информационной безопасности.

3. Область формирования информационных ресурсов, подготовки и предоставления пользователям информационных продуктов, информационных услуг.

Объекты правоотношений: право авторства и собственности на информационные ресурсы; информационные ресурсы на всех видах носителей, в том числе содержащие информацию ограниченного доступа.

Субъекты правоотношений: человек и гражданин, автор, пользователь, потребитель, участники самостоятельного оборота информации.

4. Область создания и применения информационных систем, технологий и средств их обеспечения.

Объекты правоотношений: автоматизированные информационные системы, базы и банки данных, другие информационные технологии, средства обеспечения этих объектов. При этом, прежде всего, должны защищаться:

- права авторов и собственников информационных систем и технологий, средств их обеспечения;
- машинные носители с информацией, например, средствами электронной цифровой подписи; базы данных (знаний) в составе автоматизированных информационных систем и их сетей от несанкционированного доступа;
- программные средства в составе ЭВМ, их сетей, информационные системы и их сети от несанкционированного доступа;
- информационные технологии и средства их обеспечения.

Субъекты правоотношений: создатели, производители, заказчики, исполнители.

7.5 Виды компьютерных преступлений

1) Сетевая атака и повреждение компьютерной системы. На сегодняшний день к данному типу правонарушений можно отнести следующие: а) хакерная атака с целью перехвата, уничтожения, изменения и подделки информации, хранящейся в компьютере, нарушения нормального

функционирования компьютерной системы и сетей. Ввиду распространения в Интернете различного рода программ хакерную атаку способны выполнить люди, обладающие поверхностными знаниями в области компьютерной технологии;
б) разработка и распространение компьютерных вирусов. С момента разработки первого компьютерного вируса намечается стремительный рост видов вирусов и их модификаций. Глобальная сеть Интернет является идеальной платформой для распространения компьютерных вирусов. Появились лица, которые умышленно разрабатывают и распространяют такие вирусы;
в) хищение информации, хранящейся в компьютере. На данный момент в связи с отсутствием правовых норм, регулирующих программное обеспечение в области сетевого администрирования, некоторые программы типа «троянский конь» способны повлечь за собой утечку важной информации, угрожая тем самым государственным интересам;

2) сетевое мошенничество. Как правило, преступниками посредством Интернета распространяется заведомо ложная информация о прибыльных деловых предложениях с целью привлечения средств потенциальных жертв. В Китае также были обнаружены случаи мошенничества зарубежных преступников с помощью различных схем;

3) хищение денежных средств из финансовых учреждений путем несанкционированного доступа к компьютерным системам. На данный момент оно является наиболее популярным видом преступления с разнообразными схемами. Главный объект преступления представляют собой денежные средства, банковские счета и иные финансовые документы. Были замечены случаи хищения чужого банковского счета и номера кредитной карточки с последующей кражей денег, а также хищение трафика с использованием чужого имени и пароля при регистрации. По статистике сумма, присвоенная путем хищения с использованием генерированных номеров кредитных карточек, в мире ежегодно превышает сотни миллионов долларов США; во многих случаях подобного рода преступность можно отнести к организованной;

4) азартные игры в онлайновой среде и реклама услуг сексуального характера в Интернете. Преступники используют Интернет в качестве инструмента. Появились «виртуальные казино», предлагающие различные виды азартных игр. Предложение услуг сексуального характера в Интернете также является довольно популярным видом преступления;

5) посягательства на авторские и смежные права, преступления против интеллектуальной собственности. Прогресс информационных и сетевых технологий предоставляет удобные средства для пиратской деятельности. Как правило, правонарушение связано с реализацией через Интернет пиратских копий программных продуктов, а также с посягательством на право на патенты и торговые марки, злоумышленной регистрацией доменных имен, использованием схожих с известными брэндами торговых и прочих знаков и марок;

6) хищение информации, составляющей государственную тайну, — угроза государственной безопасности. На сегодняшний день компьютерные

системы легко подвергаются компьютерным атакам. Организации и лица могут инициировать проникновение в информационные системы государственных служб, похищать информацию, затем использовать ее во враждебных целях, создавая тем самым серьезную угрозу государственной безопасности;

7) распространение информации. К данному типу преступления можно отнести: распространение в Интернете порнографической продукции, продуктов, вызывающих проявления расизма и разжигания межнациональной розни, иной информации, угрожающей государственной безопасности. Вредоносная информация в Интернете более доступна широкой аудитории, следовательно, создает большую социальную угрозу. В Китае было несколько случаев распространения информации порнографического характера в Интернете, главным образом посредством порнографических сайтов, личных домашних страниц и совершения иных преступных деяний, связанных с распространением порнографии. Ввиду сложности контроля за распространением подобного рода информации создаются определенные трудности для расследования и сбора доказательственной базы и квалификации преступления;

8) посягательство на частную жизнь гражданина. В условиях бурного развития информационных и сетевых технологий личная жизнь становится все более прозрачной. Охрана личной жизни и развитие информационных сетей вступают в противоречие. Подделку, распространение информации, ущемляющей честь и достоинство гражданина, откровенную клевету, ложь, порой под чужим именем, разглашение информации о личной жизни человека без какого-либо на то разрешения и прочие правонарушения можно отнести к данному типу компьютерной преступности.

На сегодняшний день реализация пиратских программных продуктов, мошенничество, коррупция, хищение и распространение порнографии становятся довольно популярными видами преступлений. Можно ожидать, что с популяризацией и развитием компьютерных сетей их негативные стороны станут все более очевидными: с одной стороны, увеличивается число информационных преступлений, с другой – увеличивается число преступлений, связанных с использованием компьютера. Например, происходит распространение в Интернете различных способов совершения правонарушения, таких, как мошенничество, манипуляция с ценами на фондовых биржах, разработка компьютерных вирусов, разрушающих производственный и технологический процесс, и т.д.

7.6 Контрольные вопросы

1. Государственная политика РФ в области безопасности информационных технологий?
2. Организационно-технические методы?
3. В чем состоят экономические меры?
4. В чем заключается, защита прав и свобод в информационной сфере?

8 Безопасность программного обеспечения и человеческий фактор

8.1 Человеческий фактор

Преднамеренные и непреднамеренные нарушения безопасности программного обеспечения компьютерных систем большинство отечественных и зарубежных специалистов связывают с деятельностью человека. При этом технические сбои аппаратных средств ИС, ошибки программного обеспечения и т.п. часто рассматриваются лишь как второстепенные факторы, связанные с проявлением угроз безопасности. С некоторой степенью условности злоумышленников в данном случае можно разделить на два основных класса:

• злоумышленники-любители (будем называть их хакерами);

• злоумышленники-профессионалы.

Хакеры - это люди, увлеченные компьютерной и телекоммуникационной техникой, имеющие хорошие навыки в программировании и довольно любознательные. Их деятельность в большинстве случаев не приносит особого вреда компьютерным системам.

Ко второму классу можно отнести отечественные, зарубежные и международные криминальные сообщества и группы, а также правительственные организации и службы, которые осуществляют свою деятельность в рамках концепции «информационной войны». К этому же классу можно отнести и сотрудников самих предприятий и фирм, ведущих разработку или эксплуатацию программного обеспечения.

Хакеры и группы хакеров

Хакеры часто образуют небольшие группы. Иногда эти группы периодически собираются, а в больших городах хакеры и группы хакеров встречаются регулярно. Но основная форма взаимодействия осуществляется через Интернет, а ранее - через электронные доски BBS. Как правило, каждая группа хакеров имеет свой определенный (часто критический) взгляд на другие группы. Хакеры часто прячут свои изобретения от хакеров других групп и даже от соперников в своей группе.

Существуют несколько типов хакеров. Это хакеры, которые:

• стремятся проникнуть во множество различных компьютерных систем (маловероятно, что такой хакер объявится снова после успешного проникновения в систему);

• получают удовольствие, оставляя явный след того, что он проник в систему;

• желают воспользоваться оборудованием, к которому ему запрещен доступ;

• охотятся за конфиденциальной информацией;

• собираются модифицировать определенный элемент данных, например баланс банка, криминальную запись или экзаменационные оценки;

• пытаются нанести ущерб «вскрытой» (обезоруженной) системе.

Группы хакеров, с некоторой степенью условности, можно разделить на следующие:

• группы хакеров, которые получают удовольствие от вторжения и исследования больших ЭВМ, а также ЭВМ, которые используются в различных государственных учреждениях;

• группы хакеров, которые специализируются на телефонной системе;

• группы хакеров - коллекционеров кодов - это хакеры, запускающие перехватчики кода, которые ищут карту вызовов (calling card) и номера PBX (private branch exchange - частная телефонная станция с выходом в общую сеть);

• группы хакеров, которые специализируются на вычислениях. Они используют компьютеры для кражи денег, вычисления номеров кредитных карточек и другой ценной информации, а затем продают свои услуги и методы другим, включая членов организованной преступности. Эти хакеры могут скупать у коллекционеров кодов номера PBX и продавать их за 200-500$, и подобно другим видам информации неоднократно. Архивы кредитных бюро, информационные срезы баз данных уголовного архива ФБР и баз данных других государственных учреждений также представляют для них большой интерес. Хакеры в этих группах, как правило, не находят взаимопонимания с другими хакерами;

• группы хакеров, которые специализируются на сборе и торговле пиратским программным обеспечением.

Типовой потрет хакера.

Ниже приводится два обобщенных портрета хакера, один составлен по данным работы и характеризует скорее зарубежных хакеровлюбителей, в то время как второй - это обобщенный портрет отечественного злонамеренного хакера, составленный Экспертно-криминалистическим центром МВД России.

В первом случае отмечается, что многие хакеры обладают следующими особенностями:

• мужчина: большинство хакеров - мужчины, как и большинство программистов;

• молодой: большинству хакеров от 14 до 21 года, и они учатся в институте или колледже. Когда хакеры выходят в деловой мир в качестве программистов, их программные проекты источают большую часть их излишней энергии, и корпоративная обстановка начинает менять их жизненную позицию. Возраст компьютерных преступников показан на рисунке 8.1;

• сообразительный: хакеры часто имеют коэффициент интеллекта выше среднего. Не смотря на свой своеобразный талант, большинство из них в школе или колледже не были хорошими учениками. Например, большинство программистов пишут плохую документацию и плохо владеют языком;

• концентрирован на понимании, предсказании и управлении: эти три условия составляет основу компетенции, мастерства и самооценки и

стремительные технологические сдвиги и рост разнообразного аппаратного и программного обеспечения всегда будут вызовом для хакеров;

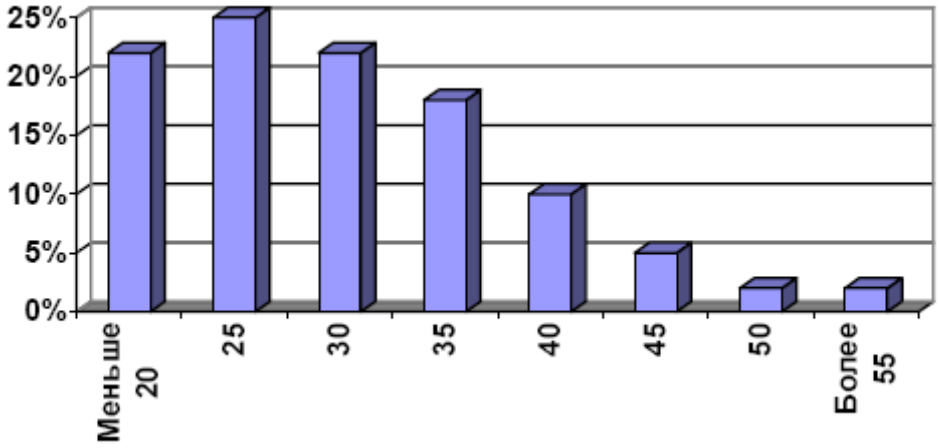

Рисунок 8.1 - Возрастное распределение обнаруженных компьютерных преступников.

• увлечен компьютерами: для многих пользователей компьютер – это необходимый рабочий инструмент. Для хакера же - это «удивительная игрушка» и объект интенсивного исследования и понимания;

• отсутствие преступных намерений: по данным [54] лишь в 10% рассмотренных случаев компьютерной преступности нарушения, совершаемые хакерами, привели к разрушению данных компьютерных систем.

В связи с этим можно предположить, что менее 1% всех хакеров являются злоумышленниками.

Обобщенный портрет отечественного хакера выглядит следующим образом: это мужчина в возрасте от 15 до 45 лет, либо имеющий многолетний опыт работы на компьютере, либо почти не обладающий таким опытом; в прошлом к уголовной ответственности не привлекался; является яркой, мыслящей личностью, способной принимать ответственные решения; хороший, добросовестный работник; по характеру нетерпимый к насмешкам и к потере своего социального статуса в рамках окружающей его группы людей; любит уединенную работу; приходит на службу первым и уходит последним; часто задерживается на работе после окончании рабочего дня и очень редко использует отпуска и отгулы.

Криминальные сообщества и группы, сценарий взлома компьютерной системы.

В связи со стремительным ростом информационных технологий и разнообразных компьютерных и телекоммуникационных средств и систем, наблюдается экспоненциальный рост как количества компьютерных атак, так и объем нанесенного от них ущерба. Это показали исследования, проведенные в 90-х гг. в США. Анализ показывает, что такая тенденция постоянно сохраняется.

За последнее время в нашей стране не отмечено ни одного компьютерного преступления, которое было бы совершено одиночкой. Более того, известны

случаи, когда организованными преступными группировками нанимались бригады из десятков хакеров. Им предоставлялись отдельные охраняемые помещения, оборудованные самыми передовыми компьютерными средствами и системами для проникновения в компьютерные сети коммерческих банков.

Специалисты правоохранительных органов России неоднократно отмечали тот факт, что большинство компьютерных преступлений в банковской сфере совершается при непосредственном участии самих служащих коммерческих банков. Результаты исследований, проведенных с привлечением банковского персонала, показывают, что доля таких преступлений приближается к отметке 70%. При осуществлении попытки хищения 2 млрд. рублей из филиала одного крупного коммерческого банка преступники оформили проводку фиктивного платежа с помощью удаленного доступа к компьютеру через модем, введя пароль и идентификационные данные, которые им передали сообщники из состава персонала этого филиала. Далее эти деньги были переведены в соседний банк, где преступники попытались снять их со счета, оформив поддельное платежное поручение.

По данным Экспертно-криминалистического центра МВД России принципиальный сценарий взлома защитных механизмов банковской компьютерной системы представляется следующим. Компьютерные злоумышленники-профессионалы обычно работают только после тщательной предварительной подготовки. Они снимают квартиру на подставное лицо в доме, в котором не проживают сотрудники ФСБ, МВД или МГТС. Подкупают сотрудников банка, знакомых с деталями электронных платежей и паролями, и работников телефонной станции, чтобы обезопасить себя на случай поступления запроса от службы безопасности банка. Нанимают охрану из бывших сотрудников МВД. Чаще всего взлом банковской компьютерной системы осуществляется рано утром, когда дежурный службы безопасности теряет свою бдительность, а вызов помощи затруднен.

Злоумышленники в профессиональных коллективах программистов-разработчиков.

Согласно существующей статистики в коллективах людей занятых той или иной деятельностью, как правило, только около 85% являются вполне лояльными (честными), а остальные 15% делятся примерно так: 5% - могут совершить что-нибудь противоправное, если, по их представлениям, вероятность заслуженного наказания мала; 5% - готовы рискнуть на противоправные действия, даже если шансы быть уличенным и наказанным складываются 50 на 50; 5% - готовы пойти на противозаконный поступок, даже если они почти уверены в том, что будут уличены и наказаны. Такая статистика в той или иной мере может быть применима к коллективам, участвующим в разработке и эксплуатации информационнотехнических составляющих компьютерных систем. Таким образом, можно предположить, что не менее 5% персонала, участвующего в разработке и эксплуатации программных комплексов, способны осуществить действия криминального характера из корыстных побуждений либо под влиянием

каких-нибудь иных обстоятельств. По другим данным считается, что от 80 до 90% компьютерных нарушений являются внутренними, в частности считается, что на каждого «... подлого хакера приходится один обозленный и восемь небрежных работников, и все они могут производить разрушения изнутри».

8.2 Информационная война

В настоящее время за рубежом в рамках создания новейших оборонных технологий и видов оружия активно проводятся работы по созданию так называемых средств нелетального воздействия. Эти средства позволяют без нанесения разрушающих ударов (например, современным оружием массового поражения) по живой силе и технике вероятного противника выводить из строя и/или блокировать его вооружение и военную технику, а также нарушать заданные стратегии управления войсками.

Одним из новых видов оружия нелетального воздействия является информационное оружие, представляющее собой совокупность средств поражающего воздействия на информационный ресурс противника. Воздействию информационным оружием могут быть подвержены прежде всего компьютерные и телекоммуникационные системы противника. При этом центральными объектами воздействия являются программное обеспечение, структуры данных, средства вычислительной техники и обработки информации, а также каналы связи.

Появление информационного оружия приводит к изменению сущности и характера современных войн и появлению нового вида вооруженного конфликта - информационная война.

Несомненным является то, что информационная война, включающая информационную борьбу в мирное и военное время, изменит и характер военной доктрины ведущих государств мира. Многими зарубежными странами привносится в доктрину концепция выигрывать войны, сохраняя жизни своих солдат, за счет технического превосходства. Ввиду того, что в мировой практике нет прецедента ведения широкомасштабной информационной войны, а имеются лишь некоторые прогнозы и зафиксированы отдельные случаи применения информационного оружия в ходе вооруженных конфликтов и деятельности крупных коммерческих организаций, анализ содержания информационной войны за рубежом возможен по отдельным публикациям, так как, по некоторым данным информация по этой проблеме за рубежом строго засекречена.

Анализ современных методов ведения информационной борьбы позволяет сделать вывод о том, что к прогнозируемым формам информационной войны можно отнести следующие:

- глобальная информационная война;
- информационные операции;
- преднамеренное изменение замысла стратегической и тактической операции;

• дезорганизация жизненно важных для страны систем;

• нарушение телекоммуникационных систем;

• обнуление счетов в международной банковской системе;

• уничтожение (искажение) баз данных и знаний важнейших государственных и военных объектов.

К методам и средствам информационной борьбы в настоящее время относят:

• воздействие боевых компьютерных вирусов и преднамеренных дефектов диверсионного типа;

• несанкционированный доступ к информации;

• проявление непреднамеренных ошибок ПО и операторов компьютерных систем;

• использование средств информационно-психологического воздействия на личный состав;

• воздействие радиоэлектронными излучениями;

• физические разрушения систем обработки информации.

Таким образом, в большинстве развитых стран мира в рамках концепции информационной войны разрабатывается совокупность разнородных средств, которые можно отнести к информационному оружию. Такие средства могут использоваться в совокупности с другими боевыми средствами во всех возможных формах ведения информационной войны. Кроме существовавших ранее средств поражающего воздействия в настоящее время разрабатываются принципиально новые средства информационной борьбы, а именно бое вые компьютерные вирусы и преднамеренные программные дефекты диверсионного типа.

8.3 Психология программирования

При создании высокоэффективных и надежных программ (программных комплексов), отвечающих самым современным требованиям к их разработке, эксплуатации и модернизации необходимо не только умело пользоваться предоставляемой вычислительной и программной базой современных компьютеров, но и учитывать интуицию и опыт разработчиков языков программирования и прикладных систем. Помимо этого, целесообразно дополнять процесс разработки программ экспериментальными исследованиями, которые основываются на применении концепции психологии мышления при исследовании проблем вычислительной математики и информатики. Такой союз вычислительных, информационных систем и программирования принято называть психологией программирования.

Психология программирования - это наука о действиях человека, имеющего дело с вычислительными и информационными ресурсами автоматизированных систем, в которой знания о возможностях и способностях человека как разработчика данных систем могут быть углублены с помощью методов

экспериментальной психологии, анализа процессов мышления и восприятия, методов социальной, индивидуальной и производственной психологии.

К целям психологии программирования наряду с улучшением использования компьютера, основанного на глубоком знании свойств мышления человека, относится и определение, как правило, экспериментальным путем, склонностей и способностей программиста как личности. Особенности личности играют критическую роль в определении (исследовании) рабочего стиля отдельного программиста, а также особенностей его поведения в коллективе разработчиков программного обеспечения. Ниже приводится список характеристик личности и их предполагаемых связей с программированием. При этом особое внимание уделяется тем личным качествам программиста, которые могут, в той или иной степени, оказать влияние на надежность и безопасность разрабатываемого им программного обеспечения.

Внутренняя/внешняя управляемость.

Личности с выраженной внутренней управляемостью стараются подчинять себе обстоятельства и убеждены в способности сделать это, а также в способности повлиять на свое окружение и управлять событиями. Личности с внешней управляемостью (наиболее уязвимы с точки зрения обеспечения безопасности программного обеспечения) чувствуют себя жертвами не зависящих от них обстоятельств и легко позволяют другим доминировать над ними.

Высокая/низкая мотивация.

Личности с высокой степенью мотивации способны разрабатывать очень сложные и сравнительно надежные программы. Руководители, способные повысить уровень мотивации, в то же время, могут стимулировать своих сотрудников к созданию программ с высоким уровнем их безопасности.

Умение быть точным.

На завершающих этапах составления программ необходимо особое внимание уделять подробностям и готовности проверить и учесть каждую деталь. Это позволит повысить вероятность обнаружения программных дефектов как привнесенных в программу самим программистом (когда нарушитель может ими воспользоваться в своих целях), так и другими программистами (в случае, если некоторые из них могут быть нарушителями) при создании сложных программных комплексов коллективом разработчиков.

Кроме того, психология программирования изучает, с точки зрения особенностей создания безопасного программного обеспечения, такие характеристики качества личности как исполнительность, терпимость к неопределенности, эгоизм, степень увлеченности, склонность к риску, самооценку программиста и личные отношения в коллективе.

Корпоративная этика.

Особый психологический настрой и моральные стимулы программисту может создать особые корпоративные условия его деятельности, в частности различные моральные обязательства, оформленные в виде кодексов чести. Ниже приводится «Кодекс чести пользователя компьютера».

• Обещаю не использовать компьютер в ущерб другим людям.
• Обещаю не вмешиваться в работу компьютера других людей.
• Обещаю «не совать нос» в компьютерные файлы других людей.
• Обещаю не использовать компьютер для воровства.
• Обещаю не использовать компьютер для лжесвидетельства.
• Обещаю не копировать и не использовать чужие программы, которые были оплачены не мною.
• Обещаю не использовать компьютерные ресурсы других людей без разрешения и соответствующей компенсации.
• Обещаю не присваивать результаты интеллектуального труда других людей.
• Обещаю думать об общественных последствиях разрабатываемых мною программ или систем.
• Обещаю всегда использовать компьютер с наибольшей пользой для живущих ныне и будущих поколений.

8.4 Контрольные вопросы

1. Понятие хакер.
2. Основные виды хакеров.
3. Назовите прогнозируемые формы информационной войны.

9 Методические указания к лабораторным работам

Целью проведения лабораторных работ является получение практических навыков разработки и использования программно-аппаратных средств защиты информации.

Цели лабораторного практикума достигаются наилучшим образом в том случае, если выполнению задания предшествует определенная подготовительная внеаудиторная работа.

Проведение лабораторных работ осуществляется в компьютерном зале, на ПК с установленным программным обеспечением (Visual Java++).

Выполнение лабораторных работ

Перед посещением компьютерного класса повторите материал, рассмотренный на последней лекции и изученный ранее.

Лабораторная работа выполняется в следующей последовательности:

1) получение задания у преподавателя;
2) разработка математической модели задачи;
3) разработка алгоритма, его анализ и оптимизация;
4) написание программы, её тестирование и отладка;
5) подготовка тестовых примеров.

Оформление отчетов производится в ходе выполнения работы непосредственно в лаборатории.

Отчет должен содержать:

- номер лабораторной работы,
- название работы,
- постановка задачи (задание, выданное преподавателем),
- математическая модель решения задачи,
- алгоритм решения задачи (блок-схема, псевдокод, словесное описание)
- текст программы,
- не менее трех тестовых примеров.

Для подготовки к защите лабораторной работы следует еще раз проанализировать результаты работы программы (и при необходимости провести отладку программы), попытаться предложить альтернативный алгоритм решения задачи, подготовить ответы на вопросы, приводимые в настоящей рабочей программе.

Темы лабораторных работ

Лабораторная работа №1 (глава 3)

Постановка задания: написать программную реализацию шифра простой перестановки и шифра Цезаря.

1. Изучить шифр простой перестановки и шифр Цезаря.
2. Выбрать язык программирования.
3. Написать программу, которая шифрует текстовое сообщение шифром простой перестановки и шифром Цезаря.
4. Написать отчет о проделанной работе.

Лабораторная работа №2 (глава 3)

Постановка задания: написать программную реализацию расширенного алгоритма Евклида.

1. Изучить алгоритм Евклида.
2. Изучить алгоритм расширенный алгоритм Евклида.
3. Выбрать язык программирования.
4. Написать программу, которая реализует расширенный алгоритм Евклида.
5. Написать отчет о проделанной работе.

Лабораторная работа №3 (глава 3)

Постановка задания: написать программу, которая реализует шифрование текста с помощью магических квадратов.

1. Изучить теорию по работе с магическими квадратами.
2. Подгруппа разбивается на 4 бригады: первая, вторая, третья, четвертая по 2 – 3 человека в каждой. В дальнейшем бригады работают друг с другом: первая с третьей, вторая с четвертой.
3. Выбрать язык программирования.

4. Каждая бригада пишет программу получения шифра двойной перестановки по ключевым словам русского осмысленного текста для таблицы перестановки 4 х 4 и программу расшифровки шифротекста двойной перестановки по ключевым словам русского осмысленного текста для таблицы перестановки 4 х 4.

5. Написать отчет о проделанной работе.

Лабораторная работа №4 (глава 3)

Постановка задания: написать программную реализацию алгоритма шифрования данных RSA.

1. Изучить все этапы алгоритма шифрования данных RSA.
2. Выбрать язык программирования.
3. Написать программу, которая кодирует и декодирует содержимое текстового файла.
4. Написать отчет о проделанной работе.

Лабораторная работа №5 (глава 3)

Постановка задания: написать программу, для формирования и проверки электронной цифровой подписи на основе алгоритма RSA.

1. Изучить алгоритм цифровой подписи RSA.
2. Для облегчения выполнения лабораторной работы в качестве хэш-функции будем использовать алгоритм шифрования ГОСТ 28147-89.
3. Выбрать язык программирования.
4. Группа разбивается на бригады по 2-3 человека. Каждый член бригады реализует свою часть алгоритма, а именно можно выделить следующие блоки для реализации: реализация хэш-функции, реализация собственно алгоритма цифровой подписи RSA.
5. Написать отчет о проделанной работе.

Лабораторная работа №6 (глава 4)

Постановка задания: Изучить методы защиты в операционной системе UNIX.

1. Изучить основные характеристики операционной системы UNIX.
2. Изучить достоинства и недостатки операционной системы UNIX.
3. Изучить методы защиты от угроз в операционной системы UNIX.
4. Написать отчет о проделанной работе.

Лабораторная работа №7 (глава 5)

Постановка задания: Научится работать с сетевым экраном операционной системы Windows XP.

1. Изучить основные характеристики операционной системы Windows XP.
2. Научиться работать с сетевым экраном.
3. Написать отчет о проделанной работе.

Лабораторная работа №8 (глава 6)

Постановка задания: научиться работать с программными продуктами AVP(«Антивирус Касперского »).

1. Изучить теорию по компьютерным вирусам.
2. Научиться работать с программой AVP.
3. Заразить вирусом типа «Worm» файлы на терминале.
4. Запустить программу AVP и проверить терминал на присутствие вируса.
5. Написать отчет о проделанной работе.

Список использованных источников

1 Малюк, А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М. : Горячая Линия – Телеком, 2001. – 148 с.

2 UNIX: Руководство системного администратора / Эви Немет, Гарт Снайдер, Скотт Сибасс, Трент Р. Хейн; пер. с англ. С.М. Тимачева; под ред. М.В. Коломыцева. – 3-е изд. – Киев : BHV, 1998. – 832 с.

3 Баричев, С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия – Телеком, 2001. – 121 с.

4 Дейтел, Г. Введение в операционные системы: в 2 т. / пер с англ. – М. : Мир, 1987. – Т. 2. – 359 с.

5 Физическая защита информационных систем // JetInfo. – 1997. – № 1. – 28 с.

6 Аудит безопасности информационных систем // JetInfo. – 1999. – № 9. – 24 с.

7 Информационная безопасность. Ситуация в мире и России // JetInfo. – 2000. – № 8. – 16 с.

8 Актуальные вопросы выявления сетевых атак // JetInfo. – 2002. – № 3. – 28 с.

9 Дж. Л. Месси. Введение в современную криптологию // ТИИЭР, 1988.-т.76, №5.-С.24-42.

10 Жельников В. Криптография от папируса до компьютера. / В. Жельников. – М: ABF, 1996.

11 A.Menezes, P.van Oorshot, S.Vanstone. Handbook of Applied Cryptography – CRC Press Inc., 1997.

12 Hal Tipton and Micki Krause. Handbook of Information Security Management – CRC Press LLC, 1998.