Оглавление

Введение

Развитие современного общества напрямую связано с ростом производства, потребления и накопления информации во всех отраслях человеческой деятельности. Информационные потоки в обществе увеличиваются с каждым днем, и этот процесс носит лавинообразный характер.

По своему значению для развития общества информация приравнивается к важнейшим ресурсам наряду с сырьем и энергией. В развитых странах большинство работающих заняты не в сфере производства, а в той или иной степени занимаются обработкой информации.

Вместе с тем можно отметить и новую тенденцию, заключающуюся во все большей информационной зависимости общества в целом и отдельного человека в частности. Именно поэтому в последнее время появились такие категории, как "информационная политика", "информационная безопасность", "информационная война" и целый ряд других новых понятий, в той или иной мере связанных с информацией.

Столь же ярко демонстрирует повышение роли информации в производственных процессах появление в XX веке такого понятия, как промышленный шпионаж. Не материальные ценности, а чистая информация становится объектом хищения. Это обстоятельство подчеркивает, насколько важной является информация для современного общества.

Информационная безопасность является одной из главных проблем, с которой сталкивается современное общество. Причиной обострения этой проблемы является широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации.

Тема 1. Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена

1.1. Понятие "информационная безопасность"

Информационная безопасность – это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Рассматривая информацию как товар, можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии, а может быть, и автор, потеряют часть рынка и т.д.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т.д.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления – производстве, транспорте и др.

Именно поэтому при определении понятия "информационная безопасность" на первое место ставится защита информации от различных воздействий.

Поэтому под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Согласно ГОСТ 50922-96:

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи, решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

Исходя из этого, отметим следующие важные выводы:

- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;
- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации это принципиально более широкое понятие.

В ряде случаев понятие "информационная безопасность" подменяется термином "компьютерная безопасность". В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем. Несмотря на это, в рамках изучаемого курса основное внимание будет уделяться изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передается с помощью компьютеров.

Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

1.2. Составляющие информационной безопасности

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

1. обеспечением доступности информации;
2. обеспечением целостности информации;
3. обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Целостность информации условно подразделяется на статическую и динамическую:

- Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации.
- Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных сообщений, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д.

Конфиденциальность – гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

1.3. Классификация угроз информационной безопасности

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности.

Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например, неконтролируемый доступ к персональным компьютерам или нелицензионное программное обеспечение.

Угрозы информационной безопасности классифицируются по нескольким признакам:

- по составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых в первую очередь направлены угрозы;

- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- по характеру воздействия (случайные или преднамеренные, действия природного или техногенного характера);
- по расположению источника угроз (внутри или вне рассматриваемой информационной системы).

Рассмотрим угрозы по характеру воздействия. Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы.

Причинами случайных воздействий при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия злоумышленника. В качестве злоумышленника может выступить служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами, например: недовольством служащего служебным положением; любопытством; конкурентной борьбой; уязвленным самолюбием и т. д.

Угрозы, классифицируемые по расположению источника угроз, бывают внутренние и внешние. Внешние угрозы обусловлены применением вычислительных сетей и созданием на их основе информационных систем.

Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

1.4. Каналы несанкционированного доступа к информации

Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющих нанести ущерб любой из

составляющих информационной безопасности, является несанкционированный доступ. Несанкционированный доступ возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки.

Каналы НСД классифицируются по компонентам автоматизированных информационных систем.

1. Через человека:
    - • хищение носителей информации;
    - • чтение информации с экрана или клавиатуры;
    - • чтение информации из распечатки.
2. Через программу:
    - • перехват паролей;
    - • расшифровка зашифрованной информации;
    - • копирование информации с носителя.
3. Через аппаратуру:
    - • подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
    - • перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т. д.

Технические каналы утечки информации

Технический канал утечки информации (ТКУИ) – это совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.

По сути, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте. Причем под разведывательной информацией обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные излучения, которые в той или иной степени связаны с обрабатываемой информацией. Физические явления, лежащие в основе появления этих излучений, имеют различный характер, тем не менее, они могут рассматриваться как непреднамеренная передача конфиденциальной информации по некоторым побочным каналам, образованным источником излучения, средой распространения и, возможно, приемной стороной (злоумышленником). Такие побочные каналы принято называть техническим каналом утечки информации.

Основными источниками образования технических каналов утечки любой, в том числе конфиденциальной, информации являются:

- преобразователи физических величин;
- излучатели электромагнитных колебаний;
- паразитные связи и наводки на провода и элементы электронных устройств.

Примером реализации системы преобразователей является звукоусилительная система, в которой микрофон превращает звук в электрический сигнал. Последний передается и усиливается усилителем низкой (звуковой) частоты, а затем поступает на громкоговоритель, воспроизводящий звук существенно более громкий, нежели тот, который воспринимается микрофоном.

Образованию каналов утечки информации способствуют определенные обстоятельства и причины технического характера, такие как несовершенство схемных решений (конструктивных и технологических), принятых для данной категории технических средств, эксплуатационный износ элементов изделия (изменение параметров элементов, аварийный выход/вывод из строя) и др.

При выявлении технических каналов утечки информации применительно к средствам вычислительной техники необходимо рассматривать все оборудование как систему, включающую основное (стационарное) оборудование, например, компьютеры, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными компьютерами и элементами вычислительной сети), распределительные и коммутационные устройства, системы электропитания, системы заземления.

В этой системе следует различать устройства, непосредственно участвующие в обработке, хранении, передаче конфиденциальной информации, и устройства, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся с основным оборудованием, обеспечивая его работу (система электропитания, заземление и т. д.) или условия для работы пользователей (система кондиционирования и т.д.).

В качестве потенциальных каналов утечки информации следует рассматривать элементы вспомогательного оборудования, имеющие выход за пределы контролируемой зоны, то есть зоны, в пределах которой исключено несанкционированное пребывание посторонних лиц, например, в пределах аудитории или отдельного здания и т. д.

Кроме соединительных линий основного и вспомогательного оборудования за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками и тоже являются потенциальными каналами утечки информации.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата технические каналы утечки информации бывают электромагнитные, электрические и параметрические.

Электромагнитные каналы утечки информации

К электромагнитным относятся каналы утечки информации, возникающие за счет:

1. **Электромагнитные излучения элементов основного и вспомогательного оборудования**

Носителем информации в технических средствах является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам основного и вспомогательного оборудования вокруг них возникает электрическое и магнитное поле. В силу этого элементы основного и вспомогательного оборудования можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

2. **Электромагнитные излучения на частотах работы высокочастотных генераторов (ВЧ-генераторов) основного и вспомогательного оборудования**

В состав основного и вспомогательного оборудования входят различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т. д.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ-генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т. д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных ВЧ-колебаний генераторов. Эти промодулированные ВЧ-колебания излучаются в окружающее пространство.

3. **Электромагнитные излучения на частотах самовозбуждения УНЧ основного и вспомогательного оборудования**

Самовозбуждение УНЧ основного и вспомогательного оборудования (например, усилителей систем звукоусиления и звукового сопровождения) возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к

переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения лежит в пределах рабочих частот нелинейных элементов УНЧ (например, полупроводниковых приборов). Сигнал на частотах самовозбуждения, как правило, оказывается модулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе УНЧ в нелинейный режим работы, то есть в режим перегрузки.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными вне контролируемой зоны.

Электрические каналы утечки информации

Причинами возникновения электрических каналов утечки информации являются:

1. **Наводки электромагнитных излучений**

Наводки электромагнитных излучений возникают при излучении элементами основного и вспомогательного оборудования (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий основного оборудования и посторонних проводников или линий вспомогательного оборудования. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий основного оборудования и посторонних проводников.

Пространство вокруг основного оборудования, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется (опасной) зоной 1.

Случайной антенной в данном случае может стать цепь вспомогательного оборудования или посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антенна представляет собой компактное техническое средство, например, телефонный аппарат, громкоговоритель радиотрансляционной сети и т. д. К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

2. **Прохождение информационных сигналов в цепи электропитания**

Прохождение информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение

напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

3. **Прохождение информационных сигналов в цепи заземления**

Кроме заземляющих проводников, служащих для непосредственного соединения основного оборудования с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны подключения к соединительным линиям вспомогательного оборудования и посторонним проводникам, проходящим через помещения, где установлено основное оборудование, а также к его системе электропитания и заземления. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Электронные устройства перехвата информации

Электронные устройства перехвата информации, устанавливаемые в основное оборудование, иногда называют аппаратными закладками. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в основное оборудование иностранного производства.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект.

Параметрический канал утечки информации

Перехват обрабатываемой в технических средствах информации возможен также путем их "высокочастотного облучения". При взаимодействии облучающего электромагнитного поля с элементами основного оборудования происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение модулируется информационным сигналом. При съеме информации для исключения взаимного влияния облучающего и переизлученного сигналов может использоваться их временная или частотная развязка. Например, для облучения основного оборудования могут использовать импульсные сигналы. При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют параметрическим.

Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства.

Важность и сложность проблемы ИБ

Информационная безопасность является важнейшей задачей на различных уровнях (национальном, отраслевом, корпоративном, персональном и др.)

1. В доктрине информационной безопасности РФ защита информации от НСД к информационным ресурсам (ИР), обеспечение безопасности информации и телекоммуникационных систем, выделены в качестве важнейших составляющих национальных интересов РФ в информационной сфере.
2. В США в 1996 году создана Комиссия по защите важных информационных ресурсов. В 1997 году Комиссия сделала вывод, что в США имеются недостаточные средства защиты от информационных угроз и нападений.
3. Ежегодно во всем мире отмечается рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (взлом ИС, атаки через Интернет, нарушения со стороны собственных сотрудников). Так в 2017 году 90% опрошенных крупных компаний сообщили, что имели место нарушения информационной безопасности, при этом 80% констатировали финансовые потери от этих нарушений. Наибольший ущерб нанесли кражи и подлоги информации.

В настоящее время всё больше угроз и нападений осуществляется через Интернет, так как она связывает огромное количество абонентов. В сеть Интернет можно входить не только по проводным телефонным линиям, но и по радиоканалу, оптико-волоконным и спутниковым линиям связи.

Даже хорошо оснащенные военные ведомства, банковские системы, научные центры и т.д. в настоящее время являются практически беззащитными против хорошо организованных компьютерных атак.

Тема 2. Информационная безопасность в условиях функционирования в России глобальных сетей

2.1. Общие сведения о безопасности в компьютерных сетях

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т.п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые или удаленные угрозы. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычислительных сетях наиболее частыми являются угрозы раскрытия и целостности, то в сетевых системах на первое место выходит угроза отказа в обслуживании.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи.

Это определение охватывает обе особенности сетевых систем – распределенность компьютеров и распределенность информации. Поэтому при рассмотрении вопросов информационной безопасности вычислительных сетей рассматриваются два подвида удаленных угроз – это удаленные угрозы на инфраструктуру и протоколы сети и удаленные угрозы на телекоммуникационные службы. Первые используют уязвимости в сетевых

протоколах и инфраструктуре сети, а вторые – уязвимости в телекоммуникационных службах.

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих "информационной безопасности":

1. Целостность данных – одна из основных целей информационной безопасности сетей - предполагает, что данные не были изменены, подменены или уничтожены в процессе их передачи по линиям связи, между узлами вычислительной сети. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.
2. Конфиденциальность данных – вторая главная цель сетевой безопасности. При информационном обмене в вычислительных сетях большое количество информации относится к конфиденциальной, например, личная информация пользователей, учетные записи (имена и пароли), данные о кредитных картах и др.
3. Доступность данных – третья цель безопасности данных в вычислительных сетях. Функциями вычислительных сетей являются совместный доступ к аппаратным и программным средствам сети и совместный доступ к данным. Нарушение информационной безопасности как раз и связана с невозможностью реализации этих функций.

В локальной сети должны быть доступны: принтеры, серверы, рабочие станции, данные пользователей и др.

В глобальных вычислительных сетях должны быть доступны информационные ресурсы и различные сервисы, например, почтовый сервер, сервер доменных имен, web-сервер и др.

При рассмотрении вопросов, связанных с информационной безопасностью, в современных вычислительных сетях необходимо учитывать следующие факторы:

- глобальную связанность;
- разнородность корпоративных информационных систем;
- распространение технологии "клиент/сервер".

Применительно к системам связи глобальная связанность означает, что речь идет о защите сетей, пользующихся внешними сервисами, основанными на протоколах TCP/IP, и предоставляющих аналогичные сервисы вовне. Весьма вероятно, что внешние сервисы находятся в других странах, поэтому от средств защиты в данном случае требуется следование стандартам, признанным на

международном уровне. Национальные границы, законы, стандарты не должны препятствовать защите потоков данных между клиентами и серверами.
Из факта глобальной связанности вытекает также меньшая эффективность мер физической защиты, общее усложнение проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, например, межсетевых экранов.
Разнородность аппаратных и программных платформ требует от изготовителей средств защиты соблюдения определенной технологической дисциплины. Важны не только чисто защитные характеристики, но и возможность встраивания этих систем в современные корпоративные информационные структуры. Если, например, продукт, предназначенный для криптографической защиты, способен функционировать исключительно на платформе Wintel (Windows+Intel), то его практическая применимость вызывает серьезные сомнения.
Корпоративные информационные системы оказываются разнородными еще в одном важном отношении – в разных частях этих систем хранятся и обрабатываются данные разной степени важности и секретности.
Использования технологии "клиент/сервер" с точки зрения информационной безопасности имеет следующие особенности:

- каждый сервис имеет свою трактовку главных аспектов информационной безопасности (доступности, целостности, конфиденциальности);
- каждый сервис имеет свою трактовку понятий субъекта и объекта;
- каждый сервис имеет специфические угрозы;
- в каждый сервис нужно по-своему администрировать;
- средства безопасности в каждый сервис нужно встраивать по-особому.

Специфика средств защиты в компьютерных сетях
Особенности вычислительных сетей и, в первую очередь, глобальных, предопределяют необходимость использования специфических методов и средств защиты, например:

- защита подключений к внешним сетям;
- защита корпоративных потоков данных, передаваемых по открытым сетям;
- защита потоков данных между клиентами и серверами;
- обеспечение безопасности распределенной программной среды;
- защита важнейших сервисов (в первую очередь Web-сервиса);

В последнее время все четче просматривается незащищенность вычислительных сетей от глобальных атак.

2.2. Сетевые модели передачи данных

Понятие протокола передачи данных

Обмен информацией между ЭВМ на больших расстояниях всегда казался более важной задачей, чем локальный обмен. Поэтому ему уделялось больше внимания и, соответственно, велось большее финансирование во многих странах. Один из немногих открытых проектов по исследованию вычислительных сетей, финансировавшийся военным ведомством США, известен под названием сеть ARPA – Advanced Research Projects Agency. С самого начала в рамках этого проекта велись работы по объединению ресурсов многих вычислительных машин различного типа. В 1960 – 1970-е годы многие результаты, полученные при эксплуатации сети ARPA, были опубликованы в открытой печати. Это обстоятельство, а также тот факт, что почти все страны занялись практически слепым копированием не только аппаратной архитектуры американских машин, но и базового программного обеспечения, обусловили сильное влияние сети ARPA на многие другие сети, именно поэтому принято считать, что сеть ARPA является предшественницей знаменитой всемирной компьютерной сети Интернет.

Основной задачей сетевой общественности явилась разработка протоколов обмена информацией. Эта задача совершенно справедливо представлялась важнейшей, поскольку настоятельно требовалось заставить понимать друг друга компьютеры, обладавшие различной архитектурой и программным обеспечением. Первоначально разработчики многочисленных корпоративных сетей договаривались о внутренних протоколах информационного обмена в своих сетях. Никакой стандартизации не было. Но уже в 70-е годы специалистам стало совершенно ясно, что стандартизация необходима и неизбежна. В эти годы шел бурный процесс создания многочисленных национальных и международных комитетов и комиссий по стандартизации программных и аппаратных средств в области вычислительной техники и информационного обмена.

Протокол сетевого обмена информацией можно определить как перечень форматов передаваемых блоков данных, а также правил их обработки и соответствующих действий.

Другими словами, протокол обмена данными – это подробная инструкция о том, какого типа информация передается по сети, в каком порядке обрабатываются данные, а также набор правил обработки этих данных.

Человек – оператор компьютера, включенного в сеть, тем или иным способом, например, с помощью программ-приложений, формирует и передает по сети сообщения, предназначенные для других людей или компьютеров. В ответ он также ожидает поступления сообщения. В этом смысле сообщение представляет собой логически законченную порцию информации, предназначенную для потребления конечными пользователями – человеком или

прикладной программой. Например, это может быть набор алфавитно-цифровой и графической информации на экране или файл целиком. Сейчас сообщения неразрывно связывают с прикладным уровнем или, как его еще называют, уровнем приложений сетевых протоколов.

Сообщения могут проходить довольно сложный путь по сетям, стоять в очередях на передачу или обработку, в том числе не доходить до адресата, о чем отправитель также должен быть уведомлен специальным сообщением.

Первоначально вычислительные сети были сетями коммутации сообщений. Это было оправдано, пока сообщения были сравнительно короткими. Но параллельно с этим всегда существовали задачи передачи на расстояние больших массивов информации. Решение этой задачи в сетях с коммутацией сообщений является неэффективным, поскольку длины сообщений имеют большой разброс – от очень коротких до очень длинных, что характерно для компьютерных сетей.

В связи с этим было предложено разбивать длинные сообщения на части (пакеты) и передавать сообщения не целиком, а пакетами, вставляя в промежутках пакеты других сообщений. На месте назначения сообщения собираются из пакетов. Короткие сообщения при этом были вырожденным случаем пакета, равного сообщению.

В настоящее время почти все сети в мире являются сетями коммутации пакетов.

Принципы организации обмена данными в вычислительных сетях

Существуют два принципа организации обмена данными:

- установление виртуального соединения с подтверждением приема каждого пакета;
- передача датаграмм.

Установление виртуального соединения или создание виртуального канала является более надежным способом обмена информацией. Поэтому он более предпочтителен при передаче данных на большие расстояния и по физическим каналам, в которых возможны помехи. При виртуальном соединении пункт приема информации уведомляет отправителя о правильном или неправильном приеме каждого пакета. Если какой-то пакет принят неправильно, отправитель повторяет его передачу. Так длится до тех пор, пока все сообщение не будет успешно передано. На время передачи информации между двумя пунктами коммутируется канал, подобный каналу при телефонном разговоре. Виртуальным его называют потому, что в отличие от телефонного коммутированного канала обмен информацией может идти по различным физическим путям даже в процессе передачи одного сообщения.

Термин датаграмма образован по аналогии с термином телеграмма. Аналогия заключается том, что короткие пакеты – собственно датаграммы –

пересылаются адресату без подтверждения получения каждого из них. О получении всего сообщения целиком должна уведомить целевая программа.

Транспортный протокол TCP и модель TCP/IP

За время развития вычислительных сетей было предложено и реализовано много протоколов обмена данными, самыми удачными из которых явились семейство протоколов TCP/IP (Transmission Control Protocol/ Internet Protocol – протокол управления передачей/ межсетевой протокол).

TCP/IP – это набор протоколов, состоящий из следующих компонентов:

- межсетевой протокол (InternetProtocol), обеспечивающий адресацию в сетях (IP-адресацию);
- межсетевой протокол управления сообщениями (Internet Control Message Protocol – ICMP), который обеспечивает низкоуровневую поддержку протокола IP, включая такие функции, как сообщения об ошибках, квитанции, содействие в маршрутизации и т. п.;
- протокол разрешения адресов (Address Resolution Protocol – ARP), выполняющий преобразование логических сетевых адресов в аппаратные, а также обратный ему RARP (Reverse ARP);
- протокол пользовательских датаграмм (User Datagram Protocol – UPD);
- протокол управления передачей (Transmission Control Protocol – TCP).

Протокол UDP обеспечивает передачу пакетов без проверки доставки, в то время как протокол TCP требует установления виртуального канала и соответственно подтверждения доставки пакета с повтором в случае ошибки.

Этот набор протоколов образует самую распространенную модель сетевого обмена данными, получившую название TCP/IP.

Модель TCP/IP иерархическая и включает четыре уровня:

Таблица 2.1 – Уровни иерархической модели TCP/IP

Уровень	**Название**	**Функция**
4	Прикладной	Приложения пользователей, создание сообщений
3	Транспортный	Доставка данных между программами в сети
2	Сетевой	Адресация и маршрутизация
1	Канальный	Сетевые аппаратные средства и их драйверы

1. Прикладной уровень определяет способ общения пользовательских приложений. В системах "клиент-сервер" приложение-клиент должно знать, как посылать запрос, а приложение-сервер должно знать, как ответить на запрос. Этот уровень обеспечивает такие протоколы, как HTTP, FTP, Telnet.

2. Транспортный уровень позволяет сетевым приложениям получать сообщения по строго определенным каналам с конкретными параметрами.
3. На сетевом уровне определяются адреса включенных в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними.
4. На канальном уровне определяется адресация физических интерфейсов сетевых устройств, например, сетевых плат. К этому уровню относятся программы управления физическими сетевыми устройствами, так называемые драйверы.

Как уже отмечалось ранее, в сетях с коммутацией пакетов, а модель TCP/IP относится к таким, для передачи по сети сообщение (сформированное на прикладном уровне) разбивается на пакеты или датаграммы. Пакет или датаграмма – это часть сообщения с добавленным заголовком пакета или датаграммы.

На транспортном уровне к полезной информации добавляется заголовок – служебная информация. Для сетевого уровня полезной информацией является уже пакет или датаграмма транспортного уровня. К ним добавляется заголовок сетевого уровня.

Полученный блок данных называется IP-пакетом. Полезной нагрузкой для канального уровня является уже IP-пакет. Здесь перед передачей по каналу к нему добавляются собственный заголовок и еще завершитель. Получившийся блок называется кадром. Он и передается по сети.

Переданный по сети кадр в пункте назначения преобразуется в обратном порядке, проходя по уровням модели снизу вверх.

2.3. Модель взаимодействия открытых систем OS1/ISO

Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO

В конце 80-х годов наблюдался подлинный бум, вызванный разработкой Международной организации по стандартизации коммуникационных протоколов – (International Standard Organization). Разработанная ISO спецификация, названная моделью взаимодействия открытых систем (OSI – Open Systems Interconnection), заполонила научные публикации. Казалось, что эта модель займет первое место и оттеснит широко распространившийся TCP/IP. Но этого не произошло. Одной из причин явилась тщательная проработка протоколов TCP/IP, их функциональность и открытость к наращиванию функциональных возможностей, хотя к настоящему времени достаточно очевидно, что они имеют и множество недостатков. Приведем сравнительную схему уровневых моделей протоколов OSI и TCP/IP (см. таблицу 2.2).

Таблица 2.2 – Сравнение уровневых моделей протоколов OSI и TCP/IP

OSI		**TCP/IP**	
7	Прикладной уровень	4	Прикладной уровень
6	Представительный уровень	3	Транспортный уровень
5	Сеансовый уровень	2	Межсетевой уровень
4	Транспортный уровень	1	Сетевой уровень
3	Сетевой уровень		
2	Канальный уровень		
1	Физический уровень		

Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют две стороны, то есть в данном случае необходимо организовать согласованную работу двух "иерархий", работающих на разных компьютерах. Оба участника сетевого обмена должны принять множество соглашений. Например, они должны согласовать уровни и форму электрических сигналов, способ определения длины сообщений, договориться о методах контроля достоверности и т. п. Другими словами, соглашения должны быть приняты для всех уровней, начиная от самого низкого – уровня передачи битов – до самого высокого, реализующего сервис для пользователей сети.

Распределение функций безопасности по уровням модели OSI/ISO

Модель взаимодействия открытых систем (Open System Interconnection, OSI) определяет различные уровни взаимодействия систем в сетях с коммутацией пакетов, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

Модель OSI была разработана на основании большого опыта, полученного при создании компьютерных сетей, в основном глобальных, в 70-е годы. В модели OSI средства взаимодействия делятся на семь уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень имеет дело с определенным аспектом взаимодействия сетевых устройств.

1. **Физический уровень**

   Физический уровень имеет дело с передачей битов по физическим каналам связи, таким, как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение

характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и другие.

2. **Канальный уровень**

Одной из задач канального уровня является проверка доступности среды передачи. Другая задача канального уровня – реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами (frames). Канальный уровень обеспечивает корректность передачи каждого кадра.

3. **Сетевой уровень**

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей. Внутри одной сети доставка данных обеспечивается канальным уровнем, а вот доставкой данных между различными сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами.

Маршрутизатор – это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями.

4. **Транспортный уровень**

Транспортный уровень обеспечивает приложениям или верхним уровням стека – прикладному и сеансовому – передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное – способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

5. **Сеансовый уровень**

Сеансовый уровень обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

6. **Представительный уровень**

   Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например, в кодах ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

7. **Прикладной уровень**

   Прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением.

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня – физический, канальный и сетевой – являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

Три верхних уровня – прикладной, представительный и сеансовый – ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было

изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.

Столь подробное рассмотрение модели OSI/ISO связано с тем, что при разработке стандартов и спецификации по сетевой безопасности специалисты ориентируются на эту перспективную модель. Так, в "Общих критериях" приводится распределение функций безопасности по уровням эталонной семиуровневой модели OSI, показано в таблице 2.3.

Таблица 2.3 – Распределение функций безопасности по уровням OSI/ISO

Функция безопасности	**Уровень OSI**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединения	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

- "+" – данный уровень может предоставить функцию безопасности;
- "-" – данный уровень не подходит для предоставления функции безопасности.

2.4. Адресация в глобальных сетях

Основы IP-протокола

Одной из главных проблем построения глобальных сетей является проблема адресации. С одной стороны, постоянное расширение глобальной сети Интернет привело к нехватке уникальных адресов для вновь подключаемых узлов. С другой стороны, система адресации в таких сетях должна быть

защищена от возможного вмешательства злоумышленников, связанных с подменой адресов и реализацией обходных маршрутов передачи сообщений.

Адресация современного Интернета основана на протоколе IP (Internet Protocol), история которого неразрывно связана с транспортным протоколом TCP.

Концепция протокола IP представляет сеть как множество компьютеров (хостов), подключенных к некоторой интерсети. Интерсеть, в свою очередь, рассматривается как совокупность физических сетей, связанных маршрутизаторами. Физические объекты (хосты, маршрутизаторы, подсети) идентифицируются при помощи специальных IP-адресов. Каждый IP-адрес представляет собой 32-битовый идентификатор. Принято записывать IP-адреса в виде 4-х десятичных чисел, разделенных точками.

Для этого 32-х битовый IP-адрес разбивается на четыре группы по 8 бит (1 байт), после чего каждый байт двоичного слова преобразовывается в десятичное число по известным правилам. Например, IP-адрес:

10010011 10000111 00001110 11100101

преобразовывается указанным способом к следующему виду: 147.135.14.229.

Классы адресов вычислительных сетей

Каждый адрес является совокупностью двух идентификаторов: сети – NetID, и хоста – HostID. Все возможные адреса разделены на 5 классов, схема которых приведена на рисунке 2.1.

Из рисунка 2.1 видно, что классы сетей определяют как возможное количество этих сетей, так и число хостов в них. Практически используются только первые три класса:

Класс A определен для сетей с числом хостов до 16777216. Под поле NetID отведено 7 бит, под поле HostID – 24 бита.

Класс B используется для среднемасштабных сетей (NetID – 14 бит, HostID – 16 бит). В каждой такой сети может быть до 65536 хостов.

Класс C применяется для небольших сетей (NetID – 21 бит, HostID – 8 бит) с числом хостов до 255.

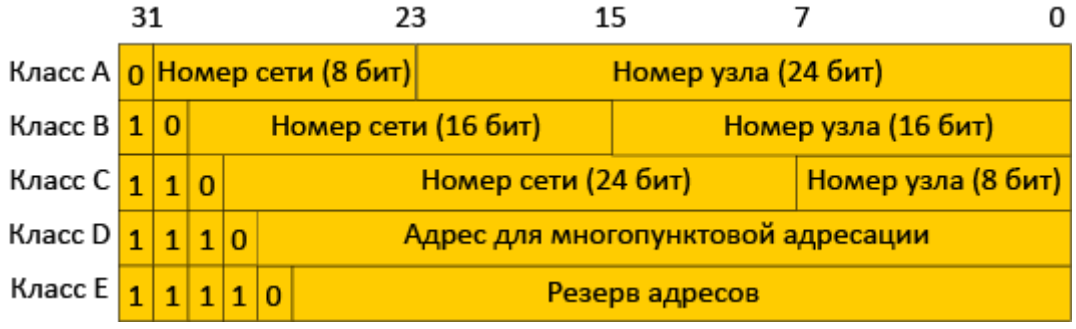


Рисунок 2.1 – Классы адресов вычислительных сетей

Система доменных имен

Постоянное расширение сети Internet привело к дефициту уникальных адресов для вновь подключаемых узлов. С другой стороны, система адресации в такой сети должна быть универсальной и удобной для пользователя. Последнее обстоятельство особенно было важно с началом использования ресурсов сети не только специалистами, но и неподготовленными пользователями, не владеющими тонкостями адресации в сети. Решающим аргументом для перехода к альтернативным способам адресации в сети, удобным для работы пользователей, было неудобство запоминания 32-х битового кода, идентифицирующего отдельный узел. Это неудобство проявилось сразу же, когда сеть использовалась узким кругом специалистов. Поэтому появилась альтернативные формы записи 32-х битового IP-адреса – десятичная (195.224.11.77) и шестнадцатеричная (0xffffff80) дот-нотации. Последняя форма записи особенно была удобной для программистов, часто применяющих шестнадцатеричный алфавит для записи кода программы.

Впоследствии с появлением в сети различных сервисов (электронная почта и другие службы), а также с увеличением числа узлов и такая форма записи оказалась неудобной, поскольку достаточно сложно запомнить несколько цифровых адресов, даже в десятичной дот-нотации. Это обусловило появление в сети ARPANET принципиально нового способа адресации, заключающегося в присвоении узлам сети доменного имени. В данном случае правильнее говорить о новом способе именования узлов сети, поскольку доменное имя не является логическим адресом, например, как IP-адрес или физическим адресом, как, например, шестибайтовый адрес сетевого интерфейса. Доменное имя – это только лишь удобная для пользователя форма идентификации узла вычислительной сети (сервис).

Домен – группа узлов сети (хостов), объединенных общим именем, которое для удобства несет определенную смысловую нагрузку.

Например, домен "ru" объединяет узлы на территории России, а домен "sport" – узлы, относящиеся к спортивным организациям или содержащие информацию о спорте и т. д.

В более широком смысле под доменом понимается множество узлов вычислительной сети, которые администрируются и поддерживаются как одно целое.

Доменное имя – это уникальный алфавитно-цифровой идентификатор узла (состоит из символов ASCII-кода – букв от A до Z латинского алфавита и цифр от 0 до 9, также допускается дефис "-").

Введение доменных имен поставило перед разработчиками задачу определения соответствия между доменным именем и логическим IP-адресом узла сети.

Подобная задача разработчиками ARPANET была решена, когда для определения соответствия между логическим IP-адресом и физическим адресом сетевого интерфейса в пределах локальной сети были введены протоколы ARP и RARP. Однако для глобальной сети решение такой задачи является более сложным.

Первоначально, когда ARPANET состояла из небольшого числа узлов, соответствие между доменными именами и IP-адресами узлов перечислялось в одном файле (hosts.txt) в виде таблицы соответствия цифрового адреса имени машины.

Авторство создания этих таблиц принадлежит Джону Постелю. Именно он первым поддерживал файл hosts.txt, который можно было получить по FTP. Этот файл хранился в сетевом информационном центре Стэндфордского исследовательского института (SRI). Администраторы сетей передавали в SRI дополнения и изменения, происшедшие в конфигурации администрируемой ими сети. Периодически администраторы переписывали этот файл в свои системы.

В локальных сетях файлы hosts используются достаточно успешно до сих пор. Практически все операционные системы от различных версий Unix до Windows последних версий поддерживают эту систему соответствия IP-адресов именам хостов.

Пользователь для обращения к узлу мог использовать как IP-адрес узла, так и его имя. Процедура использования имени заключается в следующем: сначала по имени в файле hosts находят IP-адрес, а затем по IP-адресу устанавливают соединение с удаленным информационным ресурсом.

С ростом сети ARPANET это стало чрезвычайно затруднительно, поскольку файл увеличивался в размерах, а его пересылка по сети и хранение на каждом узле требовало значительных ресурсов. Однако главное неудобство заключалось в том, что такой способ не позволял оперативно учитывать все изменения в сети.

В 1984 году в сети ARPANET стала использоваться служба, получившая название системы доменных имен (Domain Name System – DNS). DNS была описана Полом Мокапетрисом в двух документах: RFC-882 и RFC-883 (позже эти документы были заменены на RFC-1034 и RFC-1035).

В соответствии с RFC-1034 и RFC-1035, описывающими DNS, роль доменного имени в процессе установки соединения осталась прежней. Это значит, что главное, для чего используется DNS служба, – это получение IP-адреса узла сети. Исходя из этого, любая реализация DNS является прикладным процессом, который работает над стеком протоколов межсетевого обмена TCP/IP. Таким образом, базовым элементом адресации в сетях TCP/IP с введением DNS

остался IP-адрес, а доменное именование (система доменных имен) играет роль вспомогательного сервиса.

DNS состоит из трех основных частей:

- пространство (множество) доменных имен (domain name space);
- серверов доменных имен (domain name servers);
- клиентов DNS (Resolver).

Пространство доменных имен имеет вид дерева (иерархии) узлов, как показано на рисунке 3 и подчиняется следующим правилам (RFC-1034):

- имя корня – пустая строка, то есть полное имя обязательно завершается точкой[1];
- каждый узел дерева должен быть помечен простым именем, включающим допустимые символы;
- прописные и строчные буквы в доменных именах не различаются;
- допустимая длина простого имени не более 63 символов;
- доменные имена узлов в пределах одного домена должны быть уникальны;
- допускается применение одинаковых доменных имен в разных доменах, как показано на рисунке 3, где доменное имя ".mil" используется для обозначения домена первого уровня и домена второго уровня, являющегося поддоменом домена ".ru";
- полное имя узла образуется из последовательности имени самого узла и всех имен доменов, которые с ним связаны (снизу вверх по соответствующей ветви дерева) до корня включительно, записываемых слева направо и разделяемых точками, например, как показано на рисунке 3, узлу ".Ekfacultet" соответствует следующее полное доменное имя ".Ekfacultet.urgi.krasnoyarsk.ru";
- максимальная длина полного имени – 255 символов, включая точки;
- максимальное число уровней дерева – 127[2];
- кроме полного (абсолютного) имени узла (FQDN, fully qualified domain name) допускается применение относительного (относительно некоторого опорного узла) имени, в этом случае завершающая точка отсутствует;
- поддерево доменных имен вместе со своим корневым узлом называется доменом (поддоменом), например, обозначенная на рисунке 3 ветвь относится к группе узлов (".Ekfacultet", ".Urfacultet", ".Phfacultet", ".Dizfacultet", ".Reefacultet") и под-Доменов ("krasnoyarsk." ".urgi"), входящих в домен ".ru", а все узлы, показанные на рисунке 6 на самом нижнем уровне, входят в домен (поддомен) третьего уровня ".urgi" и т. д.

- объединение узлов в домены является чисто логическим, то есть не зависящим ни от месторасположения, ни от IP-адреса, ни от способа маршрутизации.

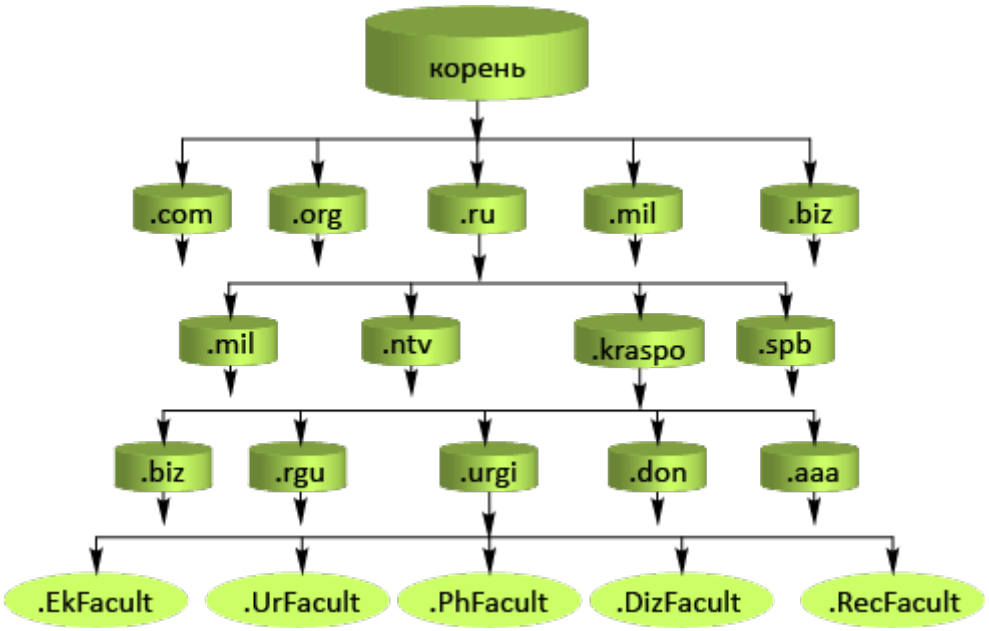


Рисунок 2.2 – Система доменных имен

Полное доменное имя узла используется как ключевая информация для поиска IP-адреса узла в базе данных, содержащей таблицы соответствия доменных имен и логических адресов.

Корень – это множество все узлов Internet. Данное множество подразделяется на домены первого или верхнего уровня (top-level или TLD).

Корневой зоной Internet и системой корневых серверов управляет ICANN, в частности, ICANN делегирует (передает) права управления зонами первого уровня gTLD (generic top-level domains, домены верхнего организационного уровня) и ccTLD (country code top-level domains, национальные домены).

В соответствии с принятыми правилами право администрирования каждого домена первого уровня передается одной конкретной организации (оператору регистра; администратором доменной зоны "ru" является РосНИИРОС). Зарегистрировать домен второго уровня, например, в доменной зоне "ru" можно у одного из многочисленных регистраторов (коммерческие организации, имеющие доступ к общей базе данных оператора регистра для данной доменной зоны).

Первоначально в ARPANET было семь доменов верхнего организационного уровня:

1. com (коммерческие организации);
2. edu (образовательные организации, в основном из США);
3. gov (правительственные организации США);

4. int (международные организации);
5. mil (военные организации США);
6. net(организации, обеспечивающие сетевую инфраструктуру);
7. org (некоммерческие организации).

В 90-х годах к ним были добавлены следующие домены:

1. aero (организации, связанные с авиацией);
2. arpa (используется для отображения адресов в имена);
3. biz (коммерческие организации);
4. coop (кооперативы);
5. info (разное);
6. museum (музеи);
7. name (персональные домены);
8. pro (лицензированные профессионалы).

Список доменов ccTLD базируется на стандарте двухбуквенных кодов государств и территорий (ISO 3166).

Примеры доменов верхнего уровня ccTLD, соответствующие отдельным государствам, приведены в таблице 2.4.

В Internet система доменных имен реализована в виде распределенной базы данных, включающей в себя серверы DNS, клиенты DNS (resolver), объединенные общим протоколом запросов к базе данных и обмена информацией между серверами.

Таблица 2.4 – Примеры национальных доменов верхнего уровня

Страна	**Код**	**Страна**	**Код**
Аргентина	ar	Кипр	cy
Армения	am	Киргизстан	kg
Австрия	at	Казахстан	kz
Азербайджан	az	Канада	ca
Белорусь	by	Индия	id
Бельгия	be	Латвия	lv
Болгария	bg	Литва	lt
Чехия	cz	Молдова	md
Эстония	ee	Нидерланды	nl
Финляндия	fi	Польша	pl
Франция	fr	Португалия	pt
Германия	de	Россия	ru

Греция	gr	Словакия	sk
Грузия	ge	Словения	si
Дания	dk	Испания	es
Венгрия	hu	Швеция	se
Италия	it	Швейцария	ch
Япония	jp	Узбекистан	uz
Украина	ua	Туркменистан	tm
Великобритания	gb	Соединенные Штаты	us

Информация, соответствующая каждому доменному имени, хранится в записях ресурсов RR (resource records) DNS-сервера. Основным типом хранимой информации является IP-адрес. Одному доменному имени может соответствовать несколько IP-адресов (в случае использования нескольких сетевых интерфейсов на компьютере). Кроме этого, в записях ресурсов может храниться дополнительная информация, например, максимально допустимое время кэширования[3] полученной информации (TTL, time to live).

В системе доменных имен различают несколько типов DNS-серверов.

В зависимости от типа отклика на запрос серверы делятся на авторитетные (authoritative) и неавторитетные (non authoritative).

- Авторитетный отклик (authoritative response) возвращают серверы, которые являются ответственными за зону, в которой описана информация, необходимая клиенту DNS.
- Неавторитетный отклик (non authoritative response) возвращают серверы, которые не отвечают за зону, содержащую необходимую клиенту информацию.

В зависимости от способа поддержания базы данных авторитетные DNS-серверы делятся на первичные (primary) и дублирующие (secondary).

- Первичный сервер доменных имен является ответственным за информацию о конкретной доменной зоне[4] и поэтому хранит эту информацию, загружает ее для ответов клиентам с локального диска узла, на котором он функционирует. Описание зоны этого сервера ведется непосредственно администратором зоны.
- Дублирующий сервер доменных имен также является ответственным за эту доменную зону. В его функции входит дублирование первичного сервера на случай нарушения его работы. Кроме этого, дублирующий

сервер, обрабатывая часть запросов, снимает нагрузку с первичного сервера.

Администратор дублирующего сервера не изменяет данные описания доменной зоны, а только обеспечивает синхронизацию базы данных дублирующего сервера с базой данных первичного сервера.

Примером такой организации является система корневых (root-servers) DNS-серверов Internet. Всего в сети Internet 13 корневых DNS-серверов.

Корневые серверы являются основой всей системы доменных имен, поскольку являются авторитетными серверами для корневой зоны и содержат ссылки на такие же серверы зон первого уровня или сами являются авторитетными серверами некоторых зон первого уровня (например, com. или net.).

На запрос о домене корневой сервер возвращает как минимум имя и адрес уполномоченного сервера домена первого уровня, в который входит указанный в запросе узел. Обратившись по полученному адресу, можно получить имя и адрес уполномоченного сервера домена второго уровня и т. д.

Из всего списка корневых серверов только один из них (A.ROOT-SERVERS.NET) является первичным, а все остальные дублирующие, хотя они содержат идентичную информацию.

Благодаря такой организации Internet выдержал несколько глобальных атак злоумышленников.

Защита DNS-серверов любого уровня, а особенно корневых, является одной из проблем современной сети Internet.

Обобщенная схема работы системы доменных имен следующая.

Пользователь инициирует запрос к web-серверу (например к "www.urgi.ru"). В соответствии с настройками сетевого подключения DNS-клиент формирует DNS-запрос к ближайшему DNS-серверу (как правило, по умолчанию DNS-сервер провайдера) об IP-адресе узла, на котором функционирует данный web-сервер.

Если DNS-сервер провайдера является авторитетным для доменной зоны ".ru", то он возвращает узлу пользователя (а вернее программе, инициировавшей запрос) DNS-отклик, в котором содержится требуемый IP-адрес (в предположении, что такой web-сервер вообще зарегистрирован).

В случае, если DNS-сервер провайдера не является авторитетным для доменной зоны ".ru", то он формирует аналогичный DNS-запрос к вышестоящему DNS-серверу (чаще всего, но не обязательно, корневому DNS-серверу). Корневой DNS-сервер в ответ на полученный запрос формирует DNS-отклик, в котором содержится IP-адрес авторитетного для данной доменной зоны DNS-сервера, получив который, DNS-сервер провайдера сформирует к нему запрос и полученный отклик вернет клиенту. При этом полученная информация будет

занесена в кэш-память DNS-сервера провайдера. В случае повторного запроса от пользователя IP-адреса web-сервера (например к "www.urgi.ru"), DNS-сервер провайдера сформирует отклик, используя информацию из кэш-памяти, и не будет обращаться к вышестоящему DNS-серверу.

Запросы клиентов (или серверов) могут быть рекурсивными или итеративными. Рекурсивный запрос подразумевает, что запрашиваемый сервер должен самостоятельно пробежаться по всей системе серверов (вплоть до корневого) до получения конечного ответа (в том числе отрицательного) и вернуть его клиенту. При этом сам сервер может пользоваться итеративными или рекурсивными запросами. Сервер может отказаться выполнять рекурсивные запросы "сторонних" клиентов. При итеративном запросе сервер делает только один шаг поиска и возвращает ссылку на авторитетный сервер (или конечный ответ, если он сам является авторитетным для данного домена). Дальнейший поиск производится самим клиентом.

Очевидно, что сервер доменных имен и клиентское программное обеспечение реализуют заложенную в DNS архитектуру "клиент-сервер", а программные средства, указанные в последнем пункте, позволяют упростить настройку сервера и управление им.

История развития сети Интернет показывает, что DNS-сервер является объектом атак со стороны злоумышленников, поскольку, выведя из строя этот сервер или изменив данные его базы, можно, нарушить работу сети.

2.5. Классификация удаленных угроз в вычислительных сетях

Удаленные угрозы можно классифицировать по следующим признакам.

По характеру воздействия:

- пассивные (класс 1.1): Пассивным воздействием на распределенную вычислительную систему называется воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу сети приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в вычислительных сетях является прослушивание канала связи в сети.
- активные (класс 1.2): Под активным воздействием на вычислительную сеть понимается воздействие, оказывающее непосредственное влияние на работу сети (изменение конфигурации, нарушение работоспособности и т. д.) и нарушающее принятую в ней политику безопасности. Практически все типы удаленных угроз являются активными воздействиями.

По цели воздействия:

- нарушение конфиденциальности информации (класс 2.1);
- нарушение целостности информации (класс 2.2);
- нарушение доступности информации (работоспособности системы) (класс 2.3).

Этот классификационный признак является прямой проекцией трех основных типов угроз – раскрытия, целостности и отказа в обслуживании.

Одна из основных целей злоумышленников – получение несанкционированного доступа к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. Примером перехвата информации может служить прослушивание канала в сети. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения. Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Данное информационное разрушающее воздействие представляет собой яркий пример активного воздействия. Примером удаленной угрозы, цель которой нарушение целостности информации, может служить типовая удаленная атака "ложный объект распределенной вычислительной сети".

Принципиально другая цель преследуется злоумышленником при реализации угрозы для нарушения работоспособности сети. В этом случае не предполагается получение несанкционированного доступа к информации. Его основная цель – добиться, чтобы узел сети или какой-то из сервисов, поддерживаемый им, вышел из строя и для всех остальных объектов сети доступ к ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить типовая удаленная атака "отказ в обслуживании".

По условию начала осуществления воздействия

Удаленное воздействие так же, как и любое другое, может начать осуществляться только при определенных условиях. В вычислительных сетях можно выделить три вида условий начала осуществления удаленной атаки:

- атака по запросу от атакуемого объекта (класс 3.1). В первом случае злоумышленник ожидает передачи от потенциальной цели атаки запроса

определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети Internet служат DNS-запросы. Отметим, что данный тип удаленных атак наиболее характерен для распределенных вычислительных сетей.

- атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2). Во втором случае злоумышленник осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект.
- безусловная атака (класс 3.3). Реализация третьего вида атаки не связана ни с какими событиями и реализуется безусловно по отношению к цели атаки, то есть атака осуществляется немедленно.

По наличию обратной связи с атакуемым объектом:

- с обратной связью (класс 4.1);
- без обратной связи (однонаправленная атака) (класс 4.2).

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, а следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адекватно реагировать на все изменения, происходящие на атакуемом объекте.

В отличие от атак с обратной связью удаленным атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную удаленную атаку можно называть однонаправленной удаленной атакой. Примером однонаправленных атак является типовая удаленная атака "отказ в обслуживании".

По расположению субъекта атаки относительно атакуемого объекта:

- внутрисегментное (класс 5.1);
- межсегментное (класс 5.2).

Рассмотрим ряд определений.

Субъект атаки (или источник атаки) – это атакующая программа или злоумышленник, непосредственно осуществляющие воздействие.

Маршрутизатор (router) – устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.

Подсеть (subnetwork) – (в терминологии Internet) совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен

одинаковый номер подсети. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

Сегмент сети – физическое объединение хостов.

Например, сегмент сети образует совокупность хостов, подключенных к серверу по схеме "общая шина". При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте.

С точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объект атаки, то есть в одном или в разных сегментах они находятся. В случае внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах. Данный классификационный признак позволяет судить о так называемой "степени удаленности" атаки.

Важно отметить, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект её и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по локализации субъекта атаки.

По уровню модели ISO/OSI, на котором осуществляется воздействие:

- физический (класс 6.1);
- канальный (класс 6.2);
- сетевой (класс 6.3);
- транспортный (класс 6.4);
- сеансовый (класс 6.5);
- представительный (класс 6.6);
- прикладной (класс 6.7).

2.6. Типовые удаленные атаки и их характеристика

Типовая удаленная атака – это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной сети.

Основной особенностью распределенной вычислительной сети является распределенность ее объектов в пространстве и связь между ними по физическим линиям связи. При этом все управляющие сообщения и данные, пересылаемые между объектами вычислительной сети, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность привела к появлению специфичного для распределенных вычислительных сетей типового удаленного воздействия, заключающегося в прослушивании канала связи, называемого анализом сетевого трафика.

Анализ сетевого трафика позволяет:

- изучить логику работы распределенной вычислительной сети, это достигается путем перехвата и анализа пакетов обмена на канальном уровне (знание логики работы сети позволяет на практике моделировать и осуществлять другие типовые удаленные атаки);
- перехватить поток данных, которыми обмениваются объекты сети, то есть удаленная атака данного типа заключается в получении несанкционированного доступа к информации, которой обмениваются пользователи (примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети).

Одной из проблем безопасности распределенной ВС является недостаточная идентификация и аутентификация (определение подлинности) удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. Обычно в вычислительных сетях эта проблема решается использованием виртуального канала, по которому объекты обмениваются определенной информацией, уникально идентифицирующей данный канал. Для адресации сообщений в распределенных вычислительных сетях используется сетевой адрес, который уникален для каждого объекта системы (на канальном уровне модели OSI – это аппаратный адрес сетевого адаптера, на сетевом уровне – адрес определяется протоколом сетевого уровня (например, IP-адрес). Сетевой адрес также может использоваться для идентификации объектов сети.

В том случае, когда в вычислительной сети используют нестойкие алгоритмы идентификации удаленных объектов, оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта сети, то есть подмена объекта или субъекта сети.

Недостаточно надежная идентификация сетевых управляющих устройств (например, маршрутизаторов) является причиной возможного внедрения в сеть ложного объекта путем изменения маршрутизации пакетов, передаваемых в сети.

Современные глобальные сети представляют собой совокупность сегментов сети, связанных между собой через сетевые узлы. При этом маршрутом называется последовательность узлов сети, по которой данные передаются от источника к приемнику. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждого адресата указывается оптимальный маршрут. Таблицы маршрутизации существуют не только у маршрутизаторов, но и у любых хостов (узлов) в глобальной сети. Для

обеспечения эффективной и оптимальной маршрутизации в распределенных ВС применяются специальные управляющие протоколы, позволяющие маршрутизаторам обмениваться информацией друг с другом (RIP (Routing Internet Protocol), OSPF (Open Shortest Path First)), уведомлять хосты о новом маршруте – ICMP (Internet Control Message Protocol), удаленно управлять маршрутизаторами (SNMP (Simple Network Management Protocol)). Эти протоколы позволяют удаленно изменять маршрутизацию в сети Интернет, то есть являются протоколами управления сетью.

Реализация данной типовой удаленной атаки заключается в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются объекты сети, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов вычислительной сети.

Получив контроль над проходящим потоком информации между объектами, ложный объект вычислительной сети может применять различные методы воздействия на перехваченную информацию, например:

1. селекция потока информации и сохранение ее на ложном объекте (нарушение конфиденциальности);
2. модификация информации:
    - • модификация данных (нарушение целостности);
    - • модификация исполняемого кода и внедрение разрушающих программных средств – программных вирусов (нарушение доступности, целостности);
3. подмена информации (нарушение целостности).

Одной из основных задач, возлагаемых на сетевую операционную систему, функционирующую на каждом из объектов распределенной вычислительной сети, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту. В общем случае в сети каждый субъект системы должен иметь возможность подключиться к любому объекту сети и получить в соответствии со своими правами удаленный доступ к его ресурсам. Обычно в вычислительных сетях возможность предоставления удаленного доступа реализуется следующим образом: на объекте в сетевой операционной системе запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т. п.), предоставляющих удаленный доступ к ресурсам данного объекта. Данные программы-серверы входят в состав телекоммуникационных служб предоставления удаленного доступа. Задача сервера состоит в том, чтобы постоянно ожидать получения запроса на подключение от удаленного объекта

и, получив такой запрос, передать на запросивший объект ответ на разрешение подключения либо на отказ. По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты сети. В этом случае непосредственно операционная система обрабатывает приходящие извне запросы на создание виртуального канала и передает их в соответствии с идентификатором запроса (номер порта) прикладному процессу, которым является соответствующий сервер. В зависимости от различных параметров объектов вычислительной сети, основными из которых являются быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи, количество одновременно устанавливаемых виртуальных подключений ограничено, соответственно ограничено и число запросов, обрабатываемых в единицу времени. С этой особенностью работы вычислительных сетей связана типовая удаленная атака "отказ в обслуживании".

Результат применения этой удаленной атаки – нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов вычислительной сети – отказ в обслуживании. Одна из разновидностей этой типовой удаленной атаки заключается в передаче с одного адреса такого количества запросов на атакуемый объект, которое позволяет трафик. В этом случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная остановка компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов. И последней, третьей разновидностью атаки "отказ в обслуживании", является передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы. Основными причинами успеха удаленных угроз в вычислительных сетях являются:

1. Отсутствие выделенного канала связи между объектами сети.
2. Недостаточная идентификация объектов и субъектов сети.
3. Взаимодействие объектов без установления виртуального канала.
4. Отсутствие в распределенных вычислительных сетях полной информации о ее объектах.
5. Отсутствие в распределенных вычислительных сетях криптозащиты сообщений.

Тема 3. Виды "нарушителей", вирусов. Угрозы

3.1. Классификация угроз

Угроза – потенциальная возможность определенным способом нарушить информационную безопасность. Попытка реализации угрозы называется атакой. Предпринимающий атаку называется злоумышленником.

Угрозы можно классифицировать по нескольким критериям:

По целям угрозы

- нарушение конфиденциальности;
- нарушение целостности;
- нарушение работоспособности.

По принципам воздействия

- с использованием доступа субъекта (пользователя) к объекту (файлу, каналу);
- с использованием скрытых каналов.

По характеру воздействия

- активное воздействие (нарушение правил);
- пассивное воздействие (наблюдение и ана.лиз)

По используемым средствам

- стандартное программное обеспечение(ПО);
- специальное ПО.

По способу воздействия на сеть

- в интерактивном режиме;
- в пакетном режиме.

По состоянию объекта атаки

- угроза хранения (на диске, ленте);
- угроза передачи по линии связи;
- угроза обработки (когда объектом атаки является процесс пользователя).

По способу воздействия

- непосредственное воздействие на объект;
- воздействие на систему разрешений;
- опосредованное воздействие.

По используемой ошибке

- недостаточная политика безопасности;
- ошибки администратора;
- ошибки в алгоритмах;
- ошибки в программах.

По объекту атаки

- автоматические системы обработки информации в целом;
- процессы пользователей;
- компоненты АСОИ;
- пакеты данных и каналы связи.

Знание наиболее уязвимых мест в системе, уже более чем на 50% спасает от угроз.

Наиболее уязвимые места:

Клиентские ПК и их ПО

- Искажение программ и данных в оперативной памяти;
- Искажение (разрушение)файлов и системных областей;
- Уменьшение скорости работы, неадекватная реакция на команды оператора;
- Вмешательство в процесс обмена сообщениями по сети путем непрерывной посылки хаотических сообщений;
- Блокирование принимаемых или передаваемых сообщений, их искажение;
- Имитация физических сбоев типа "потеря линии";
- Внедрения вирусов;
- Имитация пользовательского интерфейса или приглашений ввода пароля (ключа) с целью запоминания паролей.

Серверы локальной сети

- Искажения проходящей через сервер информации (при обмене между клиентскими ПК);
- Сохранение проходящей информации в скрытых областях внешней памяти;
- Искажение (уничтожение) собственности;
- Внедрение вирусов.

Коммутационные машины

- Вывод из строя коммутационного узла вместе со всеми абонентскими пунктами;
- Засылка пакетов не по адресу;
- Потеря пакетов, неверная сборка пакетов, их подмена;
- Внедрение вирусов в пакеты.

3.2. Угрозы информационной безопасности

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например, неконтролируемый доступ к персональным компьютерам или нелицензионное программное обеспечение.

Угрозы информационной безопасности классифицируются по нескольким признакам:

- по составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых в первую очередь направлены угрозы;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- по характеру воздействия (случайные или преднамеренные, действия природного или техногенного характера);
- по расположению источника угроз (внутри или вне рассматриваемой информационной системы).

Рассмотрим угрозы по характеру воздействия. Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы.

Причинами случайных воздействий при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия злоумышленника.

В качестве злоумышленника может выступить служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами, например: недовольством служащего служебным положением; любопытством; конкурентной борьбой; уязвленным самолюбием и т. д.

Угрозы, классифицируемые по расположению источника угроз, бывают внутренние и внешние. Внешние угрозы обусловлены применением вычислительных сетей и созданием на их основе информационных систем.

Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена.

Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

3.2.1. Каналы несанкционированного доступа к информации

Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющих нанести ущерб любой из составляющих информационной безопасности, является несанкционированный доступ. Несанкционированный доступ возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки.

Каналы НСД классифицируются по компонентам автоматизированных информационных систем.

1. Через человека:
    - хищение носителей информации;
    - чтение информации с экрана или клавиатуры;
    - чтение информации из распечатки.
2. Через программу:
    - перехват паролей;
    - расшифровка зашифрованной информации;
    - копирование информации с носителя.
3. Через аппаратуру:
    - подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
    - перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т. д.

3.2.2. Наиболее распространенные угрозы нарушения доступности информации

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (обычные ошибки администрирования).

Самый эффективный способ борьбы с непреднамеренными случайными ошибками – максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам автоматизированной информационной системы, на которые нацелены угрозы:

- отказ пользователей;

- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т. п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т. п.).

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т. п.);
- ошибки при конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рассматриваются следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо – и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности.

Опасными являются и стихийные бедствия – пожары, наводнения, землетрясения, ураганы. По статистике на долю этих источников угроз с учетом перебоев электропитания приходится 13% потерь, нанесенных информационным системам.

Угрозы доступности могут выглядеть грубо – как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего – грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов.

Одним из способов нарушения доступности является загрузка информационной системы (загрузка полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника такие угрозы подразделяется на внутренние и внешние. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Известны случаи вывода из строя сервисов глобальной сети Интернет, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Одним из опаснейших способов нарушения доступности и в целом информационной безопасности является внедрение в атакуемые системы вредоносного программного обеспечения.

Целями такого программного обеспечения является:

- внедрение другого вредоносного программного обеспечения;
- получение контроля над атакуемой системой;
- агрессивное потребление ресурсов;
- изменение или разрушение программ и/или данных.

К сожалению, количество "вредного" программного обеспечения постоянно увеличивается. Вирусы и троянские программы считают уже на десятки тысяч, а базы данных антивирусных программ обновляются практически ежедневно, несмотря на постоянно внедряемые методы "универсального" детектирования (то есть детектирования не конкретных вариантов отдельно взятого вируса, а всего "семейства" или даже целого класса вредоносных программ).

Причины роста данного вида угроз связаны с тем, что к компьютерам получают доступ все большее и большее количество кибер-хулиганов (по мере расширения глобальных информационных сетей). Какое-то число из них начинает самоутверждаться описанным выше способом.

Подробный анализ данного класса угроз рассмотрим в следующих темах.

3.2.3. Основные угрозы нарушения целостности информации

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз.

С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные, например, время создания или получения документа.

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. С этой угрозой связано понятие "аутентичность", то есть возможность подтверждения (доказательства) авторства того или иного документа или действия.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного программного обеспечения – пример подобного нарушения.

Угрозами динамической целостности являются дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т. п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

3.2.4. Основные угрозы нарушения конфиденциальности информации

Конфиденциальную информацию условно можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить не компьютерный и вообще не технический характер, например, при работе с несколькими информационными системами возникает необходимость запоминания нескольких паролей. В таких случаях чаще всего пользуются записными книжками, листками, которые зачастую находятся рядом с компьютером и т. д. Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т. п.), но идея одна – осуществить доступ к данным в тот момент, когда они наименее защищены.

Перехват данных – очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам,

их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например, на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных.

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т. д. Другой пример – нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

3.3. Компьютерные вирусы как особый класс разрушающих программных воздействий

Понятие вирусов было сформулировано в 1904 г. американским исследователем Ф.Коэном. Принято под вирусом понимать программный код, обладающий следующими свойствами:

1. Способность к созданию собственных копий, необязательно совпадающих с оригиналом, но обладающих свойствами оригинала.
2. Наличие механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

- среде обитания;
- способу заражения среды обитания;
- воздействию;
- особенностям алгоритма.

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

Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные.

1. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.
2. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

1. неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;
2. опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;
3. очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

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

Классификация вирусов по типам объектов вычислительной системы, в которых внедряются:

1. Программные файлы операционной системы – это файловые вирусы.

2. Системные области компьютеров, в частности области начальной загрузки операционной системы. Соответствующие вирусы получили название загрузочных или бутовых.
3. Макропрограммы и файлы документов современных систем обработки информации. такие вирусы называются макровирусами.

Жизненный цикл вирусов

Стадии:

1. Хранение – соответствует периоду, когда вирус хранится на диске совместно с объектом, в который он внедрен. На этой стадии вирус является наиболее уязвимым для антивирусных программ, т.к. он не может контролировать работу операционной системы с целью самозащиты. Наиболее распространенным способом защиты является шифрование большей части тела вируса. Его использование совместно с механизмами мутации кода делает невозможным выделение устойчивых характеристических фрагментов сигнатур. Это в свою очередь приводит к недееспособности антивирусных средств, основанных на методах поиска заранее выделенных сигнатур.
2. Исполнение состоит из 5 этапов:
    - а) загрузка вируса в память;
    - б) поиск жертвы;
    - в) заражение найденной жертвы;
    - г) выполнение деструктивных функций;
    - д) передача управления программе-носителю вируса.

Загрузка вируса в память

Загрузка вируса в память осуществляется операционной системой одновременно с загрузкой исполняемого объекта, в который вирус внедрен. В простейшем случае, процесс загрузки вируса представляет собой копирование с диска в оперативную память сопровождаемой настройкой адресов, после чего управление передается коду тела вируса. Эти действия выполняются операционной системой, а сам вирус находится в пассивном состоянии. В сложном случае, после получения управления вирус может выполнить ряд действий:

- использовать для защиты методы криптографической защиты. В этом случае дополнительные действия, которые вирус выполняет на этапе загрузки, состоят в расшифровании основанного тела вируса.
- объект и вирус располагаются в едином адресном пространстве. После завершения работы объекта, объект выгружается из оперативной памяти и при этом выгружается вирус, переходя в пассивную стадию хранения. Однако некоторые типы вирусов способны сохраняться в памяти и

оставаться активными после окончания работы вируса носителя. Такие вирусы называются резидентными.

Для закрепления в оперативной памяти вирусы переносят свой код либо в самостоятельно отведенные блоки памяти, либо в зарезервированные под нужды операционной системы участки памяти. Также вирус заботится, чтобы этой области передавалось оперативное управление. Вирусы изменяют код системных функций, которыми гарантированно используются прикладными программами. Добавляет в них команды передачи управления своему коду. Изменяют системные таблицы, адреса соответствующих системных функций, подставив адреса своих подпрограмм, т.е. свойство резидентности предполагает выполнение вирусом на этапе загрузки двух действий:

- закрепление в памяти;
- перехват системных функций.

Stells-вирусы, для которых характерным является перехват системных функций с целью контроля действий операционной системы. Они скрывают свое присутствие и избегают обнаружение антивирусными программами.

Поиск жертвы

По способу поиска жертвы вирусы можно разделить на два класса:

- осуществляющие активный поиск с использованием функций операционной системы. Например: файловые вирусы, использующие механизм поиска используемых файлов в текущем каталоге.
- реализующие пассивный механизм поиска. Это вирусы, расставляющие "ловушки" для программных файлов. Например: файловые вирусы устраивают "ловушки" для перехвата функции exe операционной системы. А макровирусы с помощью перехвата команд типа save as из меню файла.

Заражение найденной жертвы

Заражение найденной жертвы в простейшем случае заражение представляет собой самокопирование кода вируса выбранной в качестве жертвы объект. По способу инфицирования жертвы вирусы можно разделить на классы:

1. Вирусы, которые не внедряют свой код непосредственно в программный файл, а изменяют имя файла и создают код старым именем новый, содержащий тело вируса.
2. Вирусы, внедряющиеся непосредственно в файлы жертвы. Они характеризуются местом внедрения в файл:
    - а) в начало файла. При внедрении производится объединение собственного кода программы. Либо переписывается начальный фрагмент файлов в конец, освобождая место для себя.

- б) внедрение в конец файла. Передача управления вирусу обеспечивается модификацией первых команд программы (com) либо заголовков программы (exe)
- в) внедрение в середину файла. Используется для файлов с заранее известной структурой, либо к файлам, содержащим последовательность байтов.

3.3.1. Классификация компьютерных вирусов

Классификация компьютерных вирусов по среде обитания

По среде "обитания" вирусы делятся на:

1. Файловые вирусы внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон – вирусы), либо используют особенности организации файловой системы (link-вирусы).
2. Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record), либо меняют указатель на активный boot-сектор.
3. Макровирусы заражают файлы – документы и электронные таблицы популярных офисных приложений.
4. 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, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс- и полиморфик-технологии. Другой 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 опрерационных систем. Макровирусы заражают файлы форматов Word, Excel, пакета Office. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Классификация компьютерных вирусов по особенностям алгоритма работы

По особенностям алгоритма работы вирусы делятся на:

- резидентные;
- стелс-вирусы;

- полиморфик-вирусы;
- вирусы, использующие нестандартные приемы.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. К резидентным относятся макровирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы 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 операционной системы на чтение/запись зараженных объектов. Стелс-вирусы при этом 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 детектирования (обнаружения) вируса. Полиморфик-вирусы (polymorphic) – это достаточно труднообнаруживаемые вирусы, не имеющие сигнатур, то есть не содержащие 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 и модификациями программы-расшифровщика.

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

Классификация компьютерных вирусов по деструктивным возможностям

По деструктивным возможностям вирусы можно разделить на:

- безвредные, то есть никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске;

- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и далее повредить аппаратные средства компьютера.

3.2.2. Характеристика "вирусоподобных" программ

К "вредным программам", помимо вирусов, относятся:

- "троянские программы" (логические бомбы);
- утилиты скрытого администрирования удаленных компьютеров;
- "intended"-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

"Троянские" программы (логические бомбы)

К "троянским" программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий. Например, уничтожение информации на дисках при каждом запуске или по определенному графику и т. д. Большинство известных "троянских" программ являются программами, которые маскируются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по электронным конференциям. По сравнению с вирусами "троянские" программы не получают широкого распространения по достаточно простым причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем. К "троянским" программам также относятся так называемые "дропперы" вирусов – зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют присутствие вируса в файле. Например, файл шифруется или упаковывается неизвестным архиватором, что не позволяет антивирусу "увидеть" заражение.

Отметим еще один тип программ (программы – "злые шутки"), которые используются для устрашения пользователя, свидетельствуя о заражении вирусом или о каких-либо предстоящих действиях с этим связанных, то есть сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям. Например, к "злым шуткам" относятся программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т. д. К категории "злых шуток" можно отнести также заведомо ложные сообщения о

новых "супер-вирусах". Такие сообщения периодически появляются в сети Интернет и обычно вызывают панику среди пользователей.

Утилиты скрытого администрирования

Утилиты скрытого администрирования являются разновидностью "логических бомб" ("троянских программ"), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Единственная особенность этих программ заставляет классифицировать их как вредные "троянские" программы: отсутствие предупреждения об инсталляции и запуске. При запуске такая программа устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях программы в системе. Чаще всего ссылка на такую программу отсутствует в списке активных приложений. В результате пользователь может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т.д. в результате эти программы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т.п.

"Intended"-вирусы

К таким вирусам относятся программы, которые, на первый взгляд, являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении не помещает в начало файла команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (в большинстве приводит к "зависанию" компьютера) и т. д. К категории "intended" 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. Появляются "intended"-вирусы чаще всего из-за неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

Конструкторы вирусов

К данному виду "вредных" программ относятся утилиты, предназначенные для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно 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.

Полиморфные генераторы

Полиморфик-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. Обычно полиморфные генераторы распространяются в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор.

3.3.3. Механизмы заражения вирусами компьютерной системы

Механизмы заражения загрузочными вирусами

Рассмотрим схему функционирования очень простого загрузочного вируса, заражающего CD, DVD диски, флешки. Что происходит, когда вы включаете компьютер? Первым делом управление передается программе начальной загрузки, которая хранится в постоянно запоминающем устройстве (ПЗУ) т.е. ПНЗ ПЗУ.

Эта программа тестирует оборудование и при успешном завершении проверок пытается найти CD, DVD диск или флешку на внешнем запоминающем устройстве.

Всякая дискета или диск размечен на т.н. секторы и дорожки. Секторы объединяются в кластеры.

Среди секторов есть несколько служебных, используемых операционной системой для собственных нужд (в этих секторах не могут размещаться ваши данные). Среди служебных секторов нас пока интересует один – т.н. сектор начальной загрузки (boot-sector).

В секторе начальной загрузки хранится информация о дискете или диске – количество поверхностей, количество дорожек, количество секторов и пр. Но нас сейчас интересует не эта информация, а небольшая программа начальной загрузки (ПНЗ), которая должна загрузить саму операционную систему и передать ей управление.

Таким образом, нормальная схема начальной загрузки следующая:
ПНЗ (ПЗУ) – ПНЗ (диск) – СИСТЕМА
Теперь рассмотрим вирус. В загрузочных вирусах выделяют две части – т.н. голову и т.н. хвост. Хвост, вообще говоря, может быть пустым.
Пусть у вас имеются чистая дискета или диск и зараженный компьютер, под которым мы понимаем компьютер с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисководе появилась подходящая жертва – в нашем случае не защищенная от записи и еще не зараженная дискета или диск, он приступает к заражению. Заражая дискету (диск), вирус производит следующие действия:

- выделяет некоторую область диска и помечает ее как недоступную операционной системе, это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные (bad);
- копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор;
- замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой;
- организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке
ПНЗ (ПЗУ) – ПНЗ (диск) – СИСТЕМА
появляется новое звено:
ПНЗ (ПЗУ) – ВИРУС – ПНЗ (диск) – СИСТЕМА
Мы рассмотрели схему функционирования простого бутового вируса, живущего в загрузочных секторах дискет, CD, DVD дисков или флешки. Как правило, вирусы способны заражать не только загрузочные секторы дискет (дисков), но и загрузочные секторы винчестеров. При этом в отличие от дискет, CD, DVD дисков и флешек на винчестере имеются два типа загрузочных секторов, содержащих программы начальной загрузки, которые получают управление. При загрузке компьютера с винчестера первой берет на себя управление программа начальной загрузки в MBR (Master Boot Record – главная загрузочная запись). Если ваш жесткий диск разбит на несколько разделов, то лишь один из них помечен как загрузочный (boot). Программа начальной загрузки в MBR находит загрузочный раздел винчестера и передает управление на программу начальной загрузки этого раздела. Код последней совпадает с кодом программы начальной загрузки, содержащейся на обычных дискетах, а соответствующие загрузочные секторы отличаются только таблицами

параметров. Таким образом, на винчестере имеются два объекта атаки загрузочных вирусов – программа начальной загрузки в MBR и программа начальной загрузки в бут-секторе загрузочного диска.

Механизмы заражения файловыми вирусами

Рассмотрим теперь схему работы простого файлового вируса. В отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы совсем не обязательно резидентны. Рассмотрим схему функционирования нерезидентного файлового вируса. Пусть у нас имеется инфицированный исполняемый файл. При запуске такого файла вирус получает управление, производит некоторые действия и передает управление "хозяину".

Какие же действия выполняет вирус? Он ищет новый объект для заражения – подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. Кроме своей основной функции – размножения, вирус вполне может сделать что-нибудь замысловатое (сказать, спросить, сыграть) – это уже зависит от фантазии автора вируса. Если файловый вирус резидентный,, то он установится в память и получит возможность заражать файлы и проявлять прочие способности не только во время работы зараженного файла. Заражая исполняемый файл, вирус всегда изменяет его код – следовательно, заражение исполняемого файла всегда можно обнаружить. Но, изменяя код файла, вирус не обязательно вносит другие изменения:

- он не обязан менять длину файла;
- неиспользуемые участки кода;
- не обязан менять начало файла.

Наконец, к файловым вирусам часто относят вирусы, которые "имеют некоторое отношение к файлам", но не обязаны внедряться в их код. Рассмотрим модель, на которой ясно видна основная идея вируса. Информация о файлах хранится в каталогах. Каждая запись каталога включает в себя имя файла, дату и время создания, некоторую дополнительную информацию, номер первого кластера файла и т.н. резервные байты.

При запуске исполняемых файлов система считывает из записи в каталоге первый кластер файла и далее все остальные кластеры. Вирусы производят следующую "реорганизацию" файловой системы: сам вирус записывается в некоторые свободные секторы диска, которые он помечает как сбойные. Кроме того, он сохраняет информацию о первых кластерах исполняемых файлов в резервных битах, а на место этой информации записывает ссылки на себя.

Таким образом, при запуске любого файла вирус получает управление (операционная система запускает его сама), резидентно устанавливается в память и передает управление вызванному файлу.

Механизмы заражения загрузочно-файловыми вирусами

Обсудим крайне "популярный" в последнее время загрузочно-файловый вирус OneHalf, заражающий главный загрузочный сектор (MBR) и исполняемые файлы. Основное разрушительное действие – шифрование секторов винчестера. При каждом запуске вирус шифрует очередную порцию секторов, а зашифровав половину жесткого диска, радостно сообщает об этом. Основная проблема при лечении данного вируса состоит в том, что недостаточно просто удалить вирус из MBR и файлов, надо расшифровать зашифрованную им информацию. Наиболее "смертельное" действие – просто переписать новый здоровый MBR.

Полиморфные вирусы

Большинство вопросов связано с термином "полиморфный вирус". Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным. Объясним же, что это такое.

Полиморфные вирусы – вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Полиморфные вирусы – это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку "по ходу дела", может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

3.3.4. Антивирусные программы

Одним из наиболее эффективных способов борьбы с вирусами является использование антивирусного программного обеспечения.

Антивирусная программа – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Вместе с тем, необходимо признать, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, поскольку на любой

алгоритм антивируса всегда можно предложить новый алгоритм вируса, невидимого для этого антивируса.

При работе с антивирусными программами необходимо знать некоторые понятия:

- "Ложное срабатывание" – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).
- "Пропуск вируса" – недетектирование вируса в зараженном объекте.
- "Сканирование по запросу" – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.
- "Сканирование на лету" – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т. п.). В этом режиме антивирус постоянно активен, он присутствует в памяти "резидентно" и проверяет объекты без запроса пользователя.

Классификация антивирусных программ

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры (программы-детекторы), CRC-сканеры (ревизоры). Существуют также антивирусы блокировщики и иммунизаторы.

Сканеры

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые "маски". Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов.

Во многих сканерах используются также алгоритмы "эвристического сканирования", т. е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Сканеры также можно разделить на две категории – "универсальные" и "специализированные". Универсальные сканеры рассчитаны на поиск и

обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов.

Сканеры также делятся на "резидентные" (мониторы), производящие сканирование "на лету", и "нерезидентные", обеспечивающие проверку системы только по запросу. Как правило, "резидентные" сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как "нерезидентный" сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам – размеры антивирусных баз, которые сканерам приходится хранить и пополнять, и относительно небольшая скорость поиска вирусов.

CRC-сканеры

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 "анти-стелс" алгоритмы, реагируют практически на 100 % вирусов сразу после появления изменений на компьютере. Характерный недостаток этих антивирусов заключается в невозможности обнаружения вируса с момента его появления и до тех пор, пока не будут произведены изменения на компьютере. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в восстанавливаемых файлах или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах.

Программы-детекторы

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры 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 таких программ.

Блокировщики

Антивирусные блокировщики – это резидентные программы, перехватывающие "вирусоопасные" ситуации и сообщающие об этом пользователю.

К "вирусоопасным" относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочный сектор диска и др., которые характерны для вирусов в моменты их размножения.

К достоинствам блокировщиков 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 активизируется.

Иммунизаторы

Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

Программы-доктора

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 известные из них: Aidstest, Scan, Norton AntiVirus, Doctor Web.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление версий.

Программы-ревизоры

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf.

Программы-фильтры

Программы-фильтры или "сторожа" представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM, EXE;
- изменение атрибутов файла;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако, они не "лечат" файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их "назойливость"(например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением. Примером программы-фильтра является программа Vsafe, входящая в состав пакета утилит MS Windows.

Вакцины или **иммунизаторы** – это резидентные программы, предотвращающие заражение файлов.

Вакцины применяют, если отсутствуют программы-доктора, "лечащие" этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

Факторы, определяющие качество антивирусных программ

Качество антивирусной программы определяется несколькими факторами, перечислим их по степени важности:

- Надежность и удобство работы – отсутствие "зависаний" антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
- Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц, упакованных и

архивированных файлов. Отсутствие "ложных срабатываний". Возможность лечения зараженных объектов.

- Существование версий антивируса под все популярные платформы (DOS, Windows, Linux и т. д.).
- Возможность сканирования "на лету".
- Существование серверных версий с возможностью и администрирования сети.
- Скорость работы.

3.3.5. Профилактика компьютерных вирусов

Одним из методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение правил ("компьютерной гигиены"), позволяющих значительно снизить вероятность заражения вирусом и потери каких-либо данных. Профилактика компьютерных вирусов начинается с выявления путей проникновения вируса в компьютер и компьютерные сети.

Характеристика путей проникновения вирусов в компьютеры

Рассмотрим основные пути проникновения вирусов в компьютеры пользователей:

1. Глобальные сети – электронная почта.
2. Электронные конференции, файл-серверы ftp.
3. Пиратское программное обеспечение.
4. Локальные сети.
5. Персональные компьютеры "общего пользования".
6. Сервисные службы.

Глобальные сети – электронная почта

Основным источником вирусов на сегодняшний день является глобальная сеть Интернет. Наибольшее число заражений вирусом происходит при обмене электронными письмами через почтовые серверы E-mail. Пользователь получает электронное письмо с вирусом, который активизируется (причем, как правило, незаметно для пользователя) после просмотра файла-вложения электронного письма. После этого вирус (стелс) выполняет свои функции. В первую очередь, вирус "заботится" о своем размножении, для этого формируются электронные письма от имени пользователя по всем адресам адресной книги. Далее идет цепная реакция.

Локальные сети

Другой путь "быстрого заражения" – локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или нескольких служебных файлов на сервере. Далее пользователи при очередном подключении к сети запускают зараженные файлы

с сервера, и вирус таким образом получает доступ на компьютеры пользователей.

Персональные компьютеры "общего пользования"

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из студентов принес на своих дискетах вирус и заразил какой-либо учебный компьютер, то очередной вирус будет гулять по всему учебному заведению, включая домашние компьютеры студентов и сотрудников.

Пиратское программное обеспечение

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных "зон риска". Часто пиратские копии содержат файлы, зараженные самыми разнообразными типами вирусов. Необходимо помнить, что низкая стоимость программы может дорого обойтись при потере данных.

Сервисные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре в сервисных центрах.

Правила защиты от компьютерных вирусов

Учитывая возможные пути проникновения вирусов, приведем основные правила защиты от вирусов.

1. Внимательно относитесь к программам и документам, которые получаете из глобальных сетей. Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте его на наличие вирусов.
2. Используйте специализированные антивирусы для проверки "на лету" (например, SpIDer Guard из пакета Dr. Web и др.) всех файлов, приходящих по электронной почте (и из Интернета в целом).
3. Для уменьшения риска "заразить" файл на сервере администраторам сетей следует активно использовать стандартные возможности защиты сети, такие как: ограничение прав пользователей; установку атрибутов "только на чтение" или "только на запуск" для всех выполняемых файлов (к сожалению, это не всегда оказывается возможным) и т. д.
4. Регулярно проверяйте сервер обычными антивирусными программами, для удобства и системности используйте планировщики заданий.
5. Целесообразно запустить новое программное обеспечение на тестовом компьютере, не подключенном к общей сети.
6. Используйте лицензионное программное обеспечение, приобретенное у официальных продавцов.
7. Дистрибутивы копий программного обеспечения (в том числе копий операционной системы) необходимо хранить на защищенных от записи дисках.

8. Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов.
9. Постоянно обновляйте вирусные базы используемого антивируса.
10. Старайтесь не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.
11. Ограничьте (по возможности) круг лиц, допущенных к работе на конкретном компьютере.
12. Пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т. д.).
13. Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа.
14. При работе с Word/Excel включите защиту от макросов, которая сообщает о присутствии макроса в открываемом документе и предоставляет возможность запретить этот макрос. В результате макрос не только не выполняется, но и не виден средствами Word/Excel.

Обнаружение макровируса

Характерными проявлениями макровирусов являются:

- Word: невозможность конвертирования зараженного документа Word в другой формат;
- Word: зараженные файлы имеют формат Template (шаблон), поскольку при заражении Word-вирусы конвертируют файлы из формата Word Document в Template;
- Excel/Word: в STARTUP (Автозагрузка)-каталоге присутствуют "посторонние" файлы;
- Excel: наличие в Книге (Book) лишних и скрытых Листов (Sheets).

Для проверки системы на предмет наличия вируса можно использовать пункт меню Сервис/макрос. Если обнаружены "чужие макросы", то они могут принадлежать вирусу. Однако этот метод не работает в случае стелс-вирусов, которые запрещают работу этого пункта меню, что, в свою очередь, является достаточным основанием считать систему зараженной.

Многие вирусы имеют ошибки или некорректно работают в различных версиях Word/Excel, в результате чего Word/Excel выдают сообщения об ошибке.

Если такое сообщение появляется при редактировании нового документа или таблицы и при этом заведомо не используются какие-либо пользовательские макросы, то это также может служить признаком заражения системы.

Сигналом о вирусе являются и изменения в файлах и системной конфигурации Word, Excel и Windows. Многие вирусы тем или иным образом меняют пункты меню, разрешают или запрещают некоторые функции, устанавливают на файлы пароль при их заражении. Большое количество вирусов создает новые секции и/ или опции в файле конфигурации Windows (WIN. INI).
Естественно, что к проявлениям вируса относятся такие очевидные факты, как появление сообщений или диалогов с достаточно странным содержанием или на языке, не совпадающем с языком установленной версии Word/Excel.

Тема 4. Виды возможных нарушений информационной системы. Виды защиты. Типовая операция враждебного воздействия

4.1. Типовая операция враждебного воздействия

Типовая операция враждебного воздействия содержит следующие этапы:

1. Подготовительный этап.
2. Несанкционированный доступ.
3. Основной этап (разведывательный, диверсионный).
4. Скрытая передача информации.
5. Сокрытие следов воздействия.

Опишем методы и противодействия для каждого из этапов:

I. Подготовительный этап

Методы:

- асинхронная атака.
  Используя асинхронную природу ОС компьютерную систему заставляют работать в сложных условиях, из-за чего работа нарушается. Данная ситуация используется для внесения изменений в ОС, при чем эти изменения не будут заметны.
  Противодействия: точное выполнение требование принятой политики безопасности
- моделирование.
  Строится модель поведения компьютерной системы в различных условиях и на основе изучения организации работы оптимизируется способ манипулирования данными с целью их хищения.
  Противодействия: точное выполнение требование принятой политики безопасности.

II. Несанкционированный доступ

Методы:

- "за дураком" – электронное проникновение в средства вычислительной техники (т.е. подключается дополнительный компьютерный терминал к каналам связи в момент кратковременного выхода законного пользователя)
  Противодействия: Покидая рабочее место, не оставлять свой терминал в активном режиме.
- Физическое проникновение в производственное помещение
  Противодействие: использовать эффективные электронные средства контроля и управления доступом.
- "за хвост" – подключение к линиям связи и перехват работы после окончания сеанса законного пользователя
  Противодействие: обеспечить эффективный контроль доступа к данной линии связи (физическая защита)
- компьютерный абордаж (взлом системы) – подбор кода к системе вручную или с использованием специальной программы
  Противодействие: ограничение количества попыток неправильного ввода пароля с последующей блокировкой терминала и уведомление администратора
- "неспешный выбор" – изучается система защиты от НСД, выявляются участки, имеющие ошибки или разрывы программ, вводятся дополнительные программы, разрешающие доступ.
  Противодействие: постоянный контроль, жесткое администрирование.
- "маскарад" – проникновение в компьютерную систему, выдавая себя за пользователя, с применением его кодов (паролей) и др. шифров.
  Противодействие: использовать надежные средства идентификации, блокирование попыток взлома системы, фиксировать все события в журнале для последующего анализа.
- "мистификация" – создание условий, когда законный пользователь осуществляет связь с нелегальным терминалом, будучи уверенным в том, что он работает с необходимым ему абонентом.
- "аварийный" – создание условий для возникновения сбоев с возможностью отключения средств защиты информации.

III. Основной этап (разведывательный, диверсионный)

- Атаки "Салями" – использование погрешности вычислений, позволяющих трактовать правила округления в ту или иную сторону.
  Противодействие: Обеспечение целостности и корректности прикладных программ, обрабатывающих информацию.

- "Сборка мусора" – после окончания работы, обрабатываемая информация не всегда полностью удаляется, часть данных, оставшаяся на дисках, лентах, в оперативной памяти собирается и обрабатывается. Противодействие: Забить освобождающуюся память 0 или 1, или перезапись на это место другой информации.
- "Люки". Недокументированная точка входа в программный модуль используется для активного воздействия.
  Противодействие: при приемке программных продуктов анализировать исходный текст программ с целью обнаружения люка.
- "Троянский конь" – программа, выполняющая дополнительные, не описанные в документации действия.
  Радикальным способом защиты является замкнутость среды исполнения программы.
- "Вирус" – программа, заражающая другие программы, путем включения в них своей модифицированной копии, при чем последняя имеет способность к дальнейшему распространению. Вирусы распространяются локально, в пределах узла сети, для передачи по сети им требуется внешняя помощь (например, пересылка зараженного файла).
  Противодействия: антивирусное ПО, специальное ПО.
- "Червь" – программа, способная самостоятельно, т.е. без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение. Для активации вируса требуется запуск зараженной программы, а для червя – нет. Черви ориентированы на путешествие по сети.
- "Жадные программы" – программы, которые при выполнении стремятся монополизировать какие-либо ресурсы системы, не давая другим программам их использовать.
  Противодействия: введение ограничений на использование времени процессора, на количество операций ввода-вывода, на объем оперативной памяти.
- "Захватчики паролей" – программы специально предназначенные для перехвата паролей
- Программные закладки. Существуют следующие методы воздействие программных закладок на компьютеры:
- "Перехват"
- Программная закладка (ПЗ) записывается в ПЗУ, в системное или прикладное обеспечение и сохраняет вводимую, выводимую информацию в скрытую область памяти локального или удаленного компьютера.
  Противодействие: разработка специального ПО для защиты от ПЗ.

- "Искажение".
  ПЗ изменяет информацию, которая записывается в память компьютерной системы или инициирует возникновение ошибочной ситуации в компьютерной системе.
- "Наблюдатель".
  ПЗ встраивается в сетевое или телекоммуникационное ПО. Внедренная ПЗ может следить за всеми процессами обработки информации, а также осуществлять установку и удаление др. ПЗ.
- "Компрометация" – после получения доступа к перехваченной информации, изменение её содержания.

IV. Скрытая передача информации

Скрытые каналы – скрытая передача информации межу процессами системы, нарушающие политику безопасности.

Противодействие: поиск и блокировка скрытых каналов.

V. Сокрытие следов воздействия

"Бухинг" – электронное блокирование.

Компьютерная система блокируется одновременной атакой НСД большим количеством пользователей со своих ПК из различных регионов. Они организуют прикрытие одной незаконной операции.

Таким образом, информационные воздействия делятся на конструктивные и деструктивные.

При конструктивном – главой целью является получение копии конфиденциальной информации (разведывательное программное воздействие).

При деструктивном – конечной целью является уничтожение, разрушение компьютерных ресурсов и информации (вирусы, черви и т.д.).

4.2. Программные закладки

Программная закладка – программа, которая способна выполнить ряд разрушающих операций.

Такие программы способны выполнить следующие воздействия:

1. Скрыть признаки своего присутствия в программной среде
2. Реализовать, самодублировать, ассоциирование себя с другими программами
3. Разрушить, исказить код программ, отличных от нее
4. Перенести (сохранить) фрагменты информации из оперативной памяти в некоторые области оперативной памяти или внешней памяти прямого доступа
5. Имеет потенциальную возможность исказить произвольным образом, заблокировать или подменить выводимые во внешнюю память массив информации.

Понятие разрушающего программного воздействия

Программную закладку практически невозможно обнаружить, т.к. их действие незаметно пользователю. Назначение программной закладки: всю информацию, которую нужно скачивать скачивает в определенную область памяти.

Механизм действия программных закладок : основан на обработке прерывания от различных устройств.

Прерывание – реакция системы на некоторое событие, при котором временно прекращается исполнение программы и используется процедура обработки прерывания, после чего управление передается в основную программу.

Основным перехватом информации при работе программной закладки является ввод с клавиатуры данных, либо со сканера, из файлов. Предмет прерывания – адрес, по которому находится обработчик прерывания. Русификатор берет код клавиши и преобразует его в код русского алфавита, далее управление передает системному обработчику клавиатуры. Системный обработчик клавиатуры кладет код нажатой клавиши в буфер данных, а прикладная программа уже берет данные из этого буфера. На одном векторе может находится несколько обработчиков событий. Программная закладка перестраивает вектор прерывания на собственный обработчик, а он будет вызывать всю оставшуюся цепочку. Обработчик дублирует данные в системный буфер данных и в оперативную память. В качестве буфера данных туда будут помещаться украденная информация, могут выступать файлы на внешнем запоминающем устройстве. Обработчик будет находится в оперативной памяти пока система не будет перезагружена. Программные закладки встраиваются не в игрушки, а в программы, которые запускаются после загрузки операционной системы.

Программные закладки можно классифицировать по методу и месту их внедрения и применения:

1. BIOS
2. Закладки в программы первичной загрузки
3. Закладки, внедренные в драйвера
4. Закладки, внедренные в программы общего назначения (клавиатурные и экранные драйвера, программы тестирования компьютеров и т.д.)
5. Закладки, внедренные в программы оптимизационного назначения
6. Закладки, внедренные в программные средства игрового и уникального назначения.

Закладки должны быть загружены в оперативную память раньше, чем цель ее воздействия. Выделяют закладки двух типов:

1. Закладки резидентного типа, т.е. находятся в памяти постоянно с некоторого момента времени до окончания сеанса работы.

2. Закладки не резидентного типа, т.е. начинает работу как закладки резидентного типа, но заканчивает ее самостоятельно через некоторый промежуток времени.

Модели закладок:

1. Модель "Перехват" встраивается из ПЗУ в операционную систему или прикладное программное обеспечение, и сохраняет информацию в скрытой области локальной или удаленной внешней памяти.
2. "Троянский конь". Закладка встраивается в постоянно используемое программное обеспечение и по некоторому событию начинает работать. Моделирует сбойную ситуацию. При этом достигаются две цели:
    - а) Парализовать работу системы
    - б) Ознакомится с информацией
3. "Наблюдатель" осуществляет контроль за процессами обработки информации, съём накопленной информации.
4. "Компрометация" или "Искажение" искажает потоки данных, возникающие при работе прикладных программ (выходные), либо искажает входные потоки при работе данных.
5. "Уборка мусора" изучает остатки информации. Навязывает такой порядок работы, чтобы максимизировать количество оставшихся фрагментов ценной информации.

Перехват файловых операций. Для этого файл открывается, его часть или весь файл считывается в буфер оперативной памяти, образуется прикладная программа, оптимизирующим событием является открытие файлов. Далее вызывается диспетчер программных запросов.

Методы внедрения программных закладок: маскировка под программное обеспечение (например, под текстовый редактор и т.д.), если подобная закладка внедряется в многопользовательскую или многопрограммную среду, ее возможности по оказанию негативных воздействий ограничены, т.к. подобных программных средах исполняется изолированно друг от друга.

Тема 5. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы

5.1. Обзор Российского законодательства в области информационной безопасности

В 1992 г. Гостехкомиссия (ГТК) при Президенте РФ опубликовала пять руководящих документов, посвященных вопросам защиты от несанкционированного доступа (НСД) к информации. Рассмотрим важнейшие из них:

1. "Концепция защиты средств вычислительной техники от НСД к информации".
2. "Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации".
3. "Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации".

Идейной основой этих документов является "Концепция защиты средств вычислительной техники от НСД к информации, содержащая систему взглядов ГТК на проблему информационной безопасности и основные принципы защиты компьютерных систем.

Основная, и едва ли не единственная, задача средств безопасности в этих документах – это обеспечение защиты от НСД к информации. Если средствам контроля и обеспечения целостности еще уделяется некоторое внимание, то поддержка работоспособности систем обработки информации вообще не упоминается. Все это объясняется тем, что эти документы были разработаны в расчете на применение в информационных системах Министерства обороны и спецслужб РФ, а также недостаточно высоким уровнем информационных технологий этих систем по сравнению с современным.

Руководящие документы ГТК предлагают две группы критериев безопасности:

- показатели защищенности средств вычислительной техники (СВТ) от НСД;
- критерии защищенности автоматизированных систем (АС) обработки данных.

Данные показатели содержат требования защищенности СВТ от НСД к информации и применяются к общесистемным программным средствам и

операционным системам. Конкретные перечни показателей определяют классы защищенности СВТ и описываются совокупностью требований.

Установлено семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

В отличие от остальных стандартов отсутствует раздел, содержащий требования по обеспечению работоспособности системы, зато присутствует раздел, посвященный криптографическим средствам.

Требования к средствам защиты АС от НСД включают следующие подсистемы:

- Подсистема управления доступом.
- Подсистема регистрации и учета.
- Криптографическая подсистема.
- Подсистема обеспечения целостности.

Документы ГТК устанавливают девять классов защищенности АС от НСД, каждый из которых характеризуется определенной совокупностью требований к средствам защиты. Классы подразделяются на три группы, отличающиеся спецификой обработки информации в АС. Группа АС определяется на основании следующих признаков:

1. Наличие в АС информации различного уровня конфиденциальности.
2. Уровень полномочий пользователей АС на доступ к конфиденциальной информации.
3. Режим обработки данных в АС (коллективный или индивидуальный).

Федеральные критерии безопасности информационных технологий

Федеральные критерии безопасности информационных технологий – первый стандарт информационной безопасности, в котором определяются три независимые группы требований: функциональные требования к средствам защиты, требования к технологии разработки и к процессу квалификационного анализа.

Авторами этого стандарта впервые предложена концепция Профиля защиты – документа, содержащего описание всех требований безопасности как к самому продукту информационных технологий (ИТ-продукту), так и к процессу его проектирования, разработки, тестирования и квалификационного анализа.

Функциональные требования безопасности хорошо структурированы и описывают все аспекты функционирования ТСВ.

Требования к технологии разработки, впервые появившиеся в этом документе, побуждают производителей использовать современные технологии программирования как основу для подтверждения безопасности своего продукта.

Разработчики федеральных критериев отказались от используемого в Оранжевой книге подхода к оценке уровня безопасности ИТ-продукта на

основании обобщенной универсальной шкалы классов безопасности. Вместо этого предлагается независимое ранжирование требований каждой группы, т. Е. вместо единой шкалы используется множество частных шкал критериев, характеризующих обеспечиваемый уровень безопасности. Данный подход позволяет разработчикам и пользователям ИТ-продукта выбрать наиболее приемлемое решение и точно определить необходимый и достаточный набор требований для каждого конкретного ИТ-продукта и среды его эксплуатации.

Этот стандарт рассматривает устранение недостатков существующих средств безопасности как одну из задач защиты наряду с противодействием угрозам безопасности и реализацией модели безопасности.

Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

Конституция РФ (12 декабря 1993 г.):

- Ст. 24. Органы государственной власти и местного самоуправления должны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими права и свободы.
- Ст. 41. Гарантирует право на знание фактов и обстоятельств, создающих угрозу здоровью и жизни людей.
- Ст. 42. Гарантирует право на знание достоверной информации о состоянии окружающей среды.
- Ст. 23. Гарантирует право на личную и семейную тайну, на тайну переписки, телефонных разговоров, почтовых, телеграфных и иных сообщений.
- Ст. 29. Право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Гражданский кодекс РФ (15 мая 2001 г.):

В нем фигурируют понятия: банковская, коммерческая и служебная тайна.

Согласно ст. 139, информация составляет служебную или коммерческую тайну, если она имеет коммерческую ценность, к ней нет свободного доступа и обладатель информации принимает меры к охране её конфиденциальности.

Уголовный кодекс РФ (ред. 14 марта 2002 г.):

- Гл. 28. "Преступление в сфере компьютерной информации".
- Ст. 272 "Неправомерный доступ к компьютерной информации". За данные преступления могут быть вынесены наказания в размере от 200 минимальных зарплат до лишения свободы на срок до 5 лет.
- Ст. 273 "Создание, использование и распространение вредоносных программ для ЭВМ". Наказание в виде штрафа в размере 2 заработных плат до лишения свободы на срок до 7 лет.

- Ст. 274 "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети". Наказание в виде лишения права занимать определенные должности на срок до 5 лет, либо обязательными работами на срок до 180-200 часов. При тяжких последствиях – лишение свободы на срок до 4 лет.
- Ст. 138 УК РФ защищает конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных разговоров и т.д.
- Ст. 183 Аналогична коммерческой и банковской тайне.

О государственной тайне

Закон "О государственной тайне" (6.10.1997). В нем гос. тайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной и операционно – розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. В нем дается определение средств защиты информации – технические, криптографические, программные и др.

Об информации, информационных технологиях и защите информации

Закон "Об информации, информационных технологиях и защите информации", №149-ФЗ (от 27 июля 2006) – даются основные определения и намечаются направления развития законодательства в данной области.

Закон выделяет следующие цели защиты информации:

1. Предотвращение утечки, хищения, утраты, подделки.
2. Предотвращение угроз безопасности личности, угроз государству.
3. Предотвращение несанкционированных действий.
4. Защита конституционных прав гражданина на сохранение личной тайны.
5. Обеспечение прав субъектов в информационных процессах.

В качестве основного средства защиты информации закон предлагает мощные и универсальные средства: лицензирование и сертификацию.

В Ст. 19. данного закона:

Все ИС, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном законом РФ "О сертификации продукции и услуг".

- ИС органов государственной власти, которые обрабатывают информацию с ограниченным доступом, и средства защиты ИС подлежат обязательной сертификации.
- Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности.

- Интересы потребителя информации при использовании импортной продукции защищаются таможенными органами РФ на основе международной системы сертификации.

В Ст. 22 данного закона:

- Владелец документов, ИС обеспечивает уровень защиты информации в соответствии с законодательством РФ.
- Риск, связанный с использованием не сертифицированных ИС и средств, лежит на собственнике этих систем и средств.
- Риск, связанный с использованием информации, полученной от не сертифицированной системы, лежит на потребителе информации.
- Собственник информации имеет право обращаться в организации, осуществляющие сертификацию для проведения анализа достаточности мер защиты.
- Владелец документов, ИС обязан оповещать собственника информационных ресурсов обо всех фактах нарушения режима защиты информации.

О лицензировании отдельных видов деятельности

Закон "О лицензировании отдельных видов деятельности" (05.05.2011) – №99-8ФЗ.

Лицензия – специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении требований и условий, выданная юридическому лицу или индивидуальному предпринимателю.

Ст. 12. устанавливает перечень видов деятельности, на которые требуется лицензия:

1. Разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

2. Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;
3. Деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
4. Разработка и производство средств защиты конфиденциальной информации;
5. Деятельность по технической защите конфиденциальной информации;
6. Производство и реализация защищенной от подделок полиграфической продукции.

Об организации лицензирования отдельных видов деятельности

Постановлением Правительства РФ от 21.11.2011 №957 "Об организации лицензирования отдельных видов деятельности" основными лицензирующими органами в области защиты информации являются:

ФСБ (Федеральная служба безопасности) России:

1. Разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)
2. Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации.
3. Деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
4. Разработка и производство средств защиты конфиденциальной информации.

ФСТЭК (Федеральная служба по техническому и экспортному контролю):

1. Разработка и производство средств защиты конфиденциальной информации
2. Деятельность по технической защите конфиденциальной информации

Об электронной подписи

Закон "Об электронной подписи" (06.04.2011) – №63-ФЗ.

Цель: Обеспечение правовых условий использования ЭП, в которых ЭП признается равнозначной собственноручной подписи в бумажном документе.

Закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи:

- ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;
- ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Согласно этому закону, информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации.

Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.

5.2. Обзор зарубежного законодательства в области информационной безопасности

Рассмотрим некоторые законы нескольких стран (в первую очередь США), т.к. только в США таких законодательных актов около 500.

Ключевую роль играет американский "Закон об информационной безопасности". Его цель – реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

В начале закона называется его конкретный исполнитель – Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту информации.

Согласно Закону, все операторы федеральных ИС, содержащих конфиденциальную информацию, должны сформировать планы обеспечения ИБ. Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерства обороны, энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости. Закон предписывает создать при Министерстве торговли комиссию по информационной безопасности.

Раздел 6 Закона обязывает все правительственные ведомства сформировать план обеспечения ИБ, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, НСД или модификации информации в федеральных системах. Копии плана направляются в НИСТ и АНБ.

Раздел 3 требует от НИСТ по запросам частного сектора готовить добровольные стандарты, руководства, средства и методы для инфраструктуры открытых ключей, позволяющие сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральными ИС.

В разделе 4 особое внимание обращается на необходимость анализа средств и методов оценки уязвимых мест других продуктов частного сектора в области ИБ.

В 1997 году появилось продолжение описанного закона – законопроект "О совершенствовании информационной безопасности", направленный на усиление роли НИСТ и упрощение операций с криптосредствами. В 2001 году был представлен новый вариант законопроекта "О совершенствовании информационной безопасности". За четыре года (1997-2001 гг.) на законодательном и других уровнях ИБ было сделано многое. Смягчены экспортные ограничения на криптосредства (январь 2000 г.). Сформирована инфраструктура с открытыми ключами. Разработано большое число стандартов

(например, новый стандарт ЭП – FIPS 182-2, январь 2000 г.). Независимо от судьбы законопроекта, в США будет сформирована национальная инфраструктура электронной аутентификации. В данном случае законотворческая деятельность идет в ногу с прогрессом ИТ.

Конечно, в законодательстве США имеются в достаточном количестве и положения ограничительной направленности, и директивы, защищающие интересы таких ведомств, Министерство обороны, АНБ, ФБР, ЦРУ.

5.3. Стандарты, оценочные стандарты информационной безопасности

В 1983 г. Министерство обороны США выпустило первый стандарт в области ИБ "Критерии оценки доверенных компьютерных систем". Этот стандарт получил свое название по цвету обложки книги "Оранжевая книга". В ней дается общепризнанный понятийный базис по ИБ.

Основные понятия

В "Оранжевой книге" речь идет не о безопасных, а о доверенных системах, т.е. им можно оказать определенную степень доверия. Книга поясняет понятие "безопасной системы", которая управляет с помощью соответствующих средств доступом к информации так, что только авторизованные лица или процессы получают право читать, записывать, создавать и удалять информацию.

В ней "доверенная система" определяется, как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Степень доверия оценивается по трем критериям:

Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

Чем выше степень доверия системы, тем строже и многообразнее должна быть политика безопасности.

Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС. Он показывает, насколько корректны механизмы, отвечающие за политику безопасности.

Механизм подотчетности (протоколирования) – доверенная система должна фиксировать все события, касающиеся безопасности.

В Оранжевой книге предложены три категории требований безопасности – политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности.

- Требование 1. Политика безопасности. Система должна поддерживать точно определенную политику безопасности.
- Требование 2. Метки. С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа.
- Требование 3. Идентификация и аутентификация. Все субъекты должны иметь уникальные идентификаторы.
- Требование 4. Регистрация и учет. Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе.
- Требование 5. Контроль корректности функционирования средств защиты. Средства защиты должны содержать: независимые аппаратные и/или программные компоненты,обеспечивающие работоспособность функций защиты.
- Требование 6. Непрерывность защиты. Все средства защиты (в том числе и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом.

Приведенные выше базовые требования к безопасности служат основой для критериев, образующих единую шкалу оценки безопасности компьютерных систем, определяющую семь классов безопасности.

Оранжевая книга предусматривает четыре группы критериев, которые соответствуют различной степени защищенности

1. Группа D. Минимальная защита.
2. Группа C. Дискреционная защита.
3. Группа B. Мандатная защита.
4. Группа A. Верифицированная защита.

Приведенные классы безопасности надолго определили основные концепции безопасности и ход развития средств защиты.

Для того чтобы исключить возникшую в связи с изменением аппаратной платформы некорректность некоторых положений Оранжевой книги, адаптировать их к современным условиям и сделать адекватными нуждам разработчиков и пользователей программного обеспечения, и была проделана огромная работа по интерпретации и развитию положений этого стандарта. В результате возник целый ряд сопутствующих Оранжевой книге документов, многие из которых стали ее неотъемлемой частью. К наиболее часто упоминаемым относятся:

- Руководство по произвольному управлению доступом в безопасных системах.
- Руководство по управлению паролями.
- Руководство по применению критериев безопасности компьютерных систем в специфических средах.

Основное назначение доверенной системы – выполнение функций монитора обращений, т.е. контролировать выполнение субъектами определенных операций над объектами ИС.

Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности действий, допустимых для пользователя.

Монитор обращений должен обладать 3-мя качествами:

1. изолированность, т.е. предупредить возможность отслеживания работы монитора.
2. полнота, т.е. монитор должен вызываться при каждом обращении и не должно быть способов обойти его.
3. верифицируемотсть – возможность проанализировать и протестировать монитор и получить достоверность о правильности работы системы в целом.

Механизмы безопасности

Согласно "Оранжевой книге", политика безопасности должна включать следующие элементы:

1. произвольное управление доступом – это метод разграничения доступа к объектам, который заключается в том, что владелец объекта может по своему усмотрению предоставлять или отбирать права доступа к объекту у различных пользователей.
2. безопасность повторного использования объектов – предотвращение от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". Она должна гарантироваться для:
    - а) областей оперативной памяти (для буферов с образами экранов, паролей);
    - б) для дисковых блоков и магнитных носителей в целом.

Метки безопасности – состоят из двух частей:

- уровень секретности;
- список категорий.

Принудительное управление доступом – основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта. Субъект может записывать информацию в объект, если метка безопасности объекта выше, чем метка субъекта.

"Конфиденциальный субъект" может записывать данные в секретные файлы, но не может в несекретные.
Механизм подотчетности является дополнением политики безопасности.
Цель подотчетности – в каждый момент времени знать, кто работает в системе и что делает.
Средства подотчетности делятся на 3 категории:

1. Идентификация.
2. Предоставление доверенного пути.
3. Анализ регистрационной информации.

Идентификация (аутентификация) – ввод имени при входе в систему, стандартное средство проверки пользователя (аутентификация) – пароль.
Предоставление доверенного пути. Путь связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие потенциально опасные компоненты ИС.
Цель предоставления доверенного пути – дать пользователю возможность убедиться в подлинности обслуживающей его системы.
Анализ регистрационной информации – имеет дело с событиями, затрагивающими безопасность ИС.
Фиксировать надо не все, а выборочно протоколировать как в отношении пользователей (следить только за подозрительными), так и отношении событий.
Рассматриваются 2 вида гарантированности:

1. Операционная – относится к архитектурным и реализационным аспектам системы. Включает проверку следующих этапов:
    - • архитектура системы
    - • целостность системы
    - • проверка тайных каналов передачи информации, доверенное администрирование
    - • доверенное восстановление после сбоев
2. Технологическая – относится к методам построения и сопровождения системы. Охватывает весь ЖЦ системы, т.е. периоды проектирования, реализации, тестирования, продажи и сопровождения. Т.е. должны соблюдаться стандарты, чтобы исключить утечку информации и нелегальные "закладки".

Классы безопасности
Определяется 4 уровня доверия. Эти уровни обозначены буквами – D, C, B, A.
Уровень D – предназначен для систем, признанных неудовлетворительными в плане информационной безопасности.
При переходе от уровня C к уровню A требования к системе ожесточаются.
Всего имеется 6 классов безопасности:

- **Класс C1:**

ИС должна управлять доступом именованных пользователей к именованным объектам.
Пользователи должны идентифицировать себя, для аутентификации должен использоваться защитный механизм , например, пароли, от НСД.
Класс должен поддерживать область, защищенную от внешних воздействий, и от попыток слежения за ходом работы.
Должны иметь аппаратные и программные средства, которые позволяют периодически проверять корректность функционирования аппаратных и программных компонентов.
Должен быть прописан подход к безопасности.

- **Класс C2:**

Права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа.
Каждое действие должно ассоциироваться с конкретным пользователем.
Создание, поддержка и защита журнала регистрационной информации, относящейся к доступу к объектам.

- **Класс B1:**

ИС должна управлять метками безопасности, они должны ассоциироваться с объектом и субъектом.
Должна обеспечить реализацию принудительного управления доступом всех субъектов по всем хранимым объектам.
Должна обеспечивать взаимную изоляцию процессов, путем разделения их адресных пространств.
ИС должна быть подвергнута тщательному анализу и тестированию (архитектуры, исходные и объектные кодов).
Должна существовать неформальная и формальная модель политики безопасности.

- **Класс B2:**

Должны снабжаться метками все ресурсы системы, прямо или косвенно доступные субъектам.
Должен поддерживаться доверенный коммуникционный путь для пользователя, выполняющего операции начальной идентификации и аутентификации.
Должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью.
ИС должна быть внутренне структурирована на хорошо определенные и независимые модули.
Должна быть продемонстрирована относительная устойчивость к попыткам проникновения.

Должна быть прописана политика безопасности.

- **Класс B3:**

Для произвольного управления доступом должны обязательно использоваться списки управления доступом с указанием разрешенных режимов.
Должна быть предусмотрена регистрация появления или накопления событий, несущих угрозу политике безопасности.
Должна быть специфицирована роль администрации безопасности.
Должны существовать процедуры и механизмы, позволяющие произвести восстановление после сбоя.
Должна быть продемонстрирована устойчивость системы к попыткам проникновения.

- **Класс A1:**

Тестирование должно продемонстрировать, что реализация доверенной системы соответствует формальным спецификациям верхнего уровня.
Механизм управления безопасностью должен распространятся на весь ЖЦ и все компоненты системы.

5.4. Информационная безопасность распределительных систем

В рекомендациях выделяют сервисы безопасности:

1. Аутентификация-проверка подлинности партнеров по общению и источников данных (предотвращает маскарад, повтор предыдущего сеанса)
2. Управление доступом (защита от несанкционированного использования ресурсов, доступных по сети)
3. Конфиденциальность данных обеспечивает защиту от несанкционированного получения информации. Конфиденциальность трафика – защита информации, которую можно получить.
4. Целостность данных – защищаются не все данные, а только отдельные поля. Обеспечивается восстановление в случае нарушения целостности
5. Неотказуемость – невозможно отказаться от совершенных действий. Выделяют: с подтверждением источника данных и с подтверждением доставки данных.

Сетевые механизмы безопасности:

1. Шифрование.
2. Электронно-цифровая подпись.
3. Механизмы управления доступом- могут располагаться на любой из сторон.
4. Механизмы контроля целостности данных.

- а) целостность отдельного сообщения или поля данных
- б) целостность потока сообщений (от кражи, переупорядочивания, вставки сообщения, временные штампы, криптографическое связывание)

5. Механизмы аутентификации (за счет использования паролей, личных карточек).
6. Механизмы дополнения трафика.
7. Механизмы управления маршрутизации.
8. Механизмы нотаризации обеспечивается надежной третей стороной.

Администрирование средств безопасности

Администрирование включает распространение информации по безопасности и сбор, анализ о функционировании системы безопасности.

Обязанности администратора:

1. Управление ключами: генерация и распределение.
2. Управление шифрованием.
3. Электронно-цифровая подпись.
4. Управление доступом: распределение информации для управления (паролей, списков доступа).
5. Управление аутентификацией.
6. Управление трафиком.
7. Управление маршрутизацией.
8. Управление нотаризацией.

5.5. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

В 1993 г. несколько организаций (семь европейских и североамериканских государственных организаций) объединили усилия по созданию частных нормативных документов по информационной безопасности и начали совместную деятельность по упорядочению своих критериев в одно множество критериев безопасности продуктов информационных технологий (ПИТ), которые могли бы использоваться в рамках международного сотрудничества в данной области. Эта деятельность была названа Проектом общих критериев (ОК). Его целью должно было стать разрешение концептуальных и технических отличий, обнаруженных в предыдущих нормативных документах – источниках критериев, и представление результатов в 130 как исходных положений по разработке международного стандарта.

Версия 1.0 ОК была завершена в январе 1996 г. и одобрена 130 в апреле 1996 г. Затем Проект ОК претерпел ряд изменений, основанных на отзывах, полученных от экспертных организаций. Совет по выполнению ОК завершил

версию 2.0 в октябре 1997 г., которая была принята в качестве второго проекта. В целях сохранения историчности документ использует термин "общие критерии", однако его официальное название – "Критерии оценки безопасности информационной технологии". Объединенным техническим комитетом ISO/IEC UTC был подготовлен Международный стандарт ISO/IEC 15408, тождественный общим критериям.

Стандарт ISO/IEC 15408, состоящий из нескольких частей, определяет критерии, которые должны использоваться как основа для оценки свойств безопасности продуктов информационных технологий. Посредством установления такой базы общих критериев результаты оценки безопасности ПИТ должны быть понятны широкой аудитории.

ОК полезны как руководство для разработки защищенных ПИТ или систем с функциями безопасности и для закупки коммерческих продуктов и систем с такими функциями. Во время оценки такой продукт ПИТ или система называются объектом оценки (00ц). Объекты оценки включают, в частности, операционные системы, вычислительные сети, распределенные системы и прикладные приложения.

ОК рассматривают защиту информации от несанкционированного доступа, модификации или потери возможности использования (потерю доступности). ОК рассматривают угрозы информации, возникающие от человеческой деятельности (преднамеренной или непреднамеренной).

Кроме того, ОК могут применяться и против некоторых угроз, не связанных с человеческим фактором, а также в других областях ПИТ, но не претендуют на корректность вне области безопасности ПИТ. ОК могут быть использованы для выбора соответствующих мер безопасности ПИТ и содержат критерии для оценки требований безопасности.

Существуют три группы с общими интересами в оценке свойств безопасности продуктов и систем ПИТ:

- потребители 00ц;
- разработчики 00ц;
- оценивающие 00ц (эксперты).

Критерии, приводимые в ОК, построены так, чтобы поддерживать интересы всех трех групп. Принципиально все они считаются пользователями ОК.

ОК играют важную роль при выборе потребителем требований безопасности ПИТ для выражения их нужд. Потребители могут использовать результаты оценок, чтобы решить, действительно ли оцениваемый ПИТ удовлетворяет их нужды безопасности. Эти потребности в безопасности обычно определяются в результате как анализа риска, так и выбора направления политики

безопасности. Потребители могут также использовать результаты оценки для сравнения различных продуктов или систем.

ОК предназначены для поддержки разработчиков в подготовке продуктов и систем, их оценке, а также в определении требований безопасности, которым должен удовлетворять каждый из их продуктов или систем.

ОК содержат критерии, которые должны использоваться оценивающими (экспертами) при формировании суждений о соответствии требованиям по их безопасности. ОК описывают множество общих действий, которые должен выполнить эксперт, и функции безопасности, в соответствии с которыми выполняются эти действия. Хотя ОК ориентированы на определение и оценку свойств ПИТ, они также могут быть полезны в в.качестве справочного материала для всех, кто заинтересован в безопасности или отвечает за безопасность ПИТ. Использование общей методологии оценок содействует воспроизводимости и объективности результатов, но само по себе не является достаточным. Многие из критериев оценки требуют применения экспертного заключения и дополнительных знаний и навыков, по которым труднее достичь согласованности.

Суть данного стандарта: как произвести оценку безопасности.

Этапы критериев:

1. Определение назначений, целей, требований, условий применения безопасности.
2. Проектирование и разработка.
3. Испытание, оценка, сертификация.
4. Внедрение и эксплуатация.

Выделяют системы: 10 классов, 44 семейства, 93 компонента.

Гармонизированные критерии иностранных стран, опубликованные в июне 1991 г. Францией, Германией, Нидерландами, Великобританией

Важной чертой является отсутствие требований к условиям, в которых должна работать информационная система.

Организация, запрашивающая сертификационные услуги, формулирует цель оценки, т.е. описывает условия, в которых должны работать системы, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации: оценить насколько полно достигаются поставленные цели, т.е. насколько корректны и эффектны архитектура системы и реализация механизма безопасности в описанных спонсором условиях.

Руководящие документы Гостехкомиссии России

Выпущено два основных документа:

1. "Классификация авторизованных систем" по уровню защищенности от несанкционированного доступа.

2. "Классификация межсетевых экранов".

Согласно первому документу устанавливается 9 классов защищенности. Каждый класс характеризуется определяемой минимумом совокупностью требований по защите. Классы делятся на три группы: 1,2,3. в пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности информации.

3 группа классифицирует авторизованные системы, в которых работает один пользователь, имеющий доступ ко всей информации авторизованной системы, размещаемой на носителях конфиденциальности. К этой группе относятся: 3А и 3Б.

2 группа классифицирует авторизованные системы, в которых пользователи имеют одинаковые права доступа ко всей информации авторизованной системы, обрабатываемой или хранящейся на носителях различного уровня конфиденциальности. К этой группе относятся: 2А и 2Б.

1 группа классифицирует многопользовательские авторизованные системы, в которых одновременно обрабатывается и хранится информация различных уровней конфиденциальности и не все пользователи имеют право доступа.

5.6. Европейские критерии безопасности информационных технологий

Для того чтобы удовлетворить требованиям конфиденциальности, целостности и работоспособности, в Европейских критериях впервые вводится понятие адекватности средств защиты.

Адекватность включает в себя:

- эффективность, отражающую соответствие средств безопасности решаемым задачам;
- корректность, характеризующую процесс их разработки и функционирования.

Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации.

Набор функций безопасности может специфицироваться с использованием ссылок на заранее определенные классы-шаблоны. В Европейских критериях таких классов десять. Пять из них соответствуют классам безопасности Оранжевой книги, другие пять классов, так как их требования отражают точку зрения разработчиков стандарта на проблему безопасности.

- Предназначены для систем с высокими потребностями в обеспечении целостности, что типично для систем управления базами данных.
- Характеризуется повышенными требованиями к обеспечению работоспособности.

- Ориентированы на распределенные системы обработки информации.
- Уделяют особое внимание требованиям к конфиденциальности передаваемой информации.
- Предъявляют повышенные требования и к целостности, и к конфиденциальности информации.

Европейские критерии определяют семь уровней адекватности от минимальной адекватности (аналог уровня D Оранжевой книги). При проверке адекватности анализируется весь жизненный цикл системы – от начальной фазы проектирования до эксплуатации и сопровождения. Другие уровни адекватности выстроены по нарастанию требований тщательности контроля.

Тема 6. Основные положения теории информационной безопасности. Модели безопасности и их применение

6.1. Механизмы обеспечения информационной безопасности

Идентификация и аутентификация

Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Наличие процедур аутентификации и/или идентификации пользователей является обязательным условием любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

- набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);
- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на паролях – конфиденциальных идентификаторах субъектов. В этом случае при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам системы.

Парольные методы аутентификации по степени изменяемости паролей делятся на:

- методы, использующие постоянные (многократно используемые) пароли;
- методы, использующие одноразовые (динамично изменяющиеся) пароли.

Использование одноразовых или динамически меняющихся паролей является более надежным методом парольной защиты.

В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

- пассивные (карточки с памятью);
- активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе, и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двухкомпонентной аутентификацией.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, например, многоразовые пароли, динамически меняющиеся пароли.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100 % идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако эти методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться, требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, по почерку, по тембру голоса и др.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что исключает их перехват. Такой метод аутентификации может быть использован в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Механизм идентификации и аутентификации пользователей

Общая процедура идентификации и аутентификации пользователя при его доступе в защищенную информационную систему заключается в следующем.

Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор.

В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным

условием для защищенных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

В целом аутентификация по уровню информационной безопасности делится на три категории:

1. статическая аутентификация. Первая категория обеспечивает защиту только от несанкционированных действий в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.
2. устойчивая аутентификация. Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Устойчивая аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и использовать ее в следующих сеансах работы.
3. постоянная аутентификация. Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных. Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

6.2. Криптография и шифрование

Структура криптосистемы

Самый надежный технический метод защиты информации основан на использовании криптосистем. Криптосистема включает:

- алгоритм шифрования;

- набор ключей (последовательность двоичных чисел), используемых для шифрования;
- систему управления ключами.

Общая схема работы криптосистемы показана на рисунке 6.1.

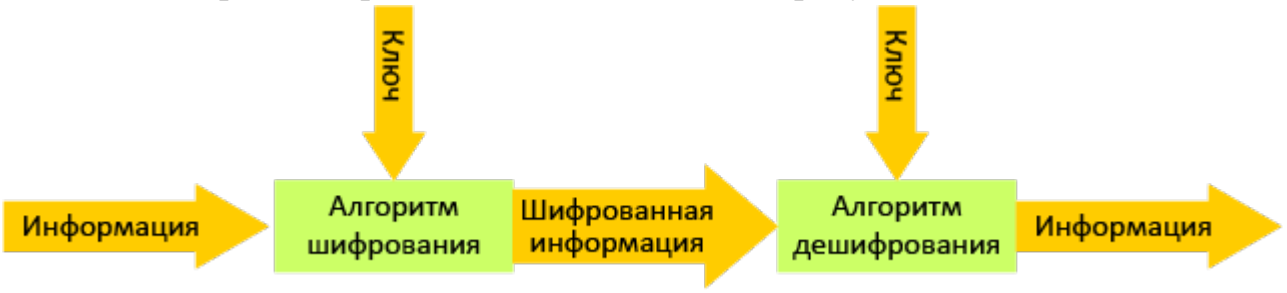


Рисунок 6.1 – Общая схема работы криптосистемы

Криптосистемы решают такие проблемы информационной безопасности, как обеспечение конфиденциальности, целостности данных, а также аутентификацию данных и их источников.

Криптографические методы защиты являются обязательным элементом безопасных информационных систем. Особое значение криптографические методы получили с развитием распределенных открытых сетей, в которых нет возможности обеспечить физическую защиту каналов связи.

Классификация систем шифрования данных

Основным классификационным признаком систем шифрования данных является способ их функционирования. По способу функционирования системы шифрования данных делят на два класса:

- системы "прозрачного" шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах прозрачного шифрования (шифрование "на лету") криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование. Системы второго класса обычно представляют собой утилиты (программы), которые необходимо специально вызывать для выполнения шифрования.

Как уже отмечалось, особое значение криптографические преобразования имеют при передаче данных по распределенным вычислительным сетям. Для защиты данных в распределенных сетях используются два подхода: канальное шифрование и оконечное (абонентское) шифрование.

В случае канального шифрования защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством: встраивание процедур шифрования на канальный

уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы.

Оконечное (абонентское) шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами. В этом случае защищается только содержание сообщений, вся служебная информация остается открытой.

Симметричные и асимметричные методы шифрования

Классические криптографические методы делятся на два основных типа: симметричные (шифрование секретным ключом) и асимметричные (шифрование открытым ключом).

В симметричных методах для шифрования и расшифровывания используется один и тот же секретный ключ. Наиболее известным стандартом на симметричное шифрование с закрытым ключом является стандарт для обработки информации в государственных учреждениях США DES (Data Encryption Standard). Общая технология использования симметричного метода шифрования представлена на рисуцнке 6.2.

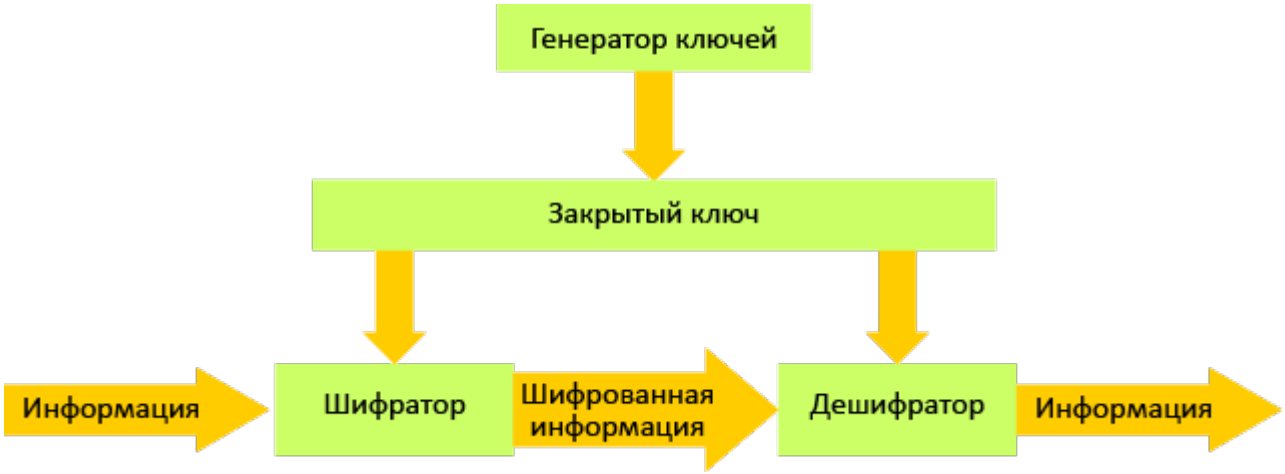


Рисунок 6.2 – Шифрование секретным ключом

Основной недостаток этого метода заключается в том, что ключ должен быть известен и отправителю, и получателю. Это существенно усложняет процедуру назначения и распределения ключей между пользователями. Указанный недостаток послужил причиной разработки методов шифрования с открытым ключом – асимметричных методов.

Асимметричные методы используют два взаимосвязанных ключа: для шифрования и расшифрования. Один ключ является закрытым и известным только получателю. Его используют для расшифрования. Второй из ключей является открытым, то есть он может быть общедоступным по сети и опубликован вместе с адресом пользователя.

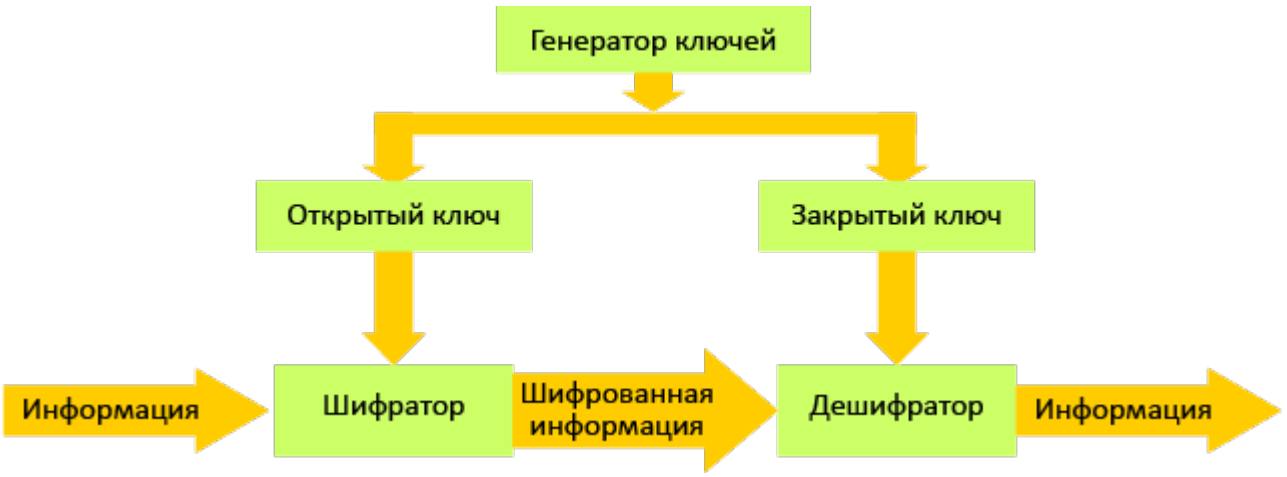


Рисунок 6.3 – Шифрование открытым ключом

Его используют для выполнения шифрования. Схема функционирования данного типа криптосистемы показана на рисунке 6.3.

В настоящее время наиболее известным и надежным является асимметричный алгоритм RSA (Rivest, Shamir, Adleman).

Электронная подпись

Для контроля целостности передаваемых по сетям данных используется электронная подпись, которая реализуется по методу шифрования с открытым ключом.

Электронная подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Идея технологии электронной подписи состоит в следующем. Отправитель передает два экземпляра одного сообщения: открытое и расшифрованное его закрытым ключом (то есть обратно шифрованное). Получатель шифрует с помощью открытого ключа отправителя расшифрованный экземпляр. Если он совпадет с открытым вариантом, то личность и подпись отправителя считается установленной.

При практической реализации электронной подписи также шифруется не все сообщение, а лишь специальная контрольная сумма – хэш, защищающая послание от нелегального изменения. Электронная подпись здесь гарантирует как целостность сообщения, так и удостоверяет личность отправителя.

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети. Различают следующие виды функций управления ключами: генерация, хранение и распределение ключей.

Способы генерации ключей для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами.

Функция хранения предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ (то есть мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключа является наиболее критическим вопросом криптозащиты.

Распределение – самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным. Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.

6.3. Методы разграничение доступа

Виды методов разграничения доступа

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются: списком ресурсов, доступным пользователю, и правами по доступу к каждому ресурсу из списка.

Существуют следующие методы разграничения доступа:

1. разграничение доступа по спискам;
2. использование матрицы установления полномочий;
3. разграничение доступа по уровням секретности и категориям;
4. парольное разграничение доступа.

При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в информационную систему, а столбцами – объекты (ресурсы) информационной системы. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Данный метод предоставляет более унифицированный и удобный подход, так как вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток – пустые).

Фрагмент матрицы установления полномочий показан в таблице 6.1.

Таблица 6.1 – Матрица полномочий

	Диск c:	**Файл d:\prog. exe**	**Принтер**
Пользователь 1	Чтение Запись Удаление	Выполнение Удаление	Печать Настройка параметров
Пользователь 2	Чтение	Выполнение	Печать с 9:00 до 17:00
Пользователь 3	Чтение Запись	Выполнение	Печать с 17:00 до 9:00

Разграничение доступа по уровням секретности и категориям заключается в разделении ресурсов информационной системы по уровням секретности и категориям.

При разграничении по степени секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем ему определен, например, пользователь имеющий доступ к данным "секретно", также имеет доступ к данным "конфиденциально" и "общий доступ".

При разграничении по категориям задается и контролируется ранг категории пользователей. Соответственно, все ресурсы информационной системы разделяются по уровням важности, причем определенному уровню соответствует категория пользователей. В качестве примера, где используются категории пользователей, приведем операционную систему Windows XP, подсистема безопасности которой по умолчанию поддерживает следующие

категории (группы) пользователей: "администратор", "опытный пользователь", "пользователь" и "гость". Каждая из категорий имеет определенный набор прав. Применение категорий пользователей позволяет упростить процедуры назначения прав пользователей за счет применения групповых политик безопасности.

Парольное разграничение представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

Разграничение прав доступа является обязательным элементом защищенной информационной системы.

Мандатное и дискретное управление доступом

В ГОСТ Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации" и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа:

1. Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.
2. Мандатное управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

При внимательном рассмотрении можно заметить, что дискретное управление доступом есть не что иное, как произвольное управление доступом, а мандатное управление реализует принудительное управление доступом.

6.4. Регистрация и аудит

Определение и содержание регистрации и аудита информационных систем

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;

- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа;
- изменение статуса объектов доступа и т. д.

Для сертифицируемых по безопасности информационных систем список контролируемых событий определен рабочим документом Гостехкомиссии РФ: "Положение о сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации".

Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

Аудит – это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день).

Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения информационной безопасности:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Рассматриваемые механизмы регистрации и аудита являются сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям – за возможные критические ошибки. Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный)журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемого администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Обнаружение попыток нарушений информационной безопасности входит в функции активного аудита, задачами которого является оперативное выявление

подозрительной активности и предоставление средств для автоматического реагирования на нее.

Подозрительная активность – поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Например, подсистема аудита, отслеживая процедуру входа (регистрации) пользователя в систему подсчитывает количество неудачных попыток входа. В случае превышения установленного порога таких попыток подсистема аудита формирует сигнал о блокировке учетной записи данного пользователя.

Этапы регистрации и методы аудита событий информационной системы

Организация регистрации событий, связанных с безопасностью информационной системы включает как минимум три этапа:

1. сбор и хранение информации о событиях;
2. защита содержимого журнала регистрации;
3. анализ содержимого журнала регистрации.

На первом этапе определяются данные, подлежащие сбору и хранению, период чистки и архивации журнала, степень централизации управления, место и средства хранения журнала, возможность регистрации шифрованной информации и др.

Регистрируемые данные должны быть защищены, в первую очередь, от несанкционированной модификации и, возможно, раскрытия.

Самым важным этапом является анализ регистрационной информации. Известны несколько методов анализа информации с целью выявления несанкционированных действий.

Статистические методы основаны на накоплении среднестатистических параметров функционирования подсистем и сравнении текущих параметров с ними.

Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз.

Эвристические методы используют модели сценариев несанкционированных действий, которые описываются логическими правилами, или модели действий, по совокупности приводящие к несанкционированным действиям.

6.5. Межсетевое экранирование

Классификация межсетевых экранов

Одним из эффективных механизмов обеспечения информационной безопасности в распределенных вычислительных сетях является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет межсетевой экран или брандмауэр (firewall).

Межсетевой экран – программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации.

Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

- по месту расположения в сети – на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
- по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов, например, при использовании сетевой операционной системы Novell Netware следует принимать во внимание протокол SPX/IPX.

Характеристика межсетевых экранов

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI. Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

1. межсетевые экраны с фильтрацией пакетов. Межсетевые экраны с фильтрацией пакетов представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их со сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы. Основным недостатком является их уязвимость при подмене адресов IP. Кроме того, они сложны при конфигурировании:

для их установки требуется знание сетевых, транспортных и прикладных протоколов.

2. шлюзы сеансового уровня. Шлюзы сеансового уровня контролируют допустимость сеанса связи. Они следят за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функцию трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым исключая подмену IP-адреса. Однако в таких межсетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.
3. шлюзы прикладного уровня. Шлюзы прикладного уровня проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип межсетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети Интернет (HTTP, FTP, Telnet и т. д.) и служат для проверки сетевых пакетов на наличие достоверных данных. Шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно в Интернете при работе по низкоскоростным каналам, но существенно при работе во внутренней сети.

4. межсетевые экраны экспертного уровня. Межсетевые экраны экспертного уровня сочетают в себе элементы всех трех описанных выше категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Межсетевые экраны экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И, наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации. Вместо применения связанных с приложениями программ-посредников,

брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработки данных на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что теоретически должно обеспечить более эффективную фильтрацию пакетов.

Таблица 6.2 – Типы межсетевых экранов и уровни модели ISO OSI

Уровень модели OSI	**Протокол**	**Тип**
Прикладной	Telnet, FTP, DNS, NFS, SMTP, HTTP	Шлюз прикладного уровня Межсетевой экран экспертного уровня
Сеансовый	TCP, UDP	Шлюз сеансового уровня
Транспортный	TCP, UDP	
Сетевой	IP, ICMP	Межсетевой экран с фильтрацией пакетов
Канальный	ARP, RAP	
Физический	Ethernet	

6.6. Технология виртуальных частных сетей (VPN)

Технология виртуальных частных сетей (VPN – Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

- шифрования (с использованием инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);
- экранирования (с использованием межсетевых экранов);
- туннелирования.

Сущность технологии VPN заключается в следующем.

На все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливается VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

Перед отправкой IP-пакета VPN-агент выполняет следующие операции:

- анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут, поддерживать одновременно несколько алгоритмов шифрования и контроля целостности). Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;

- вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;
- пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);
- формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

При получении IP-пакета выполняются обратные действия:

- из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);
- согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);
- после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложна только настройка VPN-агентов, которая может быть выполнена очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

Понятие "туннеля" при передаче данных в сетях

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется "туннелем", а технология его создания называется "туннелированием"). Вся информация передается по туннелю в зашифрованном виде.

Одной из обязательных функций VPN-агентов является фильтрация пакетов, которая реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

Тема 7. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии

7.1. Криптографические методы защиты информации

Криптографические методы защиты информации – преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на то полномочия.

Различают 4 группы методов криптографического преобразования:

1. **Шифрование**

Шифрование заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которого зашифрованная информация представляет собой хаотический набор букв, цифр и других символов.

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация, подлежащая шифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования.

2. **Стеганография**

Стеганография позволяет скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации.

3. **Кодирование**

Кодирование есть замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование применяют в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях АСУ. Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять,

чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

4. **Сжатие**

Сжатие – сокращение объема информации. Сжатая информация не может быть прочитана или использована без обратного преобразования.

Шифрование

Существуют процессы:

1. Зашифрование.
2. Расшифрование.

Современные методы шифрования должны отвечать следующим требованиям:

- стойкость шифра (противостоять криптоанализу (криптостойкость)) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- шифртекст не должен существенно превосходить по объему исходную информацию;
- ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
- время шифрования не должно быть большим;
- стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ.

Все методы шифрования могут быть классифицированы по различным признакам. Один из вариантов классификации приведен на рисунке 7.1.

Рисунок 7.1 – Классификация методов шифрования

Элементарные понятия криптографии

Наука о шифрах получила название криптология, слово образовано из двух греческих: "criptos" – тайный и "logos" – сообщение (слово). С самого начала криптология включала две взаимодополняющие ветви: криптографию, в которой изучались методы шифрования сообщений, и криптоанализ, где разрабатывались методы раскрытия шифров.

Рисунок 7.2 – Криптология

Возникновение шифров относится к глубокой древности, когда возникла потребность в обеспечении секретности некоторых ценных сведений или важных сообщений. Один из самых древних зашифрованных текстов был найден при раскопках в Месопотамии. Глиняная табличка, относящаяся к 20 веку до н.э., содержала рецепт глазури для покрытия гончарных изделий. Долгое время она была уделом талантливых одиночек и считалась искусством на грани черной магии.

До середины 20 века криптология выступала скорее как искусное ремесло, а не наука, как удел узкого круга избранных лиц. Однако большое количество эмпирического материала в области разработки, применения и раскрытия шифров, накопленного к этому времени, особенно в ходе мировых войн, создали предпосылки для научного обобщения криптологических знаний. Основополагающей работой криптологии считается работа американского ученого Клода Шеннона "Теория связи в секретных системах", опубликованная в 1949 году.

Все древние шифры были ручными, а значит весьма трудоемкими при шифровании длинных текстов. В 19-м веке появились сначала механические, а в 20-м – электромеханические и электронные устройства шифрования/дешифрования, а затем и компьютерные реализации таких алгоритмов. С широким распространением ЭВМ в начале 70-х годов появилась новая разновидность шифров – блочные, ориентированные на операции с машинными словами. До этого все шифры предполагали последовательную позначную обработку информации (их стали называть поточными шифрами).

Шифр – это множество обратимых преобразований формы сообщения с целью его защиты от несанкционированного прочтения.

Исходное сообщение, которое подвергается шифрованию, называется открытым текстом, а результат, полученный применением преобразования шифра к исходному сообщению, называется шифртекстом или криптограммой. Переход от открытого текста к шифртексту называется зашифрованием, а обратный переход – расшифрованием.

Принцип построения преобразования шифра (или просто шифра) всегда предполагает множество вариантов его реализации, а для конкретных случаев использования шифра выбирается вполне определенный вариант. Совокупность данных, определяющих конкретное преобразование шифра из множества возможных, называется ключом.

Стойкость шифра – это способность противостоять попыткам постороннего лица восстановить (дешифровать) открытый текст по перехваченному шифртексту.

В этих попытках криптоаналитик сначала пытается предугадать принцип построения шифра, а затем определить ключ. Сравнительная стойкость шифров оценивается ориентировочно по времени, необходимому противнику, вооруженному современными средствами вычислительной техники, чтобы каким-либо способом (например, полным перебором вариантов), дешифровать сообщение. Чем больше вариантов ключей возможно, тем более трудным для дешифрования является шифр.

Однако получателю зашифрованного сообщения ключ должен быть известен, чтобы он имел возможность восстановить открытый текст. Очевидно, для нормального функционирования такой системы ключ должен храниться в секрете, поэтому она получила название криптосистемы (или шифросистемы) с секретным ключом. Иными словами: К. Шеннон рассматривает шифрование как отображение исходного сообщения в зашифрованное:

$C = F_i M$,

где С – криптограмма,

F_i – отображение,

M – исходное состояние.

Индекс i соответствует конкретному используемому ключу. Для того, чтобы была возможность однозначного дешифрования сообщения отображение F_i должно иметь обратное отображение. Тогда:

$$M = F_i^{-1}C$$

Схема функционирования криптосистемы с секретным ключом (модель К.Шеннона) показана на рисунке 7.3.

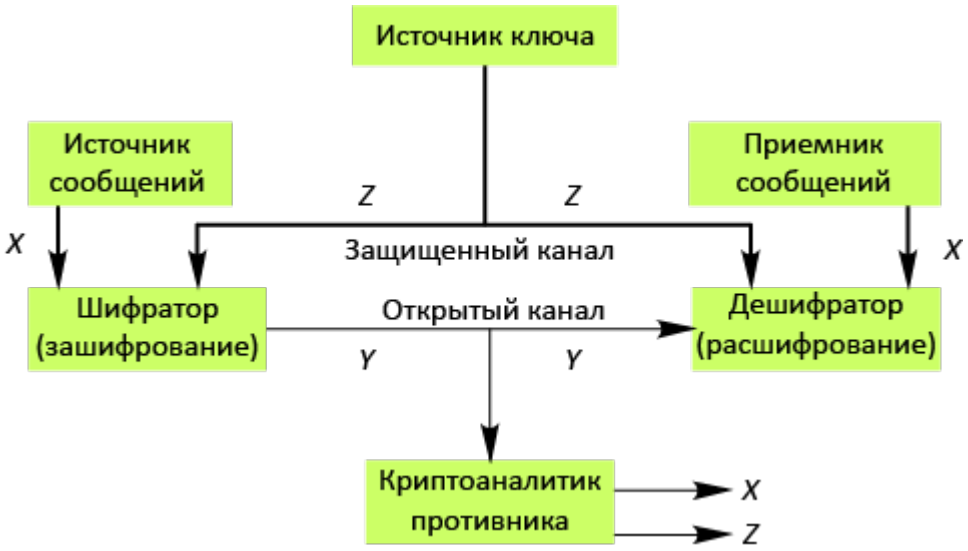


Рисунок 7.3 – Криптосистема с секретным ключом

Источник сообщений порождает открытый текст X. Источник ключей определяет ключ шифра Z, и шифратор источника с его помощью преобразует открытый текст X в шифртекст Y, который передается по открытому каналу. Шифратор приемника делает обратное преобразование, получая с помощью ключа Z открытый текст X из шифртекста Y. Важнейшей частью модели криптографической системы с секретным ключом является "защищенный" канал, по которому передается ключ. Это канал повышенной надежности и секретности, за которым может стоять некоторое устройство или даже специальный курьер. Строго говоря, защищенными должны быть все элементы системы, в которых используется секретный ключ.

Прежде чем переходить к рассмотрению современного состояния криптологии, заглянем немного в историю ее раннего развития.

7.2. Методы шифрования информации

Существуют следующие типы шифрования:

1. Шифр замены.
2. Шифр перестановки.
3. Комбинация шифра замены и перестановки.

Общие сведения

Самыми древними шифрами являются шифры подстановки (или шифры замены), когда буквы сообщения по какому-либо правилу заменяются другими символами. Например, следующее сообщение получено шифром замены (только букв).

О н р ъ к я э _ й в _ б ж п ъ б ц я с й з.

Сказать о нем что-то определенно трудно, так как мало информации. Но ключ здесь очень простой, достаточно увидеть открытый текст.

П о с ы л а ю _ к г _ в з р ы в ч а т к и.

Если кто не догадался, то каждая буква здесь была заменена на ее предшественницу в алфавите ("о" вместо "п", "н" вместо "о", "р" вместо "с", "к" вместо "л", "я" вместо "а" и т.п.).

Подобные шифры широко использовались в древности, достоверно известно, что Ю.Цезарь применял шифр замены со сдвигом на три буквы вперед при шифровании. Метод дешифрования шифра подстановки описан у Конан-Дойля в рассказе "Пляшущие человечки": достаточно сначала догадаться хотя бы об одном слове – появляются несколько известных букв, подставляя их в зашифрованный текст, можно угадать другие слова и узнать новые буквы и т.д.

Более формальный подход к дешифрованию основан на использовании средней частоты появления букв в текстах. Впервые похожий метод был предложен в конце 15-го века (итальянский математик Леон Баттиста Альберти) и использовал свойство неравномерности встречаемости разных букв алфавита. Позднее были определены средние частоты использования букв языка в текстах. Некоторые из них приведены в таблице 7.1.

Таблица 7.1 – Средние частотыиспользованиябукв

Язык	**Буквы высокой частоты использования (%)**					
Английский язык	E (12,9)	T (9,7)	A (8,0)	I (7,5)	N (7,0)	R (7,0)
Немецкий язык	E (19,2)	N (10,2)	I (8,2)	S (7,0)	R (7,0)	T (5,9)
Русский язык	О (11,0)	И (8,9)	Е (8,3)	А (7,9)	Н (6,9)	Т (6,0)

Теперь, имея шифртексты, можно было провести в них частотный анализ использования символов и на его основе получить (при неограниченном количестве шифрсообщений) точные значения всех букв. Но так как материала, как правило, не очень много, то частотный анализ дает приблизительные результаты, поэтому можно лишь с высокой долей вероятности предположить буквенное значение самых частоупотребимых символов, а далее – необходимо подставлять их в шифртексты и пытаться угадывать слова, однако результаты появляются достаточно быстро. Увлекательно на эту тему повествовал Эдгар По в своем "Золотом жуке".

На слабость шифров однозначной замены обратили внимание еще в 15-м веке. Случайные догадки – кто и кому пишет, названия городов и селений, часто употребляемые слова, вроде предлогов, – могли привести к почти мгновенному раскрытию шифра. Попытки модификации основывались на многозначной замене букв открытого текста с использованием ключевой последовательности (ключевого слова или ключа).

В наиболее чистом виде этот подход можно изложить так. Пусть мы хотим получить 10 вариантов (0, 1, ..., 9) замены каждой буквы исходного текста (в таблице 7.2 вариант замены определяет величину сдвига по алфавиту).

Придумаем ключевую последовательность из цифр 0...9 произвольной длины (например, 190 277 321 856 403). Для открытого текста надпишем над буквами цифры ключа (периодически) и выполним зашифрование, выбирая вариант замены по цифре ключа. Хорошо видно, что одни и те же буквы заменяются по разному, а разные буквы могут быть представлены одинаково:

1 9 0 2 7 7 3 2 1 8 5 6 4 0 3 1 9 0 2 7 7 3 2 1 8 5 6 ...

Наша _ Таня _ громко _ плачет, уронила ...

Ойшв _ щзрб _ дшутоо _ тмкчзщ, ыуроррж ...

Таблица 7.2 – Таблица вариантов замены

Буква	**Вариант**									
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
А	а	б	в	г	д	е	ж	з	и	й
Б	б	в	г	д	е	ж	з	и	й	к
В	в	г	д	е	ж	з	и	й	к	л
...	...	...	...	...	...	...	...	...	...	...
Я	я	а	б	в	г	д	е	ж	з	и

Идея фактически была предложена в 16-м веке французским дипломатом Блезом де Вижинером. Вместо цифр им использовались буквы, и ключевая последовательность представляла собой слово.

Легко видеть, что алгоритм многозначной замены определяет совокупность преобразований шифра, отличающихся параметром – ключевой последовательностью шифрования (ключом). Это позволяет строить надежную криптосистему на основании фиксированного (несекретного) алгоритма шифрования, но секретного ключа, который регулярно меняется. Теоретически такой шифр поддается дешифрованию на основе частотного анализа употребления букв, но для этого требуется, чтобы длина шифрсообщений, сделанных с этим ключом, значительно превышала длину самого ключа.

На основе алгоритма многозначной замены были разработаны и нашли широкое применение (особенно во время второй мировой войны) дисковые шифровальные машины. Сконструированные на принципах, используемых в арифмометрах, шифрмашины содержали 6-10 дисков на общей оси, которые могли дискретно поворачиваться один относительно другого, создавая на каждом такте уникальное сочетание из всех возможных сочетаний угловых положений.

Принцип работы дисков был одновременно открыт четырьмя изобретателями из разных стран (американец – 1918 г., голландец – 1919 г., швед – 1919г., немец Артур Шербиус – 1927 г.). Именно он сконструировал энигму (в переводе с немецкого – "загадка").

В диски из электроизоляционного материала были впрессованы латунные контактные площадки (соответствующие отдельным буквам) с каждой стороны, которые попарно соединялись внутри диска. Таких дисков (разных) в комплект шифрмашины входило больше, чем использовалось в работе. Кроме изменения набора рабочих дисков, они могли нанизываться на ось в произвольном порядке, начальный угол установки каждого диска также можно было менять.

При шифровании на контакты одного из крайних дисков подается напряжение, которое последовательно передается на связанный контакт последнего диска, чем осуществляется замена буквы исходного текста на другую букву. Затем выполняется дискретный угловой поворот первого диска, и возможно, связанных с ним других дисков, устанавливая следующие сочетания замены. Для дешифровки сообщения на шифрмашине достаточно было поменять местами вход и выход.

Такие шифрмашины использовались в войсковых соединениях и посольствах для взаимного обмена секретными сообщениями. Для работы утверждался секретный график их модификации, например:

- еженедельно устанавливается новый набор рабочих дисков;
- ежедневно устанавливается новый порядок дисков на оси;
- для каждого нового сообщения некоторому получателю в течении дня устанавливается новое начальное угловое положение дисков.

Этим фактически неявно определялось множество ключей, используемых в алгоритме шифрования.

Оригинальный вариант алгоритма многозначной замены был предложен в 1917 году американским инженером Г.С. Вернамом. Он предназначался для шифрования текстов, представленных в двоичном (телеграфном) коде (код Бодо). Главным элементом был секретный (двоичный) ключ, цифры которого как бы надписывались над исходным кодом, а шифрсообщение (также в двоичном коде) формировалось применением операции "исключающее ИЛИ"

(сложение по модулю два) к двоичным цифрам исходного текста и ключа. Как было установлено значительно позднее (доказал К.Шеннон), стойкость шифра Г.С. Вернама очень высока, если длина ключа не меньше длины сообщения (практически нераскрываемый шифр). Казалось бы проблема решена, но здесь имеются трудности с ключами (их качество, хранение, уничтожение, транспортировка). На каждом этапе существует угроза их безопасности. Поэтому этот метод используют в исключительных случаях.

Первый кто "породил" метод замены был Юлий Цезарь. Он каждую букву циклически заменял третьей буквой. Например: А Б В Г Д Е Ж З И К Л М Н О П Р С Т и т.д., тогда зашифрованное слово ЗОВ будет выглядеть следующим образом: МТЖ.

В средние века использовали квадрат Полибия. Это первый табличный способ шифрования. Для этого брался квадрат 6х6 в котором по строкам вписаны все буквы алфавита. Метод заключается в том, чтобы заменить исходную букву буквой, которая стоит ниже по квадрату Полибия. Алгоритм усложнится , если буквы в квадрате расположить не по алфавиту, а в беспорядке. Все эти шифр замены легко вскрываются, т.к. есть закономерность появления сдвоенных букв.

Рассмотрим более подробно методы замены.

7.3. Методы замены

Метод прямой замены

Сущность методов замены (подстановки) заключается в замене символов исходной информации, записанных в одном алфавите, символами из другого алфавита по определенному правилу. Самым простым является метод прямой замены. Символам S_{0i} исходного алфавита A_0, с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы S_{1i} шифрующего алфавита A_1. В простейшем случае оба алфавита могут состоять из одного и того же набора символов. Например, оба алфавита могут содержать буквы русского алфавита.

Задание соответствия между символами обоих алфавитов осуществляется с помощью преобразования числовых эквивалентов символов исходного текста T_0, длиной – K символов, по определенному алгоритму.

Алгоритм моноалфавитной замены может быть представлен в виде последовательности шагов.

Шаг 1

Формирование числового кортежа L_{0h} путем замены каждого символа $S_{0i} \in T_0 (i = \overline{1,K})$, представленного в исходном алфавите A_0 размера $[1 \times K]$, на число $h_{0i}(S_{0i})$, соответствующее порядковому номеру символа S_{0i} в алфавите A_0.

Шаг 2

Формирование числового кортежа L_{1h} путем замены каждого числа кортежа ш на соответствующее число h_{1h} кортежа L_{1h}, вычисляемое по формуле:

$$h_{1i} = \left(k_1 * h_{0i}\left(S_{0i}\right) + k_2\right) (\mathrm{mod}\, R),$$

где k_1 – десятичный коэффициент;

k_2 – коэффициент сдвига.

Выбранные коэффициенты k_1, k_2 должны обеспечивать однозначное соответствие чисел h_{0i} и h_{1h}, а при получении $h_{1h}=0$ выполнить замену $h_{1h}=R$.

Шаг 3

Получение шифртекста T_1 путем замены каждого числа $h_{1i}(s_{1i})$ кортежа L_{1h} соответствующим символом $S_{1i} \in T_1 (i = \overline{1,K})$ алфавита шифрования A_1 размера $[1 \times R]$.

Шаг 4

Полученный шифртекст разбивается на блоки фиксированной длины b. Если последний блок оказывается неполным, то в конец блока помещаются специальные символы-заполнители (например, символ *).

Пример. Исходными данными для шифрования являются:

$T_0 = <М\ Е\ Т\ О\ Д\ \_\ Ш\ И\ Ф\ Р\ О\ В\ А\ Н\ И\ Я>;$

$A_0 = <А\ Б\ В\ Г\ Д\ Е\ Ж\ З\ И\ К\ Л\ М\ Н\ О\ П\ Р\ С\ Т\ У\ Ф\ Х\ Ц\ Ч\ Ш\ Щ\ Ъ\ Ы\ Ь\ Э\ Ю\ Я\ \_>;$

$A_1 = <О\ Р\ Щ\ Ь\ Я\ Т\ Э\ \_\ Ж\ М\ Ч\ Х\ А\ В\ Д\ Ы\ Ф\ К\ С\ Е\ З\ П\ И\ Ц\ Г\ Н\ Л\ Ъ\ Ш\ Б\ У\ Ю>;$

$R = 32;\ k_1 = 3;\ k_2 = 15;\ b = 4.$

Пошаговое выполнение алгоритма приводит к получению следующих результатов.

Шаг 1

L_{0h} = <12, 6, 18, 14, 5, 32, 24, 9, 20, 16, 14, 3, 1, 13, 9, 31>.

Шаг 2

L_{1h} = <19, 1, 5, 25, 30, 15, 23, 10, 11, 31, 25, 24, 18, 22, 10, 12>.

Шаг 3

T_1 = <С О Я Г Б Д И М Ч У Г Ц К П М Х>.

Шаг 4

T_2 = <С О Я Г Б Д И М Ч У Г Ц К П М Х>.

При расшифровании сначала устраняется разбиение на блоки. Получается непрерывный шифртекст T_1 длиной K символов. Расшифрование осуществляется путем решения целочисленного уравнения:

$$k_1 h_{01} + k_2 = nR + h_{1i}$$

При известных целых величинах k_1, k_2, h_{1h} и R величина h_{0i} вычисляется методом перебора n.

Последовательное применение этой процедуры ко всем символам шифртекста приводит к его расшифрованию.

По условиям приведенного примера может быть построена таблица замены, в которой взаимозаменяемые символы располагаются в одном столбце (см. таблицу 7.3).

Таблица 7.3 – Таблица замены

s_{0i}	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
h_{0i}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	25	26	27	28	29	30	31	32
s_{1i}	К	З	Ц	Л	Б	О	Ь	Э	М	А	Ы	С	П	Г	Ъ	У	Р	Я	_	Ч	В	Ф	Е	Н	Ш	Ю	Щ	Т	Ж	Х	Д

Использование таблицы замены значительно упрощает процесс шифрования. При шифровании символ исходного текста сравнивается с символами строки S_{0i} таблицы. Если произошло совпадение в i-м столбце, то символ исходного текста заменяется символом из строки S_{1i}, находящегося в том же столбце i таблицы.

Расшифрование осуществляется аналогичным образом, но вход в таблицу производится по строке S_{1i}.

Основным недостатком метода прямой замены является наличие одних и тех же статистических характеристик исходного и закрытого текста. Зная, на каком языке написан исходный текст и частотную характеристику употребления символов алфавита этого языка, криптоаналитик путем статистической обработки перехваченных сообщений может установить соответствие между символами обоих алфавитов.

Методы полиалфавитной замены

Существенно более стойкими являются методы полиалфавитной замены. Такие методы основаны на использовании нескольких алфавитов для замены символов исходного текста. Формально полиалфавитную замену можно представить следующим образом. При N – алфавитной замене символ S_{01} из исходного алфавита A_0 заменяется символом s_{11} из алфавита A_1, S_{02} заменяется символом S_{22} из алфавита A_2 и так далее. После замены S_{0N} символом S_{NN} из A_N символ $S_{0(N+1)}$ замещается символом $S_{1(N+1)}$ из алфавита A_1 и так далее.

Наибольшее распространение получил алгоритм полиалфавитной замены с использованием таблицы (матрицы) Вижинера ТВ, которая представляет собой квадратную матрицу [RxR], где R – количество символов в используемом алфавите. В первой строке располагаются символы в алфавитном порядке. Начиная со второй строки, символы записываются со сдвигом влево на одну позицию. Выталкиваемые символы заполняют освобождающиеся позиции справа (циклический сдвиг). Если используется русский алфавит, то матрица Вижинера имеет размерность [32 × 32].

$$T_B = \begin{vmatrix} А & Б & В & Г & Д & \dots & Ъ & Э & Ю & Я & \_ \\ Б & В & Г & Д & Е & \dots & Э & Ю & Я & \_ & А \\ В & Г & Д & Е & Ж & \dots & Ю & Я & \_ & А & Б \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \_ & А & Б & В & Г & \dots & Ы & Ъ & Э & Ю & Я \end{vmatrix}$$

Шифрование осуществляется с помощью ключа, состоящего из M неповторяющихся символов. Из полной матрицы Вижинера выделяется матрица шифрования $T_Ш$, размерностью $[(M+1), R]$. Она включает первую строку и строки, первые элементы которых совпадают с символами ключа. Если в качестве ключа выбрано слово <ЗОНД>, то матрица шифрования содержит пять строк:

$$T_Ш = \begin{vmatrix} АБВГДЕЖЗИКЛМНООПРСТУФХЦЧШЩЪЫЬЭЮЯ\_ \\ ЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ\_АБВГДЕЖ \\ ОПРСТУФХЦЧШЩЪЫЬЭЮЯ\_АБВГДЕЖЗИКЛМН \\ НОПРСТУФХЦЧШЩЪЫЬЭЮЯ\_АБВГДЕЖЗИКЛМ \\ ДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ\_АБВГ \end{vmatrix}$$

Алгоритм зашифрования с помощью таблицы Вижинера представляет собой следующую последовательность шагов.

Шаг 1

Выбор ключа K длиной M символов.

Шаг 2

Построение матрицы шифрования $T_Ш=(b_{ij})$ размерностью $[(M+1), R]$ для выбранного ключа K.

Шаг 3

Под каждым символом S_{0r} исходного текста длиной I символов размещается символ ключа k_m. Ключ повторяется необходимое число раз.

Шаг 4

Символы исходного текста последовательно замещаются символами, выбираемыми из $T_Ш$ по следующему правилу:

1. определяется символ k_m ключа K, соответствующий замещаемому символу S_{0r};
2. находится строка i в T_i, для которой выполняется условие $k_m=b_{i1}$;
3. определяется столбец j, для которого выполняется условие: $S_{0r}=b_{1j}$;
4. символ S_{0r} замещается символом b_{ij}.

Шаг 5

Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, служебными символами до полного объема.

Расшифрование осуществляется в следующей последовательности:

Шаг 1

Под шифртекстом записывается последовательность символов ключа по аналогии с шагом 3 алгоритма зашифрования.

Шаг 2

Последовательно выбираются символы S_{1r} из шифртекста и соответствующие символы ключа k_m. В матрице $T_ш$ определяется строка i, для которой выполняется условие $k_m = b_{i1}$. В строке 1 определяется элемент $b_{ij} = S_{1r}$. В расшифрованный текст на позицию r помещается символ b_{1j}.

Шаг 3

Расшифрованный текст записывается без разделения на блоки. Убираются служебные символы.

Пример:

Требуется с помощью ключа K = <ЗОНД> зашифровать исходный текст T = <БЕЗОБЛАЧНОЕ_НЕБО>.

Механизмы зашифрования и расшифрования представлены в таблицу 7.4.

Таблица 7.4 – Пример шифрования с помощью матрицы Вижинера

Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО
Ключ	ЗОНДЗОНДЗОНДЗОНД
Текст после замены	ИУФТИШНЫФЫТГФУОТ
Шифртекст	ИУФТ ИШНЫ ФЫТГ ФУОТ
Ключ	ЗОНД ЗОНД ЗОНД ЗОНД
Расшифрованный текст	БЕЗО БЛАЧ НОЕ_ НЕБО
Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО

Криптостойкость методов полиалфавитной замены значительно выше методов простой замены, так как одни и те же символы исходной последовательности могут заменяться разными символами. Однако стойкость шифра к статистическим методам криптоанализа зависит от длины ключа.

Для повышения криптостойкости может использоваться модифицированная матрица шифрования. Она представляет собой матрицу размерности [11, R], где R – число символов алфавита. В первой строке располагаются символы в алфавитном порядке. Остальные 10 строк нумеруются от 0 до 9. В этих строках символы располагаются случайным образом.

В качестве ключей используются, например, непериодические бесконечные числа π, e и другие. Очередной n-й символ исходного текста заменяется соответствующим символом из строки матрицы шифрования, номер которой совпадает с n-й цифрой бесконечного числа.

7.4. Методы перестановки

Другой разновидностью используемых с давних времен шифров являются так называемые шифры перестановки. Суть их в том, что буквы исходного сообщения остаются прежними, но их порядок меняется по какому-либо "хитрому" закону.

Табличная перестановка

Простейший вариант перестановки – прямоугольная таблица с секретным размером столбца (см. таблицу 7.5), куда исходный текст записывается по столбцам, а шифрсообщение считывается по строкам.

Таблица 7.5 – Шифр табличной перестановки

П	л	к	з	ч	и
о	а	Г	р	а	#
с	ю	-	ы	т	#
ы	-	В	в	к	#

Открытый текст: Посылаю _ кг _ взрывчатки###.
Шифрсообщение: Плкзчиоагра#сю_ыт#ы_ввк#.
‘#’ – произвольные символы.

Для расшифрования надо длину сообщения разделить на длину столбца, чтобы определить длину строки, вписать шифрсообщение в таблицу по строкам, а затем прочитать открытый текст.

Кодирование перестановкой по группам символов

Другой вариант – кодирование перестановкой по группам символов, используя некоторые зигзагообразные шаблоны, например, как показано на рисунке 7.4. Стоит записать:

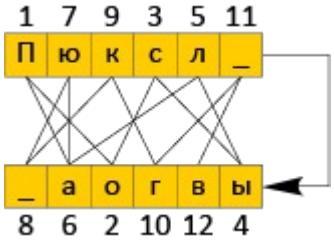


Рисунок 7.4 – Зигзагообразный шифр перестановки

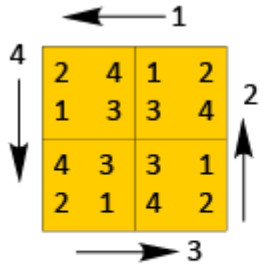
Открытый текст: Посылаю_кг_взрывчатки###
Шифрсообщение: Пюксл_ывгоа_ зтиыч#в##рак
‘#’- произвольные символы.

Символы открытого текста по зигзагу, а прочитать по кругу (или наоборот) – и шифрсообщение готово, если кажется ненадежным, то можно ввести дополнительные усложнения.

Ручные системы

Использовались и более сложные (ручные) системы, также групповые. Например, в квадрате (см. рисунок 7.5), состоящем из 4 малых квадратов с определенной нумерацией клеток, вырезают 4 клетки под разными номерами. Квадрат кладется в начальное положение ("1" – вверху) и в отверстия (слева направо/сверху вниз) вписываются буквы открытого сообщения. Затем квадрат поворачивается против часовой стрелки на 90 градусов ("2" – вверху) и также вписываются следующие буквы, потом повторяем процесс для положения "3" и "4". Если остаются свободные клетки – они заполняются произвольными

символами. Шифрсообщение получают, считав по столбцам или по строкам последовательность записанных в прямоугольнике букв.



1	2	3	4
П О		П о	л	П о г	К Л	з о П г	р л к ы
ы	с	а ы ю	с _	А ы ю	С в _	а ы в ю	С В _ _

Посылаю_кг_взрывчатки
ЗоаыПгвюрлсвкы ...
группа_1 группа_2

Рисунок 7.5 – Шифровальный квадрат

Фактически, рассмотренные выше и другие шифры перестановки с современной точки зрения абсолютно единообразны, так как представляют собой последовательность элементарных процедур перестановки группы символов вида (см. рисунок 7.6):

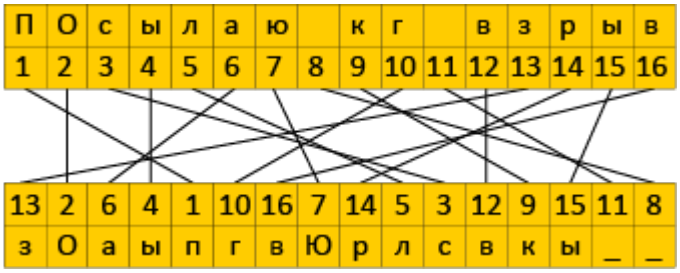


Рисунок 7.6 – Перестановки

Дешифровка сообщений, полученных шифром перестановки, значительно труднее, чем при использовании шифров замены. Какой-либо теоретической предпосылки, кроме перебора вариантов, не существует, хотя отдельные догадки могут упростить задачу.

Суть методов перестановки заключается в разделении исходного текста на блоки фиксированной длины и последующей перестановке символов внутри каждого блока по определенному алгоритму.

Перестановки получаются за счет разницы путей записи исходной информации и путей считывания зашифрованной информации в пределах геометрической фигуры. Примером простейшей перестановки является запись блока исходной информации в матрицу по строкам, а считывание – по столбцам.

Последовательность заполнения строк матрицы и считывания зашифрованной информации по столбцам может задаваться ключом. Криптостойкость метода зависит от длины блока (размерности матрицы). Так для блока длиной 64 символа (размерность матрицы 8 × 8) возможны 1,6 × 109 комбинаций ключа. Для блока длиной 256 символов (матрица размерностью 16 × 16) число возможных ключей достигает 1,4 × 1026. Решение задачи перебора ключей в последнем случае даже для современных ЭВМ представляет существенную сложность.

Перестановки используются также в методе, основанном на применении маршрутов Гамильтона. Этот метод реализуется путем выполнения следующих шагов.

Шаг 1

Исходная информация разбивается на блоки. Если длина шифруемой информации не кратна длине блока, то на свободные места последнего блока помещаются специальные служебные символы-заполнители (например *).

Шаг 2

Символами блока заполняется таблица, в которой для каждого порядкового номера символа в блоке отводится вполне определенное место (см. рисунок 7.7).

Шаг 3

Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает Криптостойкость шифра. Маршруты выбираются либо последовательно, либо их очередность задается ключом К.

Шаг 4

Зашифрованная последовательность символов разбивается на блоки фиксированной длины L. Величина L может отличаться от длины блоков, на которые разбивается исходная информация на шаге 1.

Расшифрование производится в обратном порядке. В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту.

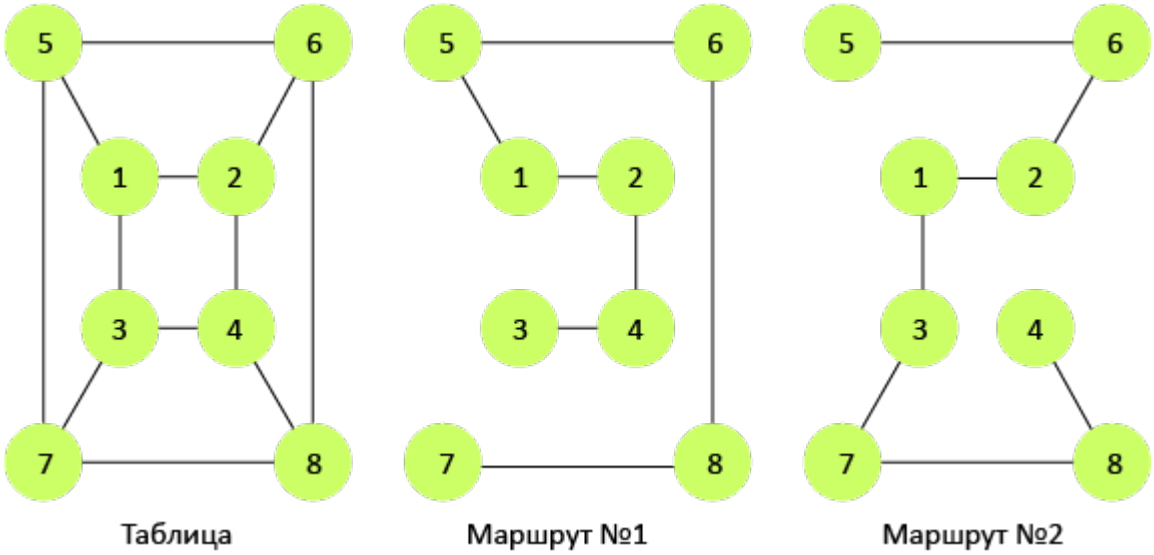


Рисунок 7.7 – Вариант 8-элементной таблицы и маршрутов Гамильтона

Из таблицы символы считываются в порядке следования номеров элементов. Ниже приводится пример шифрования информации с использованием маршрутов Гамильтона.

Пусть требуется зашифровать исходный текст T_0 = <МЕТОДЫ_ПЕРЕСТАНОВКИ>. Ключ и длина зашифрованных блоков соответственно равны: К = <2, 1, 1>, L = 4. Для шифрования используются таблица и два маршрута, представленные на рисунке 7.7.

Для заданных условий маршруты с заполненными матрицами имеют вид, показанный на рисунке 7.8.

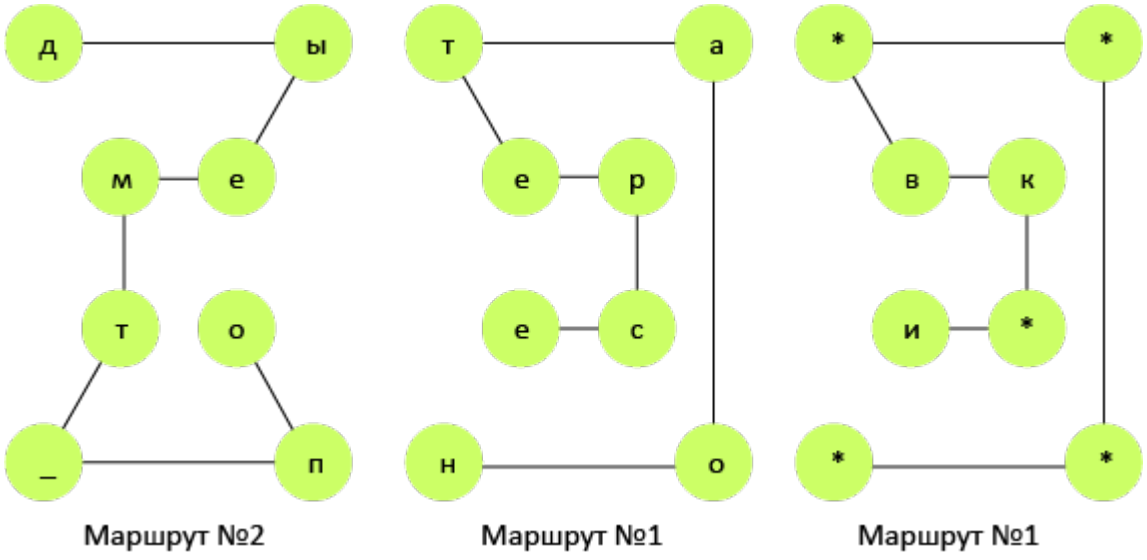


Рисунок 7.8 – Пример шифрования с помощью маршрутов Гамильтона

Шаг 1

Исходный текст разбивается на три блока:

$Б_1$ = <МЕТОДЫ_П>;

$Б_2$ = <ЕРЕСТАНО>;

$Б_3$ = <ВКИ*****>.

Шаг 2

Заполняются три матрицы с маршрутами 2, 1, 1 (см. рисунок 7.8).

Шаг 3

Получение шифртекста путем расстановки символов в соответствии с маршрутами.

T_1 = <ОП_ТМЕЫДЕСРЕТАОНИ*КВ****>.

Шаг 4

Разбиение на блоки шифртекста.

T_1 = <ОП_Т МЕЫД ЕСРЕ ТАОН И*КВ ****>.

В практике большое значение имеет использование специальных аппаратных схем, реализующих метод перестановок (см. рисунок 7.9).

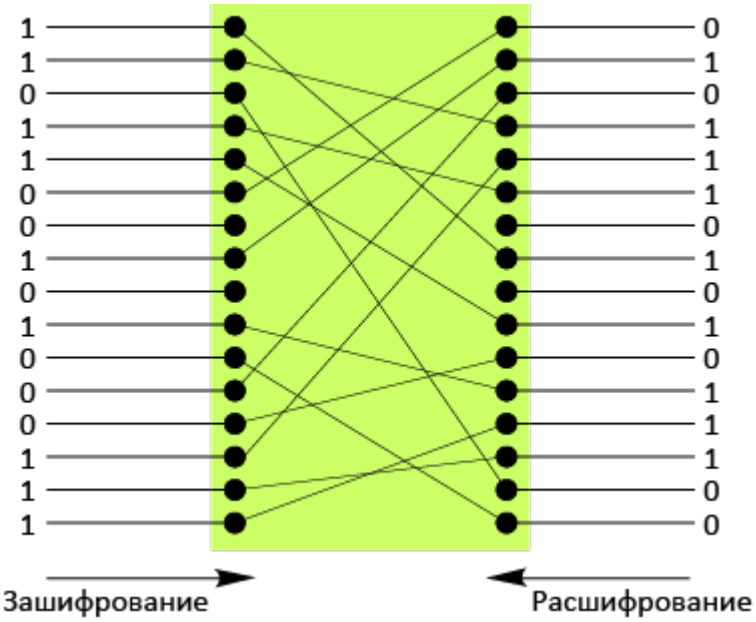


Рисунок 7.9 – Схема перестановок

Современные блочные шифры

Современные криптосистемы ориентированы на программно-аппаратные методы реализации. Блочные криптосистемы представляют собой блочные (групповые) шифрпреобразования. Блочная криптосистема разбивает открытый текст M на последовательные блоки M_1, M_2,... и зашифровывает каждый блок с помощью одного и того же обратимого преобразования E_k, выполненного с помощью ключа K. $E_k(M)=E_k(M_1)$, $E_k(M_2)$,…. Любое из них можно рассматривать как последовательность операций, проводимых с элементами ключа и открытого текста, а так же производными от них величинами. Произвол в выборе элементов алгоритма шифрования достаточно велик, однако "элементарные" операции должны обладать хорошим криптографическими свойствами и допускать удобную техническую или программную реализацию. Обычно используются операции:

- побитового сложения по модулю 2 (обозначение операции $\oplus$) двоичных векторов (XOR):
  $0 \oplus 0 = 0$
  $0 \oplus 1 = 1$
  $1 \oplus 1 = 0$
- сложение целых чисел по определенному модулю:
  например, по модулю 2^{32}, обозначение операции – [+]
  $a[+]b = a+b$, если $a+b < 2^{32}$,
  $a[+]b = a+b-2^{32}$, если $a+b \geq 2^{32}$
  где + – сложение целых чисел;
- умножение целых чисел по определенному модулю:
  ab(mod n) = res(ab/n) – остаток от деления произведения целых чисел *ab* на *n*;
- перестановка битов двоичных векторов;
- табличная замена элементов двоичных векторов.

Практическая стойкость алгоритмов шифрования зависит и от особенностей соединения операций в последовательности. Примерами блочных систем являются алгоритмы блочного шифрования, принятые в качестве стандартов шифрования данных в США и России – DES–алгоритм и ГОСТ 28147-89 соответственно.

DES-алгоритм

В 1973 году Национальное Бюро Стандартов США начало работы по созданию стандарта шифрования данных на ЭВМ. Был объявлен конкурс, который выиграла фирма IBM, представившая алгоритм шифрования, сейчас известный как DES-алгоритм (Data Encryption Standard.

Рассмотрим работу DES-алгоритма в простейшем (базовом) режиме ECB – электронной кодовой книги. Алгоритм работы показан на рисунке 7.10.

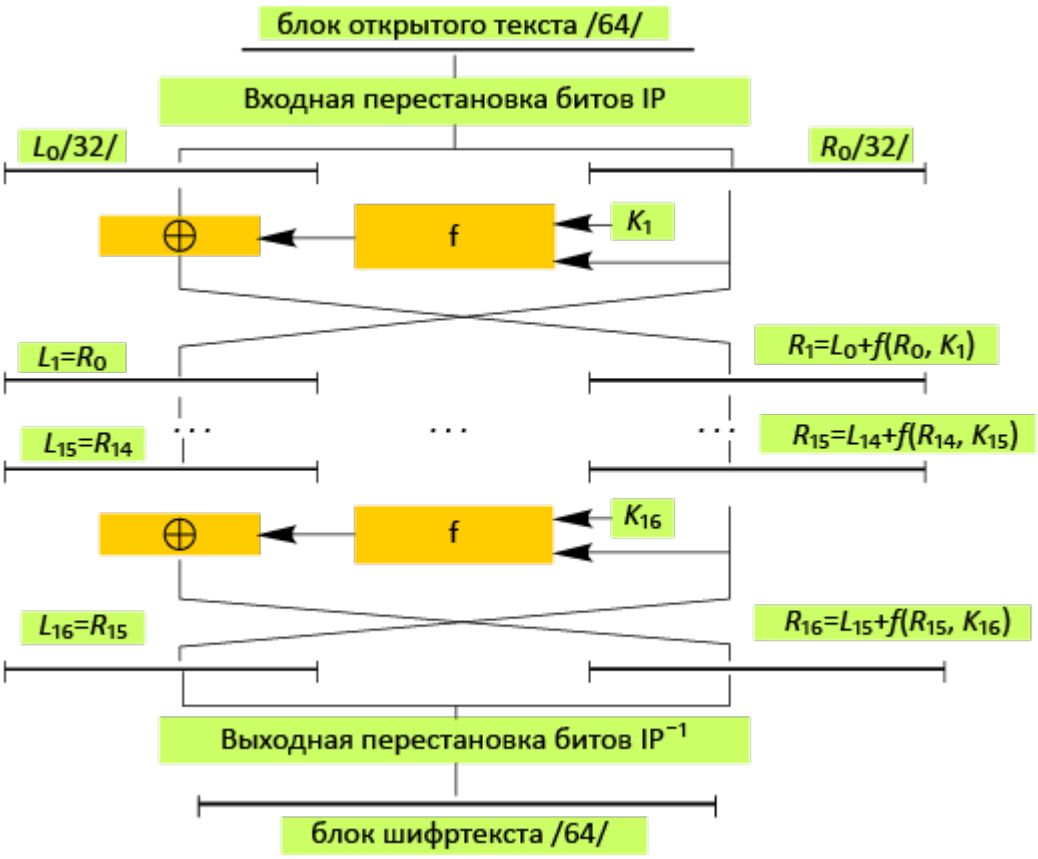


Рисунок 7.10 – Блок-схема DES-алгоритма

Входные 64-битовые векторы, называемые блоками открытого текста, преобразуются в выходные 64-битовые векторы, называемые блоками шифртекста, с помощью 56-битового ключа К (число различных ключей равно $2^{56}=7*10^6$)

Алгоритм реализуется в 16 аналогичных циклах шифрования, где в i-ом цикле используется цикловой ключ K_i, предоставляющий собой выборку 48 битов из 56 битов ключа К. Реализация алгоритма функции f показана на рисунке 7.11. Здесь операция Е – расширение 32-битового вектора до 48-битового, операция S_j (S-боксы) – замена 6-битовых векторов на 4 – битовые.

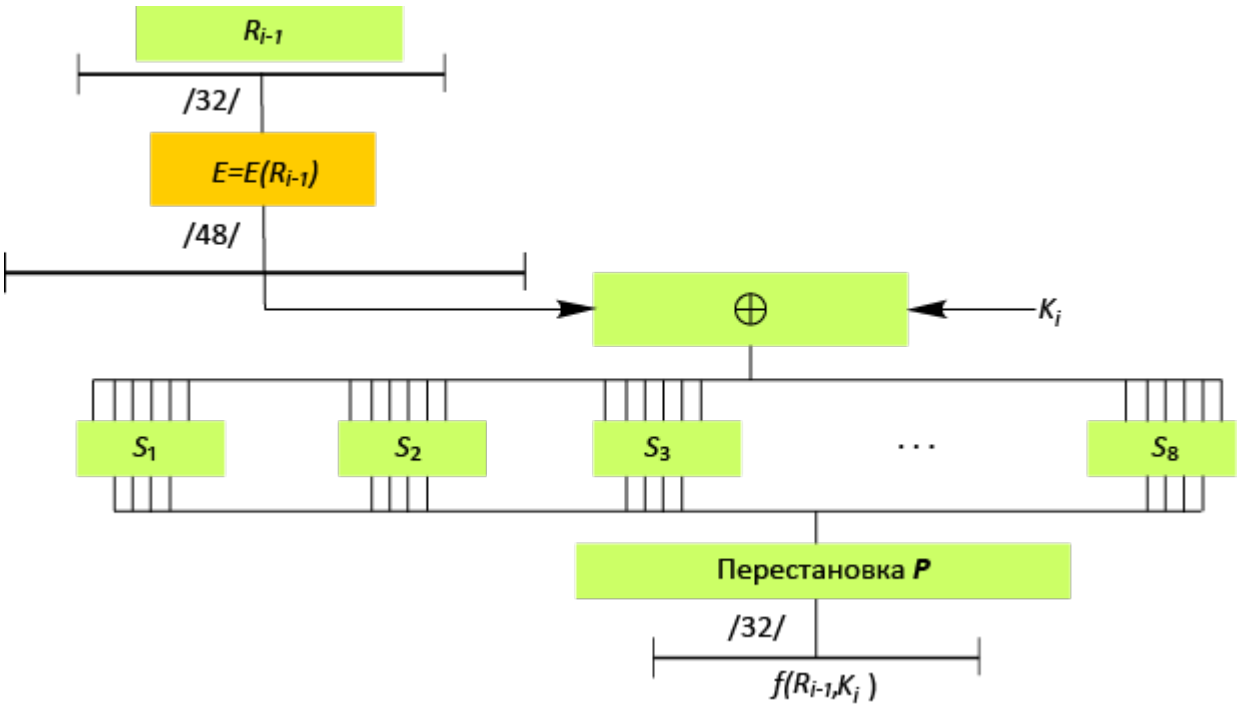


Рисунок 7.11 – Блок-схема функции f DES-алгоритма

Основным недостатком алгоритма считается 56-битовый ключ, слишком короткий для противостояния полному перебору ключей на специализированном компьютере. Недавние результаты показали, что современное устройство стоимостью 1 млн. долл. способно вскрыть секретный ключ с помощью полного перебора в среднем за 3.5 часа. Поэтому было принято решение использовать DES-алгоритм для закрытия коммерческой (несекретной) информации. В этих случаях практическая реализация перебора всех ключей экономически нецелесообразна, так как затраты не соответствуют ценности зашифрованной информации.

В ходе открытого обсуждения алгоритма в прессе, рассматривались пути усиления его криптографических свойств. Наиболее простой вариант предполагал использовать независимые 48-битовые векторы в качестве цифровых ключей, что позволит увеличить общее число ключей до 2^{768}.

Режим электронной кодовой книги (ECB) используется в основном для шифрования коротких сообщений служебного содержания – паролей, ключей и т.п. Наиболее общий режим – режим сцепления блоков (CBC), (Cifer Block Chaining) схема которого показана на рисунке 7.12. Здесь каждый входной блок зависит от всех предыдущих. Начальный вектор bo (случайный начальный вектор) вырабатывается для каждого сообщения и может передаваться в линию связи, как в открытом, так и в шифрованном виде, что препятствует атакам на шифротекст, основанным на наличии стандартов в начале сообщения (вспомните "Семнадцать мгновений весны": Центр – Юстасу...).

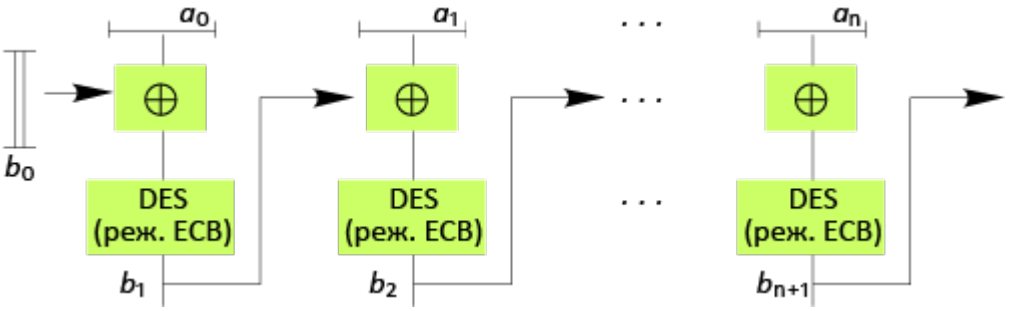


Рисунок 7.12 – Реализация DES-алгоритма в режиме сцепления блоков

DES алгоритм является первым примером широкого производства и внедрения технических средств в область защиты информации. К настоящему времени выпускается несколько десятков устройств аппаратно – программной реализации DES-алгоритма. Для выпуска такого рода устройства необходимо получить сертификат Национального Бюро Стандартов на право реализации продукта, который выдается только после всесторонней проверки по специальным тестирующим процедурам.

Достигнута высокая скорость шифрования. По некоторым сообщениям, в одном из устройств на основе специализированной микросхемы она составляет около 45 Мбит/сек.

Основные области применения DES-алгоритма:

- хранение данных в ЭВМ (шифрование файлов, паролей);
- электронная система платежей (между клиентом и банком);
- электронный обмен коммерческой информацией (между покупателем и продавцом).

Российский стандарт шифрования

В 1989 году был разработан блочный шифр для использования в качестве государственного стандарта шифрования (зарегистрирован как ГОСТ 28147-89). В основном алгоритм применяется в банковской системе, судя по публикациям – несколько медлителен, но обладает весьма высокой стойкостью.

Его общая схема близка к схеме DES-алгоритма, лишь отсутствует начальная перестановка и число циклов шифрования равно 32 (вместо 16 в DES-алгоритме). Ключом считается набор из 8 элементарных 32-битовых ключей X_1, X_2, ..., X_8 (общее число ключей 2^{256}). В циклах шифрования трижды используется прямая последовательность элементарных ключей и один раз – обратная: X_8, X_7,..., X_1.

Основное отличие – в реализации функции f стандарта шифрования (см. рисунок 7.13). Элементы S_1, S_2, ..., S_8 – представляют собой таблицы замены 4-битовых векторов и могут рассматриваться как долговременные ключи

ГОСТ 28147-89, как DES-алгоритм, предусматривает различные режимы использования и только базовый (режим простой замены) совпадает, по сути, с

базовым режимом DES-алгоритма, остальные – в той или иной мере отличаются.

Известна специальная реализация алгоритма шифрования ГОСТ 28147-89 аппаратная плата шифрования данных "Криптон-3" для IBM PC, ее производительность – 50 Кбит/сек.

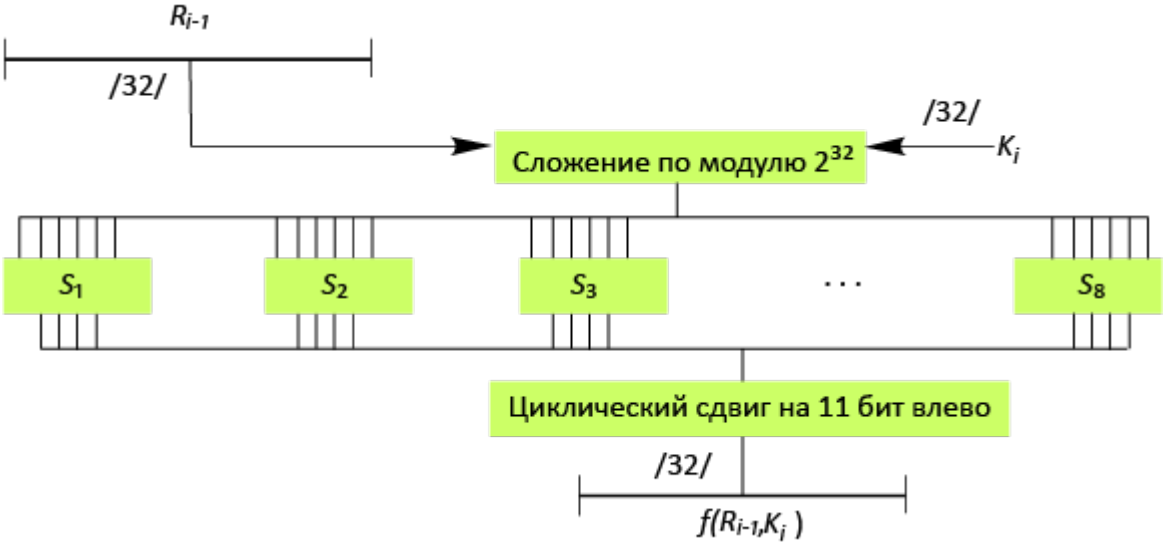


Рисунок 7.13 – Блок-схема функции f алгоритма ГОСТ 28147-89

7.5. Аналитические методы шифрования

Для шифрования информации могут использоваться аналитические преобразования. Наибольшее распространение получили методы шифрования, основанные на использовании матричной алгебры. Зашифрование k-го блока исходной информации, представленного в виде вектора $B_k = ||b_j||$, осуществляется путем перемножения матрицы-ключа $A = ||a_{ij}||$ и вектора B_k. В результате перемножения получается блок шифртекста в виде вектора $C_k = ||c_i||$, где элементы вектора C_k определяются по формуле:

$$C_i = \sum_j a_{ij} b_j$$

Расшифрование информации осуществляется путем последовательного перемножения векторов C_k и матрицы A^{-1}, обратной матрице A.

Пример шифрования информации с использованием алгебры матриц.

Пусть необходимо зашифровать и расшифровать слово T^0 = < ЗАБАВА> с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}.$$

Для зашифрования исходного слова необходимо выполнить следующие шаги.

Шаг 1

Определяется числовой эквивалент исходного слова как последовательность соответствующих порядковых номеров букв слов $T_э$: $T_э$ = <8, 1, 2, 1, 3, 1> .

Шаг 2

Умножение матрицы A на векторы B_1 = {8, 1, 2} и B_2 = {1, 3, 1}:

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \bullet \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix} = \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix}; \quad C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \bullet \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix} = \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix}.$$

Шаг 3

Зашифрованное слово записывается в виде последовательности чисел B^1 = <28, 35, 67, 21, 26, 38>.

Расшифрование слова осуществляется следующим образом.

Шаг 1

Вычисляется определитель $|A|$ = -115.

Шаг 2

Определяется присоединенная матрица A*, каждый элемент которой является алгебраическим дополнением элемента матрицы А:

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}.$$

Шаг 3

Получается транспонированная матрица A^T:

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}.$$

Шаг 4

Вычисляется обратная матрица A^{-1} по формуле:

$$A^{-1} = A^T / |A|.$$

В результате вычислений обратная матрица имеет вид:

$$A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}.$$

Шаг 5

Определяются векторы B_1 и B_2:

$$B_1 = A^{-1} * C_1; \quad B_2 = A^{-1} * C_2;$$

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \bullet \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix} = \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix}; \quad B_2 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \bullet \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix} = \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix}$$

Шаг 6

Числовой эквивалент расшифрованного слова $T_э$ = <8, 1, 2, 1, 3, 1> заменяется символами, в результате чего получается исходное слово T_0 = <ЗАБАВА>.

7.6. Аддитивные методы шифрования

Сущность аддитивных методов шифрования заключается в последовательном суммировании цифровых кодов, соответствующих символам исходной информации, с последовательностью кодов, которая соответствует некоторому кортежу символов. Этот кортеж называется гаммой. Поэтому аддитивные методы шифрования называют также гаммированием.

Для данных методов шифрования ключом является гамма. Криптостойкость аддитивных методов зависит от длины ключа и равномерности его статистических характеристик. Если ключ короче, чем шифруемая последовательность символов, то шифртекст может быть расшифрован криптоаналитиком статистическими методами исследования. Чем больше разница длин ключа и исходной информации, тем выше вероятность успешной атаки на шифртекст. Если ключ представляет собой непериодическую последовательность случайных чисел, длина которой превышает длину шифруемой информации, то без знания ключа расшифровать шифртекст практически невозможно. Как и для методов замены в качестве ключа могут использоваться неповторяющиеся последовательности цифр, например, в числах π, e и других.

На практике самыми эффективными и распространенными являются аддитивные методы, в основу которых положено использование генераторов (датчиков) псевдослучайных чисел. Генератор использует исходную информацию относительно малой длины для получения практически бесконечной последовательности псевдослучайных чисел.

Для получения последовательности псевдослучайных чисел (ПСЧ) могут использоваться конгруэнтные генераторы. Генераторы этого класса вырабатывают псевдослучайные последовательности чисел, для которых могут быть строго математически определены такие основные характеристики генераторов как периодичность и случайность выходных последовательностей.

Среди конгруэнтных генераторов ПСЧ выделяется своей простотой и эффективностью линейный генератор, вырабатывающий псевдослучайную последовательность чисел T(i) в соответствии с соотношением

$$T(i+1) = (a * T(i) + c) \bmod m,$$

где a и c – константы, T(0) – исходная величина, выбранная в качестве порождающего числа.

Период повторения такого датчика ПСЧ зависит от величин a и c. Значение m обычно принимается равным 2^s, где s – длина слова ЭВМ в битах. Период повторения последовательности генерируемых чисел будет максимальным тогда и только тогда, когда c – нечетное число и a (mod 4) = 1. Такой генератор может быть сравнительно легко создан как аппаратными средствами, так и программно.

Шифр гаммирования

Здесь уделяется внимание получению из ключа программно длинных случайных или псевдо-случайных рядов чисел, называемых на жаргоне отечественных криптографов гаммой, по названию γ- буквы греческого алфавита, которой в математических записях обозначаются случайные величины.

Эти программы, хотя они и называются генераторами случайных чисел, на самом деле выдают детерминированные числовые ряды, которые только кажутся случайными по своим свойствам. От них требуется, чтобы, даже зная закон формирования, но не зная ключа в виде начальных условий, никто не смог бы отличить числовой ряд от случайного.

Можно сформулировать 3 основных требования к криптографически стойкому генератору псевдослучайной последовательности или гаммы:

1. Период гаммы должен быть достаточно большим для шифрования сообщений различной длины.
2. Гамма должна быть труднопредсказуемой. Это значит, что если известны тип генератора и кусок гаммы, то невозможно предсказать следующий за этим куском бит гаммы с вероятностью выше заданной.
3. Генерирование гаммы не должно быть связано с большими техническими и организационными трудностями.

Режим гаммирования ГОСТ 28147-89

Схема реализации режима гаммирования приведена на рисунке 7.14.

Открытые данные, разбитые на 64-разрядные блоки $T_0^{(i)}$ зашифровываются в режиме гаммирования путем поразрядного суммирования по модулю 2 в сумматоре $СМ_5$ с гаммой шифра $Г_Ш^{(i)}$, которая вырабатывается блоками по 64 бита. Число двоичных разрядов в блоке $T_0^{(M)}$, где M определяется объемом шифруемых даных может быть меньше 64, при этом неиспользованная для зашифрования часть гаммы шифра из блока $Г_Ш^{(M)}$ отбрасывается.

В КЗУ вводятся 256 бит ключа. В накопители N_1, N_2 вводится 64-разрядная двоичная последовательность (синхропосылка) $S=(S_1,S_2,...,S_{64})$, являющаяся

исходным заполнением этих накопителей для последующей выработки M блоков гаммы шифра. Синхропосылка вводится в N_1 и N_2 так, что значение S_1 вводится в 1-ый разряд N_1, значение S_{33} – в 1-ый разряд N_2, S_{64} – в 32-й разряд N_2.

Исходное заполнение накопителей N_1 и N_2 (синхропосылка S) зашифровывается в режиме простой замены (нижняя часть рисунка). Результат зашифрования $A(S)=(Y_0, Z_0)$ переписывается в 32-разрядные накопители N_3 и N_4 так, что заполнение N_1 переписывается в N_3, а N_2 - в N_4.

Заполнение накопителя N_4 суммируется по модулю $(2^{32}-1)$ в сумматоре $СМ_4$ с 32-разрядной константой C_1 из накопителя N_6, результат записывается в N_4.

Заполнение накопителя N_3 суммируется по модулю 2^{32} в сумматоре $СМ_3$ с 32-разрядной константой C_2 из накопителя N_5, результат записывается в N_3.

Заполнение N_3 переписывается в N_1, а заполнение N_4 – в N_2. При этом заполнение N_3, N_4 сохраняется.

Заполнение N_1 и N_2 зашифровывается в режиме простой замены. Полученное в результате в N_1, N_2 зашифрование образует первый 64-рарядный блок гаммы шифра $Г_ш^{(1)}$, который суммируется в $СМ_5$ с первым 64- разрядным блоком открытых данных $T_0^{(1)}$.

В результате получается 64-разрядный блок зашифрования данных $Г_ш^{(1)}$.

Для получения следующего 64-разрядного блока гаммы шифра $Г_ш^{(2)}$ заполнение N_4 суммируется по модулю $(2^{32}-1)$ в $СМ_4$. С константой C_1 из N_6, заполнение N_3 суммируется по модулю 2^{32} в сумматоре $СМ_3$ с C_2 (в N_5). Новое заполнение N_3 переписывается в N_1, а новое заполнение N_4 переписывается в N_2., при этом заполнение N_3, N_4 сохраняется.

Заполнение N_1 и N_2 зашифровывается в режиме простой замены. Полученное в результате зашифрования заполнение N_1, N_2 образует второй 64-разрядный блок гаммы шифра $Г_ш^{(2)}$, который поразрядно суммируется по модулю 2 в $СМ_5$ со вторым блоком открытых данных $T_0^{(2)}$.

Аналогично вырабатываются блоки гаммы шифра $Г_ш^{(3)}$, ... , $Г_ш^{(M)}$ и зашифровываются блоки открытых данных $Г_0^{(3)}$, ..., $Г_0^{(M)}$.

В канал связи (или память ЭВМ) передается синхропосылка S и блоки зашифрованных данных $T_ш^{(1)}$, $T_ш^{(2)}$, ..., $T_ш^{(M)}$.

Уравнение зашифрования имеет вид:

$$T_ш^{(i)} = A\left(Y_{i-1}[+]C_2,\ Z_{i-1}[+]C_1\right) \oplus T_0^{(i)} = Г_ш^{(i)} \oplus T_0^{(i)},$$

где [+] – суммирование по модулю 2^{32},
[+]’ – суммирование по модулю 2^{32}-1,
$\oplus$ – суммирование по модулю 2,
Y_i – содержимое накопителя N_3 после зашифрования i-го блока открытых данных $T0^{(i)}$;
Z_i – содержимое накопителя N_4 после зашифрования i-го блока открытых данных $T0^{(i)}$.

$(Y_0, Z_0) = A(S)$

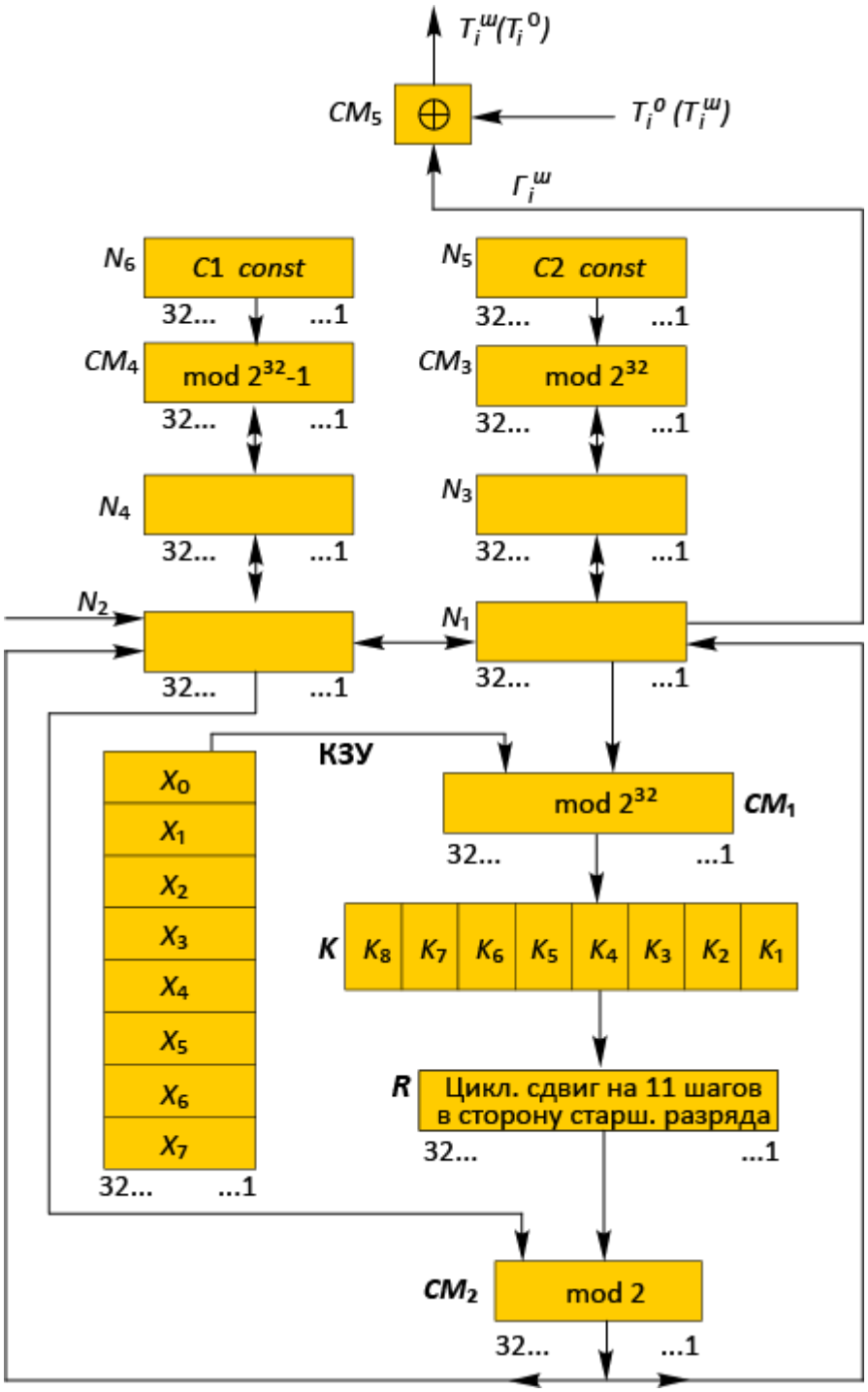


Рисунок 7.14 – Режим гаммирования ГОСТ 28147-89

Открытое распределение ключей. Схема Диффи-Хеллмана

Важной составной частью шифрсистемы является ключевая система шифра. Под ней понимается описание всех видов ключей (долговременных, суточных, сеансовых и других) и алгоритмов их использования.

Одной из основных характеристик ключа является его размер, определяющий число всевозможных ключевых установок шифра. Если размер ключа чрезмерно велик, то это приводит к удорожанию изготовления ключей, усложнению процедуры установки ключа, понижению надежности работы шифрующего устройства.

Важнейшей частью практической работы с ключами является обеспечение секретности ключа. К основным мерам по защите ключей относятся следующие:

- ограничение круга лиц, допущенных к работе с ключами;
- регламентация рассылки, хранения и уничтожения ключей;
- регламентация порядка смены ключей;
- применение технических мер защиты ключевой информации от несанкционированного доступа.

Рассмотрим один из принципов распределения ключей (на основе односторонней функции), проработка которого имела весьма неожиданные последствия – была изобретена система шифрования с открытым ключом. Сначала небольшое отступление.

Понятие односторонней функции было введено в теоретическом исследовании о защите входа в вычислительные системы. Функция f(x) называется односторонней (one-way function), если для всех x из ее области определения легко вычислить $y=f(x)$, но нахождение по заданному Y_0 такого x_0, для которого $f(x_0)=y_0$, вычислительно неосуществимо, то есть требуется настолько огромный объем вычислений, что за них просто и не стоит браться.

Однако существование односторонних функций не доказано. В качестве приближения была предложена Гиллом Дж. целочисленная показательная функция $f(x)=a^x(mod\ n)$, где основание a и показатель степени x принадлежат интервалу (1, n-1), а умножение ведется по модулю n $(3*4 \bmod 10 = 2;\ 7*8 \bmod 9 = 2)$. Функция вычисляется достаточно эффективно по схеме Горнера. Если представление числа x в двоичной форме имеет вид:

$$x_{k-1}2^{k-1} + x_{k-2}2^{k-2} + \ldots + x_1 2^1 + x_0 2^0,$$

то

$$y = f(x) = a^x \bmod n = ((\ldots(a^{xk-1})^2 * a^{xk-2})^2 * \ldots * a^{x1})^2 * a^{x0} \bmod n.$$

Операция, обратная к этой, известна как операция вычисления дискретного логарифма: по заданным y, a и n найти такое целое x, что $a^x (\mathrm{mod} n) = y$. До настоящего времени не найдено достаточно эффективных алгоритмов решения этой задачи.

Американские криптологи Диффи и Хеллман (Diffi W., Hellman M.E. New direction in criptography. IEEE Trans. Inf. Theory, v. IT-22, 1976) предложили схему распространения (рассылки) ключей для секретной связи на основе односторонней показательной функции. Ее суть состоит в следующем.

В протоколе обмена секретными ключами предполагается, что все пользователи знают некоторые числа n и a (1< a < n). Для выработки общего секретного ключа пользователи *A* и *B* должны проделать следующую процедуру:

1. Определить секретные ключи пользователей *KA* и *KB*.
   Для этого каждый пользователь независимо выбирает случайные числа из интервала (1,..., n-1).
2. Вычислить открытые ключи пользователей *YA* и *YB*.
   Для этого каждый использует одностороннюю показательную функцию $Y=a^x \ mod \ n$ со своим секретным ключом.
3. Обменяться ключами *YA* и *YB* по открытому каналу связи.
4. Независимо определить общий секретный ключ K.

Для этого пользователи выполняют вычисления с помощью той же односторонней функции:

A: $Y_B{}^{KA} (\mathrm{mod} n) = \left[\mathbf{a}^{KB} \right]^{KA} \mathrm{mod} n = \mathbf{a}^{KA*KB} \mathrm{mod} n = K$.

B: $Y_A{}^{KB} (\mathrm{mod} n) = \left[\mathbf{a}^{KA} \right]^{KB} \mathrm{mod} n = \mathbf{a}^{KB*KA} \mathrm{mod} n = K$.

Здесь каждый имеет показатель степени, а основание получает от партнера.

Безопасность (секретность) изложенной схемы зависит от сложности вычисления секретных ключей пользователей (*KA* и *KB*). Пока не найдено удовлетворительных быстрых алгоритмов нахождения *K* из *a*, *YA* и *YB* без явного определения *KA* или *KB*.

7.7. Системы шифрования с открытым ключом

Наряду с традиционным шифрованием на основе секретного ключа в последние годы все большее признание получают системы шифрования с открытым ключом. В таких системах используются два ключа. Информация шифруется с помощью открытого ключа, а расшифровывается с использованием секретного ключа.

В основе применения систем с открытым ключом лежит использование необратимых или односторонних функций. Эти функции обладают следующим свойством. По известному x легко определяется функция y = f(x). Но по

известному значению y практически невозможно получить x. В криптографии используется односторонние функции, имеющие так называемый потайной ход. Эти функции с параметром z обладают следующими свойствами. Для определенного z могут быть найдены алгоритмы E_Z и D_Z. С помощью E_Z легко получить функцию $f_Z(x)$ для всех x из области определения. Так же просто с помощью алгоритма D_Z получается и обратная функция $x = f^{-1}(y)$ для всех y из области допустимых значений. В то же время практически для всех z и почти для всех y из области допустимых значений нахождение $f^{-1}(y)$ при помощи вычислений невозможно даже при известном E_Z. В качестве открытого ключа используется y, а в качестве закрытого – x.

При шифровании с использованием открытого ключа нет необходимости в передаче секретного ключа между взаимодействующими субъектами, что существенно упрощает криптозащиту передаваемой информации.

Криптосистемы с открытыми ключами различаются видом односторонних функций. Среди них самыми известными являются системы RSA, Эль-Гамаля и Мак-Элиса. В настоящее время наиболее эффективным и распространенным алгоритмом шифрования с открытым ключом является алгоритм RSA, получивший свое название от первых букв фамилий его создателей: Rivest, Shamir и Adleman.

Алгоритм основан на использовании операции возведения в степень модульной арифметики. Его можно представить в виде следующей последовательности шагов.

Шаг 1

Выбираются два больших простых числа p и q. Простыми называются числа, которые делятся только на самих себя и на 1. Величина этих чисел должна быть больше 200.

Шаг 2

Получается открытая компонента ключа n:

$$n = p * q$$

.

Шаг 3

Вычисляется функция Эйлера по формуле:

$$f(p,q) = (p-1)*(q-1)$$

.

Функция Эйлера показывает количество целых положительных чисел от 1 до n, которые взаимно просты с n. Взаимно простыми являются такие числа, которые не имеют ни одного общего делителя, кроме 1.

Шаг 4

Выбирается большое простое число d, которое является взаимно простым со значением f(p, q).

Шаг 5

Определяется число e, удовлетворяющее условию:

$e*d=1\left(\mathrm{mod}\, f\left(p,q\right)\right)$

Данное условие означает, что остаток от деления (вычет) произведения e*d на функцию f(p, q) равен 1. Число e принимается в качестве второй компоненты открытого ключа. В качестве секретного ключа используются числа p и q.

Шаг 6

Исходная информация, независимо от ее физической природы, представляется в числовом двоичном виде. Последовательность бит разделяется на блоки длиной L бит, где L – наименьшее целое число, удовлетворяющее условию: $L\geq log_2\left(n+1\right)$. Каждый блок рассматривается как целое положительное число X(i), принадлежащее интервалу [0, n-1]. Таким образом, исходная информация представляется последовательностью чисел $X\left(i\right),i=\overline{1,l}$. Значение I определяется длиной шифруемой последовательности.

Шаг 7

Зашифрованная информация получается в виде последовательности чисел Y(i), вычисляемых по формуле:

$Y\left(i\right)=\left(X\left(i\right)\right)^e\left(\mathrm{mod}\, n\right).$

Шаг 8

Для расшифрования информации используется следующая зависимость:

$X\left(i\right)=\left(Y\left(i\right)\right)^d\left(\mathrm{mod}\, n\right)$

Пример применения метода RSA для криптографического закрытия информации. Примечание: для простоты вычислений использованы минимально возможные числа.

Пусть требуется зашифровать сообщение на русском языке "ГАЗ".

Для зашифрования и расшифрования сообщения необходимо выполнить следующие шаги.

Шаг 1

Выбирается p = 3 и q = 11.

Шаг 2

Вычисляется n = 3 * 11 = 33.

Шаг 3

Определяется функция Эйлера:

$f\left(p,q\right)=\left(3-1\right)*\left(11-1\right)=20$

Шаг 4

В качестве взаимно простого числа выбирается число.

Шаг 5

Выбирается такое число e, которое удовлетворяло бы ношению: (e*3) (mod 20) = 1. Пусть e = 7.

Шаг 6

Исходное сообщение представляется как последовательность целых чисел. Пусть букве А соответствует число 1, букве Г – число 4, букве З – число 9. Для представления чисел в двоичном коде требуется 6 двоичных разрядов, так как в русском алфавите используются 33 буквы (случайное совпадение с числом n). Исходная информация в двоичном коде имеет вид:

000100 000001 001001.

Длина блока L определяется как минимальное число из целых чисел, удовлетворяющих условию: $L \geq log2(33+1)$, так как n=33. Отсюда L = 6. Тогда исходный текст представляется в виде кортежа X(i) = <4, 1, 9>.

Шаг 7

Кортеж X(i) зашифровывается с помощью открытого ключа {7, 33}:

$$Y(1) = \left(4^7\right)(\mathrm{mod}\ 33) = 16384(\mathrm{mod}\ 33) = 16;$$

$$Y(2) = \left(1^7\right)(\mathrm{mod}\ 33) = 1(\mathrm{mod}\ 33) = 1;$$

$$Y(3) = \left(9^7\right)(\mathrm{mod}33) = 4782969(\mathrm{mod}33) = 15.$$

Получено зашифрованное сообщение Y(i) = <16, 1, 15>.

Шаг 8

Расшифровка сообщения Y(i) = <16, 1, 15> осуществляется с помощью секретного ключа {3, 33}:

$$X(1) = \left(16^3\right)(\mathrm{mod}\ 33) = 4096(\mathrm{mod}\ 33) = 4;$$

$$X(2) = \left(1^3\right)(\mathrm{mod}\ 33) = 1(\mathrm{mod}\ 33) = 1;$$

$$X(3) = \left(15^3\right)(\mathrm{mod}33) = 3375(\mathrm{mod}33) = 9.$$

Исходная числовая последовательность в расшифрованном виде X(1) = <4, 1, 9> заменяется исходным текстом "ГАЗ".

Система Эль-Гамаля основана на сложности вычисления дискретных логарифмов в конечных полях. Основным недостатком систем RSA и Эль-Гамаля является необходимость выполнения трудоемких операций в модульной арифметике, что требует привлечения значительных вычислительных ресурсов.

7.8. Стандарты шифрования

Российский стандарт ГОСТ 28147-89

В Российской Федерации установлен государственный стандарт (ГОСТ 28147-89) на алгоритмы криптографического преобразования информации в ЭВМ, вычислительных комплексах и вычислительных сетях. Эти алгоритмы допускается использовать без ограничений для шифрования информации

любого уровня секретности. Алгоритмы могут быть реализованы аппаратными и программными способами.

Стандартом определены следующие алгоритмы криптографического преобразования информации:

- простая замена;
- гаммирование;
- гаммирование с обратной связью;
- выработка имитовставки.

Общим для всех алгоритмов шифрования является использование ключа размерностью 256 бит, разделенного на восемь 32-разрядных двоичных слов, и разделение исходной шифруемой двоичной последовательности на блоки по 64 бита.

Криптосистема RSA

Название криптосистемы образовано из первых букв фамилий предложивших ее авторов (Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and pablic-key cryptosystems. Commun. ACM, v.21, N2, 1978).

Система относится к блочным экспоненциальным системам, так как каждый блок M открытого текста рассматривается как целое число в интервале (0,..., n-1) и преобразуется в блок C следующим открытым преобразованием:

$$C = E(e,n)(M) = M^e \pmod{n},$$

где E(e,n) – преобразование, а (e,n) – ключ зашифрования.

При расшифровании блок открытого текста M восстанавливается таким же преобразованием, но с другим показателем степени.

$$M = D(d,n)(C) = C^d \pmod{n},$$

где D(d,n) – преобразование, а (d,n) – ключ расшифрования.

В основе этого метода лежит довольно сложное теоретическое обоснование. Числа e и d связаны с n определенной зависимостью и существуют рекомендации по выбору ключевых элементов на основе простых чисел. Если взять два простых числа p и g, определить $n = p \times q$, то можно определить пару чисел e и d, удовлетворяющих заданным условиям. Если сделать открытыми числа e и n, а ключ d (и обязательно p и g) держать в секрете – то предложенная система является RSA-криптосистемой открытого шифрования. Очевидно, ее стойкость определяется сложностью операции извлечения из C корня степени e по модулю n.

Рассмотрим основные этапы реализации алгоритма RSA.

1. Отправитель вычисляет $n = p \times q$ и M=(p-1)(q-1).
2. Затем он выбирает случайное целое число e, взаимно простое с M и вычисляетd, удовлетворяющее условию:

$ed = 1 (\mathrm{mod}\, M)$.

Напомним, что два числа являются взаимно простыми, если их HOD =1. Числа a и b имеют HOD d, если d делит и a и b и максимальный среди таких чисел.

3. После этого он публикует e и n как свой открытый ключ шифрования, сохраняя d, как закрытый (секретный) ключ.
4. Рассмотрим теперь числа e и d. Предположим, что мы знаем одно из них и знаем соотношение, которым они связаны. Мы могли бы легко вычислить второе число, однако мы не знаем чисел p и q. Следовательно можно одно из чисел подарить кому-нибудь вместе с n и попросить его посылать нам сообщения следующим образом.
5. Сообщение представить как векторы (блоки) длины l:
   $X = (x_1, x_2 \ldots, x_l)$
   $0 < x_i < M$
6. Каждое x_i возвести в степень e по mod n.
7. Прислать нам:
   $Y = \left(x_1^e (\mathrm{mod}\, n),\ x_2^e (\mathrm{mod}\, n), \ldots,\ x_l^e (\mathrm{mod}\, n)\right)$.

Обозначим $t = y_i = x_i^e (\mathrm{mod}\, n)$ и рассмотрим расшифрование полученной информации.

Для этого возведем полученное число t в степень второго числа пары – d:

$R = t^d (\mathrm{mod}\, n) = x^e (\mathrm{mod}\, n)^d (\mathrm{mod}\, n) = x^{ed} (\mathrm{mod}\, n)$.

В соответствие с п.2 соотношение ed=1(mod M), а это означает, что ed-1 делится нацело на (p-1)(q-1), т.е. ed=1+a(p-1)(q-1), где a – целое число.

Утверждается, что

$x^{ed} (\mathrm{mod}\, n) = x$.

Действительно,

$x^{ed} (\mathrm{mod}\, n) = x^{1+a(p-1)(q-1)} (\mathrm{mod}\, n)$.

Учитывая, что $x^{p-1} = 1 \mathrm{mod}\, p,\ x^{q-1} = 1 \mathrm{mod}\, q$ (эти соотношения доказываются как малая теорема Ферма) получим:

$x^{(p-1)(q-1)} = 1 (\mathrm{mod}\, pq)$

$x^{1+a(p-1)(g-1)} (\mathrm{mod}\, n) = x$, т.к.

$x^{a(p-1)(q-1)} = 1 (\mathrm{mod}\, pq)$, из-за того,

что $x^{(p-1)(q-1)} = 1 (\mathrm{mod}\, pq)$,

$x \mathrm{mod}\, n = x$, так как $x < M$.

Что и требовалось доказать.

Цифровая (электронная) подпись

Одним из основных применений криптосистем с открытым ключом является их использование при создании так называемой цифровой или электронной подписи (digital signature). Впервые идея цифровой подписи была высказана в работе Диффи и Хеллмана.

Один из вариантов изложения принципа электронной подписи выглядит так. Требуется, чтобы существовали взаимообратные преобразования E_k и D_k, для которых выполняется:

$$E_k\left[D_k(M)\right] = M,$$

для любого открытого текста M.

Тогда D_k считается секретным преобразованием, с помощью которого пользователь может зашифровать исходный текст $C=D_k(M)$ и послать это значение в качестве цифровой подписи к сообщению M другим пользователям, обладающим знанием открытого преобразования E_k. Очевидно, что определение D_k при знании E_k должно быть вычислительно неразрешимой задачей.

Система RSA широко используется в системе цифровой подписи, так как ее преобразования обладают всеми необходимыми свойствами. Использование цифровой подписи предполагает существование двух процедур: подписывания и проверки.

Процедура подписывания сообщения M – это возведение числа M в степень d по mod n:

$$S = M^d \pmod n.$$

Число S есть цифровая подпись, которую может выработать только владелец секретного ключа.

Процедура проверки подписи S, соответствующей сообщению M – это возведение числа S в целую степень e по mod n:

$$M' = S^e \pmod n.$$

Если M'= M, то сообщение M признается подписанным пользователем, который предоставил ранее открытый ключ e.

В реализации для сокращения времени подписывания и размера подписи, в качестве источника для подписи служит не само исходное сообщение M (произвольной длины), а некоторая производная от него (фиксированной длины). Для ее получения используется общеизвестная функция H, отображающая любое сообщение M в сообщение H(M) фиксированного малого размера, которое далее преобразуется в цифровую подпись. Функция H называется функцией хеширования (hash function), в простейшем случае это

может быть, например, функция вычисления контрольной суммы текста сообщения по модулю 2^{32}, размер приведенного для электронного подписывания сообщения тогда будет равен 32 двоичным разрядам (четырем байтам).

Стандарт США – DES

Государственным стандартом США на шифрование информации является стандарт DES (Data Encryption Standard). Алгоритм шифрования, положенный в основу стандарта, был разработан фирмой IBM. После проверки специалистами Агентства Национальной Безопасности США алгоритм получил статус государственного стандарта. Стандарт DES используется федеральными департаментами для закрытия информации в автоматизированных системах, за исключением некоторых видов информации, определенных специальными актами. Кроме того, этот стандарт шифрования широко используется негосударственными организациями не только в США, но и во всем мире.

В стандарте DES исходная информация разбивается на блоки по 64 бита в каждом и подвергается криптографическому преобразованию с использованием ключа, длиной 56 или 64 бита.

Блоки исходной информации подвергаются итерационной обработке с использованием операций перестановки и функции шифрования. Для вычисления функции шифрования предусматривается получение 48-битового ключа из 64-битового, расширение 32-битового кода до 48-битового, преобразование 6-битового кода в 4-битовый и перестановка бит в 32-битовой последовательности.

Процесс расшифрования является инверсным по отношению к процессу шифрования и выполняется с использованием того же ключа, что и при шифровании.

7.9. Сжатие информации

Сжатие сокращает объем пространства, требуемого для хранения файлов в ЭВМ, и количество времени, необходимого для передачи информации по каналу установленной ширины пропускания. Это есть форма кодирования. Другими целями кодирования являются поиск и исправление ошибок, а также шифрование. Процесс поиска и исправления ошибок противоположен сжатию – он увеличивает избыточность данных, когда их не нужно представлять в удобной для восприятия человеком форме. Удаляя из текста избыточность, сжатие способствует шифрованию, что затрудняет поиск шифра доступным для взломщика статистическим методом.

Рассмотрим обратимое сжатие или сжатие без наличия помех, где первоначальный текст может быть в точности восстановлен из сжатого состояния. Необратимое или ущербное сжатие используется для цифровой

записи аналоговых сигналов, таких как человеческая речь или рисунки. Обратимое сжатие особенно важно для текстов, записанных на естественных и на искусственных языках, поскольку в этом случае ошибки обычно недопустимы. Хотя первоочередной областью применения рассматриваемых методов есть сжатие текстов, что отражает и наша терминология, однако, эта техника может найти применение и в других случаях, включая обратимое кодирование последовательностей дискретных данных.

Сжатие – сокращение объема информации. Сжатая информация не может быть прочитана или использована без обратного преобразования.

7.10. Понятие кодирования и декодирования

Использование электронно-вычислительных машин для переработки информации явилось коренным этапом в совершенствовании систем планирования и управления на всех уровнях народного хозяйства. Однако при этом, в отличие от обычных способов сбора и обработки информации, возникли проблемы преобразования информации в символы, понятные для машины. Неотъемлемым элементом этого процесса является кодирование информации.

Код – совокупность символов, соответствующих элементам информации или ее характеристикам.

Сам процесс составления кода в виде совокупности символов или списка сокращений для соответствующих элементов и характеристик называется кодированием. В литературе термин "код" иногда заменяется идентичным ему термином "шифр".

Цель кодирования состоит в том, чтобы представить информацию в более компактной и удобной форме для оперирования при передаче и обработке информации; приспособить кодированную информацию к обработке на вычислительных устройствах; обеспечить использование некоторого определенного метода поиска, сортировки и упорядочения информации.

Принципиальная схема обработки информации состоит из поиска, сортировки и упорядочения, в которой кодирование является частью операции ввода данных в виде входных кодов. В результате обработки информации получаются выходные коды, которые после их декодирования выдаются как результат проведенной обработки.

Декодирование является операцией, обратной кодированию. Если при кодировании происходит преобразование информации в сигналы в виде определенного сочетания символов, соответствующих данному объекту или его характеристике, то при декодировании, наоборот, по заданному коду определяется соответствующий объект или его признаки. Например, в телефонном справочнике указан код, т.е. номер телефона, связанный с некоторым элементом (лицом или учреждением). Операция декодирования

состоит из набора кода номера телефона, который в виде сигналов поступает в АТС, где декодируется с помощью электрической схемы.

Процесс кодирования

Процесс кодирования информации может производиться либо ручным, либо автоматическим способом. При ручном, неавтоматическом способе кодирования вручную отыскивается нужный код в предварительно составленном каталоге кодов и записывается в документе в виде цифровых или алфавитно-цифровых символов.

При автоматическом способе кодирования человек производит запись на естественном языке в виде слов, цифр и общепринятых обозначений в документе, который читается специальным автоматом. Этот автомат предварительно кодирует документ и записывает все данные в двоичном коде.

Ввод информации в ЭВМ в виде буквенно-цифрового текста на естественном языке и кодировании в машине требует хранения в памяти ЭВМ словаря, в котором каждому слову соответствует определенный код. По этому словарю машина сама кодирует текст. При этом отпадает необходимость в классификации и кодировании информации по ее смысловому содержанию, так как кодируются сами слова, выражающие определенные характеристики предметов.

Большое разнообразие технических характеристик и других данных, относящихся к производству и потреблению многочисленных видов продукции, не позволяет включить все необходимые данные для их производства в код продукции, так как этот код содержал бы большое число символов.

Поэтому задача кодирования продукции заключается в том, чтобы иметь возможно более короткий код, по которому в памяти машины можно было бы найти подробную информацию о всех необходимых данных, относящихся к каждому изделию. Таким кодом является ключевой код. Для каждого ключевого кода в памяти ЭВМ должен храниться массив данных, которые извлекаются из памяти и используются для решения различных задач. Этот массив информации должен быть единым для всех решаемых задач, например каталогом продукции, где в одном месте хранятся все необходимые данные о каждом предмете. Разделение его на ряд отдельных массивов, записанных, например, на различных участках магнитной ленты, нецелесообразно, так как это привело бы к повторению одной и той же информации и увеличению объема хранимой информации.

Основное требование к ключевому коду – однозначный поиск ЭВМ признаков, относящихся к данному предмету, для которого ключевой код является адресом.

Ключевой код может быть просто порядковым регистрационным номером и не нести какой-либо конкретной информации о продукции или, наоборот, может

быть построен по определенной системе классификации и содержать конкретную информацию об основных признаках продукции, вполне ее определяющих.

Второй способ кодирования более эффективен, так как регистрационный код не дает возможности осуществить предварительную сортировку информации по ее содержанию.

Ключевой код позволяет производить сортировку карточек продукции по главным определяющим признакам. Детальная спецификация и ее остальные характеристики находятся в предварительно отсортированных карточках.

Виды кодов

Код, символы которого соответствуют определенным предметам или характеристикам, называется прямым кодом. Если код непосредственно не содержит информацию о предмете или его признаках, а представляет адрес, указывающий местоположение информации, где содержится необходимые сведения, то он называется адресным кодом. Адресный код применяется для сокращения кода и быстрого поиска больших массивов информации.

За единицу количества информации принимается 1 бит, т.е. один двоичный разряд (0 или 1). Буквы, десятичные цифры и другие символы внутри ЭВМ представляются в виде групп двоичных разрядов. Операция представления их в таком виде называется двоичным кодированием. Группа из n двоичных чисел позволяет закодировать 2n различных символов. Такая группа называется байтом.

Более крупной единицей информацией является машинное слово, представляющее собой последовательность символов, занимающих одну ячейку в памяти машины. В зависимости от ЭВМ машинного слова может колебаться в пределах – от 16 до 64 двоичных разрядов. машинное слово может быть командой, числом или буквенно-цифровой последовательностью. Обычно машинное слово используется как единое целое в ЭВМ, хотя на некоторых машинах допускается обработка частей машинного слова.

Массив информации, содержащий 1024 машинных слова, называется страницей. Каждый отдельный блок памяти содержит обычно 16 и более страниц. Местоположение (адрес) слова в памяти определяется кодом адреса, содержащим номер блока, страницы и номера слова в этой странице.

Для упорядочения информации о множестве объектов, а также для облегчения их поиска и сортировки по заданным признакам или характеристикам применяется классификация этого множества. Классификация-это условное разбиение множества на ряд классов, подклассов и других группировок по принятой системе счисления и по заданным признакам и характеристикам. Классификационный код – это такой код, в котором отдельными символами или

группой символов представлен каждый из классифицируемых признаков или каждая конкретная характеристика предмета.

Структура и число символов классификационного кода целиком определяется принятой классификацией множества, которая, в свою очередь, зависит от поставленных целей и задач. В классификационном коде каждый символ заключает в себе определенную информацию о конкретном признаке или характеристике предмета. В отличии от этого порядковый, или регистрационный код, содержащий присвоенный данному предмету порядковый номер при его регистрации без учета его признаков и характеристик, может служить только адресом для поиска местоположения информации о данном предмете. Во многих случаях применяются смешанные коды, в которых имеется как классификационная часть, так и порядковые номера для списка классифицируемых предметов множества.

7.11. Стеганография

Стеганография использует принципиально другой подход. Она скрывает не только информацию, но и сам факт её наличия. В качестве примера из обычной жизни можно привести такой. Конечно, секретное письмо можно хранить в большом кованом сундуке с навесным замком, но можно и спрятать, скажем, в потайном кармане. И если в первом случае информацию, возможно, кто-то попытается заполучить, то во втором случае у злоумышленника не будет практически никаких зацепок, где она может находиться. Такой принцип сохранения и передачи ценой информации известен уже давно. Ещё Геродот описывал послания, написанные на деревянных дощечках. В отличие от обычного способа записи, когда сначала наносился слой воска, а потом писался текст, здесь секретная запись выцарапывалась прямо на дощечке, которую потом покрывали воском, где уже и писали – чаще всего, ложное сообщение. Также известны случаи передачи сообщений на голове раба. Сначала его брили, затем писали сообщение, а когда волосы снова отрастали, отправляли в путь.

Компьютерная стеганография

Основной целью компьютерной стеганографии является скрытие файла сообщения внутри файла-контейнера. Кроме того, такая операция должна остаться незамеченной – файл-контейнер обязан не терять функций, а наличие скрытого сообщения должно быть максимально сложно обнаружить.

Рассмотрим основные направления программных реализаций.

Алгоритмы, основывающиеся на свойствах текста

Это направление наиболее близко к некомпьютерной стеганографии. В качестве такого универсального примера можно указать, например, акростих. Но есть и чисто компьютерные методы, основывающиеся, например, на сходстве написания кириллических и латинских символов (можно считать одни

единицами, а другие нулями). Также можно выделять отдельные буквы или слова из текста по определённому алгоритму. Это одно из немногих направлений в информационной безопасности, где собственные алгоритмы могут довольно успешно конкурировать с известными, уже использующимися – ведь чем менее изучен будет алгоритм, тем труднее будет определить наличие скрытого сообщения.

Методы, использующие особенности компьютерных форматов

Этот метод прост в реализации и зачастую не требует специального ПО. Конкретные примеры – поле комментариев в формате JPEG и поле Company в свойствах исполняемых EXE. Простота реализации оборачивается и простотой обнаружения. Хотя и данные алгоритмы могут использоваться, когда у злоумышленников нет даже подозрения на передачу тайной информации.

Алгоритмы, использующие избыточность аудиовизуальной информации

Второе название этого метода – метод младших бит. Основными контейнерами в данном способе скрытия являются форматы так называемого прямого кодирования, например, BMP для графики, или WAV для звука. В них каждый минимальный элемент, каковым, например, является пиксель в BMP, описывается отдельной записью и никак не связан с остальными. Так в обычном BMP на каждый пиксель отводится 24 бита – по 8 бит на канал. При изменении младшего бита изображение практически не изменится. Во всяком случае, не каждый человек и не всегда сможет заметить разницу между пустым и заполненным контейнером.

Это направление – самое популярное среди разработчиков. Современные программы научились обращаться с форматами, поддерживающими сжатие; для самых популярных разработок появились дешифровщики.

В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стенографии только начинается, но проведенные исследования показывают ее перспективность. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов.

Содержанием процесса кодирования информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Недостатками кодирования конфиденциального информации является необходимость хранения и распространения кодировочных таблиц,

которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

Сжатие

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

Тема 8. Основные технологии построения защищенных ЭИС. Защита от разрушающих программных воздействий. RAID-массивы и RAID-технология

8.1. Современные методы и средства обеспечения безопасности в каналах ИВС и телекоммуникаций

Эволюция технологии обеспечения безопасности связи показывает, что только концепция комплексного подхода к защите информации может обеспечить современные требования безопасности в каналах телекоммуникаций. Комплексный подход подразумевает комплексное развитие всех методов и средств защиты и требует проведения их классификации.

Рассмотрим кратко основное содержание методов и средств обеспечения безопасности в каналах телекоммуникаций.

Управление доступом – метод защиты информации регулированием использования всех ресурсов системы (элементов баз данных, программных и технических средств).

Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.).

Маскировка – метод защиты информации в каналах телекоммуникаций путем ее криптографического закрытия.

Этот метод защиты широко применяется за рубежом как при обработке, так и при хранении информации, в том числе на гибких магнитных дисках. При передаче информации по каналам телекоммуникаций большой протяженности этот метод является единственно надежным. В отечественных коммерческих системах этот метод используется еще достаточно редко из-за недостатка технических средств криптографического закрытия и их высокой стоимости в настоящее время.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение – такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – такой метод защиты, который побуждает пользователя и персонал системы не нарушать установленных за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и "неписаных").

Рассмотренные выше методы обеспечения безопасности в каналах телекоммуникаций реализуются на практике применением различных средств защиты, – технических, программных, организационных, законодательных и морально-этических.

Рассмотрим основные средства, используемые для создания механизмов защиты.

Технические средства

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на

аппаратные и физические. Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Из наиболее известных аппаратных средств можно отметить схемы контроля информации по четности, схемы защиты полей памяти по ключу и т. п.

Физические средства реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Программные средства

Программные средства представляют из себя программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Указанные выше средства и составляли основу механизмов защиты на первой фазе развития технологии обеспечения безопасности связи в каналах телекоммуникаций. При этом считалось, что основными средствами защиты являются программные. Первоначально программные механизмы защиты включались, как правило, в состав операционных систем управляющих ЭВМ или систем управления базами данных. Практика показала, что надежность подобных механизмов защиты является явно недостаточной. Особенно слабым звеном оказалась защита по паролю. Поэтому в дальнейшем механизмы защиты становились все более сложными, с привлечением других средств обеспечения безопасности.

Организационные средства

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

Морально-этические средства

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в данной стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета и престижа человека. Наиболее показательным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

Законодательные средства

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

В заключение необходимо также отметить, что все рассмотренные средства защиты делятся на формальные (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

8.2. Анализ типовых мер обеспечения безопасности ПК

В связи с тем, что за последние годы широкое распространение получили персональные ЭВМ (ПК) и локальные вычислительные сети (ЛВС), в государственных учреждениях и промышленных фирмах особую важность приобретает решение проблемы защиты от несанкционированного доступа к ним для предупреждения возможности утечки или кражи коммерческих, финансовых и других ценных данных.

Аналогичные проблемы существуют и для больших ЭВМ, но для них разработаны эффективные аппаратные и программные средства, предотвращающие или сводящие к минимуму подобную опасность. В отличие от них для персональных компьютеров на рынке пока еще немного аппаратных и программных средств, предупреждающих потери данных или несанкционированный доступ к ним. Положение усугубляется еще и тем, что сами пользователи не осознают в достаточной мере возможной опасности, связанной с обработкой данных на персональных ЭВМ. В самом деле, информация, хранящаяся в центрах обработки данных, представляет собой, как правило, не поддающиеся непосредственному восприятию необработанные данные, требующие инженерного анализа и структурирования перед их использованием, в то время как личная информация пользователя содержит преимущественно уже оформленные, готовые к использованию оперативные данные.

Необходимо учитывать и специфические особенности ПК: персональные компьютеры – это небольшие системы (часто портативные) для непосредственной обработки и подготовки текстов с автоматизированным составлением документации для последующего ее редактирования и печатания. Они используются также для подготовки чертежей, распределения и передачи данных другому пользователю в рамках локальной сети. Несмотря на присущие им некоторые ограничения в скорости обработки данных и возможности расширения памяти, по своей производительности они относятся к системам обработки данных в реальном масштабе времени.

Очевидно, что безопасность любой компьютерной системы зависит в первую очередь от ее аппаратных и программных средств и от их взаимодействия. Поэтому предусмотренные в самой аппаратуре (встроенные) или установленные в непосредственной близости от нее внешние средства безопасности обеспечивают более высокий уровень ее защиты, нежели меры безопасности, принимаемые уже после утечки информации. При разработке эффективных мер и средств защиты аппаратных и программных средств должны быть учтены все уязвимые места процедуры обработки данных на ПК, которые следует устранить или свести к минимуму еще на стадии проектирования. Изготовители программных средств должны в дальнейшем разработать соответствующие вспомогательные программы, позволяющие пользователю реализовать необходимые меры безопасности. Должна быть разработана четкая методика выполнения различных операций, выделены наиболее уязвимые участки для несанкционированного доступа к данным.

Утечка данных возможна в результате несанкционированного доступа к системам обработки данных, центральному процессору и другим устройствам (включая принтер, жесткие и гибкие диски, магнитные ленты и т. д.). Источником утечки данных могут оказаться и программные средства, так как существует возможность изменения готовых программ или использования собственных программ пользователя при несанкционированном доступе к ним. В линиях связи замкнутых и открытых сетей передачи данных связующие элементы способны стать источником перехвата данных. Несанкционированный доступ к ПК может быть получен через коммутируемые линии.

Главным объектом "атаки" является устройство контроля доступа, предусмотренное для систем обработки данных, которое злоумышленники стремятся любым способом обойти или отключить для получения доступа к секретным данным. Однако, поскольку большинство ПК не имеет таких базисных систем контроля доступа, возможность незаконного получения важных данных упрощается. Она может быть реализована путем применения хранимых программ (например, сервисных или подобных им) для копирования данных. Могут быть также использованы для этой программы, разработанные и документированные обычным способом, но содержащие дополнительные несанкционированные средства.

Конфиденциальные сведения могут быть получены при несанкционированном использовании пароля. Они могут быть получены и непреднамеренным путем, например, при чистке памяти только путем считывания логически сброшенных данных файлов, содержащихся в оперативной памяти ЭВМ или в

периферийных и внешних запоминающих устройствах (магнитных лентах, гибких и жестких дисках и т. д.).

Другими объектами доступа к данным могут служить копии или распечатки или же данные более общего характера, сброшенные без всякого учета и контроля. Их анализ может позволить получить ценные сведения.

Всеобщая система информационной защиты должна предусматривать и другие меры безопасности, в частности следующие:

- запрет несанкционированного доступа к конфиденциальным данным и к ПК;
- ограничение доступа к особо важным данным (доступ может быть разрешен лишь ограниченному числу лиц);
- все ежедневные информационные операции на ПК должны регистрироваться с указанием личности пользователя, времени работы и используемой программы, а также сопровождаться анализом этих сведений.

Все требования по обеспечению информационной защиты должны быть систематизированы и изданы в качестве руководства (или инструкции), обязательного для исполнения каждым пользователем учреждения или фирмы с обязательным указанием степени конфиденциальности обрабатываемой и хранимой информации и уязвимых мест. В идеальном варианте система защиты может охватывать все сферы работы с ПВЭМ. Для всех уровней пользователей, начиная с верхних эшелонов и кончая рядовыми работниками, должны быть, разработаны специальные учебные программы и тренинги.

Для защиты данных, хранимых на сменных или фиксированных носителях (например, гибких или жестких дисках), от возможного копирования с постоянного носителя на гибкий диск или кражи самого диска щелевое отверстие дисководе должно запираться ключом.

Одной из мер безопасности, предупреждающей несанкционированный доступ к носителям, является шифрование пользователем всех данных с помощью встроенного или дополнительного аппаратного средства.

Идеальным вариантом информационной защиты ПК является интеграция средств контроля доступа в ее операционную систему. Система контроля доступа к ресурсу должна включать четкую организацию проверки пользователей по паролю в соответствии со списком пользователей, имеющих доступ к операционной системе.

И, наконец, все виды операций, выполняемых на ПК, должны строго учитываться и периодически проверяться.

8.3. Методы защиты информации от НСД в сетях ЭВМ

В настоящее время все больше стирается грань между локальными вычислительными сетями и региональными глобальными сетями. Современные сетевые операционные системы, такие как NetWare версии 4.x фирмы Novell или Vines версии 4.11 фирмы Banyan Systems, позволяют поддерживать функционирование ЛВС с выходом на региональный уровень. Наличие в сетях серверов удаленного доступа приближает их по характеристикам к глобальным сетям.

Постоянно растущие технические возможности ЛВС, построенных на базе ПК, требуют расширения, усложнения, совершенствования методов защиты информации в них. Однако в силу высокой структурной сложности, пространственной распределенности и разнообразия режимов функционирования вычислительных сетей используемое программное обеспечение и обрабатываемая в них информация могут оказаться весьма уязвимыми.

Проблемы, возникающие при организации защиты информации в сетях ЭВМ, обусловлены большими размерами и сложностью систем.

Основные факторы, оказывающие существенное влияние на безопасность распределенных систем, которые необходимо учитывать при выборе и создании средств защиты, таковы:

- Большое количество субъектов, имеющих доступ к системе. Количество пользователей и персонала различных категорий, имеющих доступ к ресурсам сети, может достигать значительной величины. Во многих случаях доступ к сети могут иметь неопределенное количество неконтролируемых лиц.
- Значительный объем ресурсов, сосредоточенных в сети. Концентрация в базах данных больших объемов информации наряду с возможностью размещения необходимых пользователю данных в различных удаленных узлах сети.
- Большое количество и разнообразие средств, наличие оборудования разных производителей. Хотя производители обычно декларируют свою приверженность стандартам, на практике функционирование оборудования разных фирм в одной системе может оказаться слабо совместимым.
- Большой объем программного обеспечения, сложность и многоуровневость ПО, высокая степень разнообразия, наличие в сети ПО разных производителей.
- Большое разнообразие вариантов доступа. Требуется обеспечить множество разнообразных вариантов доступа к ресурсам сети. Это

определяется большим числом ресурсов в сети, большим числом пользователей сети и разнообразием их потребностей.

- Значительная территориальная разнесенность элементов сети. Узлы системы могут находиться на большом расстоянии друг от друга, возможно, в разных странах. Наличие протяженных линий связи, необходимость использования при передаче данных промежуточных узлов.
- Интенсивный обмен информацией между компонентами сети.
- Совместное использование ресурсов. Совместное использование ресурсов сети большим количеством пользователей увеличивает риск НСД.
- Распределенная обработка данных (технология клиент-сервер). Распределенная обработка информации требует согласованного совместного функционирования нескольких узлов сети. Это приводит к появлению дополнительных возможностей для НСД и возникновению несогласованностей в данных, расположенных в разных узлах.
- Расширенный объем контроля.
- Практически бесконечное множество комбинаций различных программно-аппаратных средств и режимов их работы. Соединение в сеть нескольких систем, даже однородных по характеру, увеличивает уязвимость системы в целом. Каждая отдельная система настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимыми с требованиями других систем. В случае соединения разнородных систем риск повышается.
- Неизвестный периметр. Легкая расширяемость сетей ведет к тому, что определить границы сети подчас сложно; один и тот же узел может быть доступен пользователям разных сетей. Более того, для многих из них не всегда можно определить, сколько пользователей имеют доступ к определенному узлу и кто они. Границы системы становятся неопределенными, особенно при необходимости обеспечения доступа по коммутируемым линиям связи.
- Множество точек атаки. Данные могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Размерность множества возможных точек атаки многократно возрастает при наличии доступа по коммутируемым линиям связи. Такой способ легко реализуем, но трудно контролируем: он считается одним из наиболее опасных. Линии связи и коммутационное оборудование относятся к наиболее уязвимым местам сети.
- Сложность управления и контроля доступа к системе. Атаки на сеть могут осуществляться без получения физического доступа к определенному

узлу из удаленных точек. В этом случае проведение идентификации может стать очень сложной задачей. Кроме того, время атаки может оказаться слишком небольшим для принятия адекватных мер защиты.

Защищать сеть необходимо от следующих угроз:

- считывание данных в массивах других пользователей;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- мистификация (маскировка под запросы системы);
- использование программных ловушек;
- использование недостатков языков программирования и операционных систем;
- включение в библиотеки программ специальных блоков типа "троянского коня" (называемых в некоторых источниках троянскими программами);
- злоумышленный вывод из строя механизмов защиты;
- внедрение и использование компьютерных вирусов.

В системе защиты сети каждый ее узел должен иметь индивидуальную защиту в зависимости от выполняемых функций и возможностей сети. На каждом отдельном узле необходимо организовать:

- администрирование системы защиты (обеспечение включения данных по санкционированным пользователям в базы данных системы защиты, в т.ч. идентификатор пользователя, (зашифрованные) данные о паролях и/или других идентифицирующих пользователя параметрах, данные по правам доступа);
- идентификацию и аутентификацию пользователей, получающих доступ к данному узлу из сети;
- контроль доступа ко всем файлам и другим наборам данных, доступным из локальной сети и других сетей;
- контроль сетевого трафика (объем информации, передаваемый за определенное время по одному или по нескольким каналам);
- контроль доступа к ресурсам локального узла, с которым работают пользователи сети;
- контроль за распространением информации в пределах локальной сети и связанных с нею других сетей.

В структурно-функциональном составе сети, как правило, принято выделять следующие компоненты:

- рабочие станции или удаленные абонентские пункты сети;

- серверы (хост-машины) – высокопроизводительные ЭВМ, поддерживающие сетевые службы управления файлами, печатью, базами данных и т. п.
- межсетевые шлюзы (мосты, центры коммутации пакетов), обеспечивающие прозрачное соединение нескольких сетей передачи данных либо нескольких сегментов одной и той же локальной сети, имеющих различные протоколы взаимодействия;
- каналы связи (локальные, телефонные коммутируемые каналы).

Первые три компонента могут строиться на базе ПК с использованием специального программного обеспечения. Для защиты данных компонента от побочных электромагнитных излучений и наводок применимы требования и рекомендации, используемые для ПК, обрабатывающих конфиденциальную информацию.

Для обработки конфиденциальной информации необходимо использовать ПК, которые прошли специальные исследования.

Вопрос о необходимости и достаточности мер защиты ПК решается по результатам их специальных исследований (СИ) и на основании анализа условий расположения здания, размера контролируемой (проверяемой) зоны, типа и состава ПК, а также состава вспомогательных технических средств.

Структурно-функциональный состав сети в значительной степени влияет на средства защиты программного и информационного обеспечения. Программные средства защиты при этом могут быть как комплексными, предназначенными для всей сети в целом (например, такие как штатные средства защиты сетевых операционных систем), так и ориентированными на обеспечение безопасности отдельных компонентов.

Важным требованием, предъявляемым к средствам защиты, может служить их функциональная полнота.

Можно выделить следующие основные функции защиты программного и информационного обеспечения, характерные для вычислительной сети как сложного объединения средств электронно-вычислительной техники:

- **администрирование сети.**

Администрирование – один из очевидных и первых встроенных в систему компонентов, которые обеспечивают основу системы безопасности сети. Администратор сети создает новых пользователей, назначает им права, возможное время и возможные рабочие станции для доступа, устанавливает лимиты ресурсов сети. Гибкие средства администрирования позволяют эффективно управлять ресурсами сети и доступом пользователей к ним.

Средства администрирования сети должны обеспечивать возможность включения в БД системы защиты данных о пользователях, в т. ч.

идентификатора пользователя, паролей и других параметров, используемых для аутентификации пользователей, данных о правах пользователя и т. д. Для больших сетей отсутствие развитых средств делает администрирование труднорешаемой, изобилующей ошибками задачей.

- **обеспечение идентификации и аутентификации пользователей;**

Целью аутентификации является идентификация пользователя перед предоставлением ему доступа к информации в сети. Для работы с файлами, директориями и утилитами, находящимися в сети, пользователь должен получить разрешение от операционной системы. Если необходимо, пароли могут быть зашифрованы перед передачей по каналу и перед записью на диск. Может быть установлена минимальная длина пароля и введено требование периодической смены пароля.

Периодическая смена паролей пользователями уменьшает риск их раскрытия, а большая длина паролей затрудняет их угадывание. Возможность регистрации пользователей может быть ограничена по времени (например, только в рабочее время) и месту (только с определенных рабочих станций).

Набор средств, определяющий (образующий) уровень проверки полномочий, использующий идентификатор и пароль пользователя, является базовым средством защиты в любой сети. Первое, на что необходимо обратить внимание при защите сети, – аутентификация. Без нее нельзя управлять полномочиями, доступом или поддерживать контрольный журнал. В любом случае первая задача при предоставлении доступа – это подтверждение прав на него.

Обеспечение контроля доступа в вычислительных сетях заключается в управлении доступом к ресурсам сети. Эта функция должна быть реализована путем проверки подлинности пользователей при начале работы с сетью (идентификация и аутентификация пользователя), проверки подлинности при соединениях (контроль соединений) и собственно организацией контроля (разграничения) доступа (контроль передаваемой информации, управление файлами, контроль прикладных программ).

Идентификация и аутентификация пользователя при начале работы с сетью основываются на системе паролей, на значения которых должны накладываться различные условия, либо их генерация должна осуществляться с помощью специальных средств. При задании паролей пользователями они должны проверяться на возможность их легкого угадывания. Более подробно рекомендации по использованию паролей рассмотрены ниже.

Для проверки подлинности при работе с удаленных рабочих станций нужно использовать модемы "с обратным вызовом" или коммуникационные пакеты, реализующие ее программно с помощью стандартных модемов.

В общем случае необходимым условием обеспечения требуемого уровня защищенности от НСД процедуры аутентификации удаленных пользователей является применение средств шифрования на основе индивидуальных и открытых ключей.

Корректное применение средств шифрования в комплексе с другими средствами позволяет обеспечить необходимый уровень защиты данных.

- **разграничение доступа к ресурсам сети;**

Путем разграничения доступа устанавливается факт: разрешено или нет пользователю иметь доступ к определенному ресурсу сети.

Механизмы разграничения доступа могут охватывать как объекты ЛВС в целом (серверы, сетевые печатающие устройства и т. д.), так и объекты на файл-сервере (процессы, файлы, атрибуты файлов и т. д.).

Разграничение доступа к ресурсам вычислительной сети реализуется, как правило, на нескольких уровнях.

- **очистка "мусора";**
- **обеспечение защиты данных, передаваемых между элементами сети;**

Для обеспечения защиты данных, передаваемых между элементами сети, необходимо осуществлять меры по:

- предотвращению раскрытия содержимого передаваемых сообщений;
- предотвращению анализа потоков сообщений, потоков информационного обмена (трафика);
- предотвращению и выявлению попыток модификаций потока сообщений;
- предотвращению и обнаружению прерываний передачи сообщений;
- обнаружению инициирования ложного соединения.

Для решения задачи по обеспечению защиты данных, передаваемых между элементами сети, хранения критических данных на долговременных запоминающих устройствах, защиты целостности программного обеспечения и сообщений используются криптографические методы.

- **регистрация действий, требующих доступа к защищаемым ресурсам, выявление фактов нарушений;**

Средства регистрации для вычислительных сетей должны обеспечивать возможность автоматического протоколирования обращений к системе разграничения доступа, как легальных, так и попыток несанкционированного доступа к ресурсам сети.

Средства регистрации должны обеспечивать возможность сбора информации о нарушениях в масштабах всей сети. Доступ к журналам регистрации должен быть ограничен средствами разграничения.

Для поддержания средств регистрации и анализа собранной в них информации должны быть разработаны процедуры, построенные на сочетании программных средств обработки и организационных мер безопасности.

- **контроль целостности (корректности процесса изменения состояний) наиболее важных компонентов программного и информационного обеспечения вычислительной сети.**

Применение метода контроля целостности в условиях сети значительно расширяется и усложняется в реализации, так как помимо контроля информации, важной с точки зрения защиты, на отдельных компьютерах сети, необходимо контролировать целостность сетевого программного обеспечения.
Помимо этого в связи с распространением компьютерных вирусов возрастает значение данного метода как одного из средств антивирусной защиты ЛВС.

8.4. Оценка безопасности связи в сети Internet

Развитие систем передачи данных и появление созданных на их основе средств предоставления телекоммуникационных услуг привели к необходимости регламентации доступа пользователей к предоставляемым сетевым и вычислительным ресурсам. Тем не менее, до сих пор проблема несанкционированного доступа к вычисли тельным системам сети Internet до конца не решена, хотя и сформулирован ряд положений по обеспечению безопасности обработки информации.

Средства обеспечения анонимности абонента

Авторизация доступа в Internet предназначена, прежде всего, для учета использования вычислительных ресурсов и оплаты услуг, предоставляемых различными фирмами. Поэтому, как правило, авторизация доступа осуществляется фирмами провайдерами услуг Internet и предназначена исключительно для коммерческого использования.
Необходимо отметить, что различные фирмы предоставляют своим клиентам различную степень свободы. Так, например, при прямом TCP/IP подключении пользователь оказывается привязанным к конкретному географическому адресу, на который выведен выделенный канал связи. При подключении же с помощью коммутируемой линии связи вход в сеть может быть осуществлен практически с любого телефонного аппарата. В то же время это всего лишь иллюзия свободы, поскольку до того, как абонент получит право доступа в сеть, он должен зарегистрироваться в фирме, предоставляющей услуги.
В то же время сам факт пользования сетью Internet вовсе не является каким-либо компрометирующим деянием. Более того, борьба за привлечение все новых и новых пользователей заставляет наиболее крупных поставщиков сетевых услуг, таких как American Online, Prodigy, Delphi, искать новые методы в конкурентной борьбе. Одно из решений - создание системы "гостевых" входов

в сеть, позволяющих некоторое время (суммарное время доступа не превышает нескольких часов) работать в сети без регистрации и оплаты. В частности, программное обеспечение, предназначенное для подобного доступа, поставляется в комплекте со всеми модемами фирмы Zoom.

Это позволяет решить задачу передачи данных и приема информации без предварительной регистрации абонента. Так, передача данных может осуществляться с использованием "гостевого" сетевого адреса, динамически назначаемого при инициации сеанса абонента. Прием информации может обеспечиваться с использованием диалогового режима работы посредством использования систем WWW или FTP. Очевидно, что в этом случае на сервере должны быть развернуты соответствующие службы общего доступа.

8.5. Сетевые средства защиты от несанкционированного доступа

Основным средством защиты сети Internet от несанкционированного доступа в настоящее время являются средства firewalls ("огненные стены"). Они контролируют информационные потоки между локальными вычислительными сетями (ЛВС), причем уровень контроля определяется в первую очередь сферой интересов компании, структурой ЛВС и целями, ради которых она связана с Internet. В этом случае корпоративную сеть часто сравнивают с крепостью, окруженной глубоким рвом, через который перекинуты два моста. Караулы останавливают всех, кто входит и выходит из крепости, и проверяют пароль. Взломщики часто перехватывали пароль и получали право доступа к корпоративным сетям. Поэтому в настоящее время все чаще применяют одноразовые пароли и схемы проверки полномочий, исключающие использование злоумышленниками любой перехваченной информации.

Система Firewall обеспечивает защиту программного обеспечения сервера от доступа без соответствующей авторизации, но в то же время не препятствует нормальной работе ряда штатных служб (sendmail, ftp, www и так далее). Система Firewall является наиболее распространенным средством усиления традиционных средств защиты от несанкционированного доступа, используемого в семействе UNIX, и используется для обеспечения защиты данных при организации межсетевого взаимодействия. Конкретные реализации Firewall в значительной степени зависят от используемых вычислительных платформ, но тем не менее все системы этого класса используют два механизма, один из которых обеспечивает блокировку сетевого трафика, а второй, наоборот, разрешает обмен данными. При этом некоторые версии Firewall делают упор на блокировании нежелательного трафика, а другие – на регламентировании разрешенного межмашинного обмена.

Большинство организаций и центров обработки данных, использующих сетевые, технологии, к моменту появления Firewall уже имели сложившуюся систему обеспечения безопасности. И в большинстве случаев внедрение новой системы не внесло никаких изменений в традиционные подходы к защите данных. Поскольку основная проблема при работе с Internet состоит именно в обеспечении безопасности локальных данных, появление Firewall оказалось фактором, в значительной мере способствующим росту количества пользователей сети, что, в свою очередь, не замедлило сказаться на развитии и самой технологии защиты данных.

Кроме того, Firewall может использоваться в качестве корпоративной открытой части сети, видимой со стороны Internet. Во многих организациях Firewall-системы используются для хранения данных с открытым доступом, например, информации о продуктах и услугах, файлах из баз FTP, сообщений об ошибках и так далее. Отметим, что некоторые из подобных систем "двойного назначения", например, uunet.uu.net или gatekeeper.dec.com, играют важную роль в "скелете" Internet и, по словам владельцев систем, справляются с возложенными на них задачами.

Как правило, Firewall предназначены для предотвращения несанкционированной регистрации в системе по телекоммуникационным сетям, то есть из "внешнего мира". Этого в большинстве случаев оказывается достаточно для предотвращения регистрации вандалов в системе или сети. Существуют и более мощные системы защиты, которые блокируют весь трафик, инициированный внешней частью сети, но дают возможность пользователям системы без каких-либо ограничений взаимодействовать с внешним миром, что позволяет, с точки зрения разработчиков, защититься от любой сетевой атаки.

Ряд Firewall-систем разрешает обмен только электронной почтой, что в еще большей степени ограничивает возможности злоумышленника по проникновению в систему. Но, вообще говоря, подобные меры используются исключительно редко, поскольку накладывают слишком сильные ограничения и на самих пользователей системы.

8.6. Методы криптографической защиты сети

Наиболее надежным методом защиты информационного обеспечения в сетях обмена коммерческой информации является метод шифрования этой информации. Более подробно данную проблему рассмотрим на примере США. Опыт США показывает, что в настоящее время используются три основных алгоритма: алгоритм DES, современный алгоритм АНБ – Clipper (для коммерческой информации) и так называемая общественная инициатива шифрования – алгоритм PGP.

Алгоритм шифрования DES

Алгоритм шифрования DES (Data Encryption Standard) был разработан в начале 70-х годов. В 1974 году фирма IBM предложила этот алгоритм национальному институту стандартов и технологий. Известно, что фирма IBM занимается проблемами криптографии с конца 60-х годов. Ею разработан в 1971 году шифр "Люцифер" (Lucifer). Алгоритм шифрования DES был выполнен в виде интегральной схемы с длиной ключа в 64 символа (56 символов используются непосредственно для алгоритма шифрования и 8 – для обнаружения ошибок). Расчет алгоритмов в то время показывал, что ключ шифрования может иметь 72 квадриллиона комбинаций.

Алгоритм DES был принят в США в качестве федерального стандарта обработки информации в 1977 году и каждые пять лет проходит процедуру подтверждения сертификата этого стандарта. В середине 80-х годов DES был предложен в качестве международного стандарта и подтвержден как DEA-1 (Data Encription Algorithm-1).

Алгоритм DES широко используется при обмене информацией в сети Internet.

Криптоаналитик Циммерман (изобретатель PGP) оценивает криптографическую стойкость DES следующим образом. Интегральная схема DES стоит 10,5 долл. Компьютер, содержащий 57 тысяч интегральных схем подобного типа сложности, будет стоить порядка 1 млн. долл. и в состоянии раскрыть шифр DES максимум за 7 часов, в среднем – за 3,5 часа. При затратах в 10 млн. долл. на раскрытие шифра DES потребуется 21 минута, а при затратах в 100 млн. долл. – всего 2 минуты. АНБ в США обладает такими возможностями.

Новый метод шифрования информации – технология "КЛИППЕР" (CLIPPER)

Правительством США опубликован новый метод шифрования информации, который принят как федеральный стандарт шифрования. Он разработан совместно с Агентством национальной безопасности (АНБ) и неправительственными организациями США. Основной вариант метода, рассчитанный на защиту от прослушивания телефонных разговоров, получил название CLIPPER. Второй вариант, предназначенный для защиты данных, называется CAPSTON.

Метод CLIPPER реализуется на кремниевых кристаллах с микросхемами шифрования (крипточипах) со встроенным алгоритмом шифрования. Эти крипточипы могут быть использованы только при наличии криптографических ключей. Ключи распределяются централизованно на основе подхода, названного "депонированием ключей" (key descrow). Для шифрования и дешифрования речевых сообщений по методу CLIPPER или данных по методу

CAPSTON требуются два ключа. Предполагается, что пользователи получают эти ключи в двух пунктах, управляемых правительственными органами или частными концернами. Правоохранительным органам ключи сообщаются только по решению суда, в соответствии с действующим законодательством о прослушивании линий связи.

Отношение пользователей и экспертов к новому методу неоднозначно. Одна их часть одобряет этот метод и считает, что он решит проблемы, связанные с защитой конфиденциальной информации в неправительственной сфере и приватной информации отдельных граждан, и ограничит возможные неправомерные действия правоохранительных органов. Другая часть высказывает определенные возражения против принятия метода CLIPPER как федерального стандарта и подозревает, что он содержит скрытые "ловушки", известные только правоохранительным органам (АНБ), что позволяет им контролировать определенную информацию. Правительственные агентства, участвовавшие в разработке метода CLIPPER, отрицают наличие таких "ловушек".

Микросхема, получившая наименование CLIPPER, представляет собой сопроцессор шифрования данных, обеспечивающий скорость передачи 12 Мбит/с. Микросхема была разработана фирмой Mykotronx и изготовляется фирмой VLSI Technology (обе – США). Особая конструкция корпуса, в котором размещен кристалл шифратора, предотвращает возможность восстановления секретного алгоритма шифрования по топологии микросхемы. В 1994 году эти фирмы предложили увеличить скорость шифрования до 1 гигабита в секунду за счет создания схемы CLIPPER на арсениде галлия. Это позволяет шифровать информацию, передаваемую по каналу спутниковой связи в реальном масштабе времени.

Криптографические программные средства "PGP"

В июне 1991 года американский программист и компьютерный консультант Филипп Циммерманн (Philip Zimmermann) разработал криптографическую программу для зашифровки передаваемых по электронной почте и сетям связи сообщений.

Разработка программных средств PGP (Pretty Good Privacy) заняла у Циммерманна более полугода напряженной работы. Программный пакет PGP стоит на рынке программных средств 100-150 долл. и продается фирмой Via Crypt. По мнению президента фирмы RSA Data Security Inc., для создания алгоритма шифрования Циммерманн использовал один из запатентованных фирмой криптографических алгоритмов. Математическая часть этого алгоритма разработана специалистами Массачусетского технологического института и опубликована ими в различных, в том числе модернизированных, вариантах.

Программа PGP попала в свободное обращение и циркулирует в сети Internet. Разработанные программные средства PGP стали своеобразным стандартом шифрования сообщений, передаваемых всеми пользователями по электронной почте в сети Internet. Алгоритм шифрования PGP при свободной циркуляции в сети Internet практически бесплатно доступен для любого пользователя, обратившегося в сеть. Циммерманн считает, что он добился своей цели по обеспечению полной конфиденциальности при передаче двусторонних сообщений как основного аспекта сохранения прав человека в США.

Создание алгоритма PGP и его выход в сеть Internet вызвало беспокойство правоохранительных органов США и таких организаций, как АНБ и ФБР. Циммерманн в настоящее время работает над программой зашифровки телефонных речевых переговоров, названной им "Voice PGP". Он является противником правительственного проекта по развитию технологии "Clipper Chip", дающего АНБ возможность вести подслушивание граждан США. По мнению президента Via Crypt, достоинством PGP является тот факт, что алгоритм практически не поддается расшифровке даже такими организациями, как АНБ, и считается американскими специалистами по компьютерной безопасности стойким к дешифровке. В основе стойкости к дешифровке алгоритма PGP лежит принцип использования двух ключей при шифровании и дешифровании. Один ключ находится у отправителя сообщения, а второй ключ находится у абонента, принимающего сообщение. Причем отправителю достаточно пользоваться только одним ключом. Второй ключ сообщения находится в компьютере и защищен шифровальной фразой, а не просто обычным паролем. Такая организация шифрования практически не поддается дешифровке и мешает государственным организациям осуществлять прослушивание. Посылающий сообщение использует для зашифровки только один ключ, открыто пересылаемый ему получателем сообщения. Принимающий сообщение использует для расшифровки оба ключа, причем второй ключ никогда не покидает его компьютера, где он дополнительно защищен паролем-фразой. Программа PGP при достаточно сложной математике делает процесс шифрования и дешифрования на современных персональных компьютерах достаточно быстрым и эффективным, а также стойким к несанкционированному доступу. Циммерманн совершенствует свои программные средства.

Появление алгоритма PGP в Internet вызвало скандал в криптографических кругах и правоохранительных органах США, хотя Циммерманн был давно известен своей правозащитной деятельностью.

Одной из ведущих частных фирм США, занимающихся проблемой криптографической защиты в компьютерных сетях, является фирма RSA.

Фирма RSA Data Security образована в США в 1982 году. Областью деятельности фирмы является специализация на создании средств криптографической защиты компьютерных данных и средств связи программными способами. В своих криптографических методах фирма использует принцип создания кодов за счет умножения больших простых чисел. Расшифровка таких кодов является чисто арифметической задачей, но требующей очень длительного времени и больших компьютерных мощностей. Алгоритм PGP, запатентованный фирмой RSA, юридически в США принадлежит этой фирме, и для использования его в США требуется лицензия или покупка с правом пользования у фирмы RSA.

Фирма RSA разрабатывает также методы применения цифровой подписи (ЦП) под сообщениями, передаваемыми по электронной почте (RSA Digital Signatures), используемые в системе MailSafe. Алгоритм такого шифрования фирма экспортирует по цене порядка 215 долл. за пакет программных средств.

Российский стандарт шифрования данных ГОСТ 28147-89

Единственный в настоящее время коммерческий российский алгоритм ГОСТ 28147-89 является универсальным алгоритмом криптографической защиты данных, как для крупных информационных систем, так и для локальных вычислительных сетей и автономных компьютеров.

Многолетний опыт использования данного алгоритма показал его высокую надежность и удачную конструкцию. Этот алгоритм может реализовываться как аппаратным, так и программным способом, соответствует всем криптографическим требованиям, сложившимся в мировой практике. Он также позволяет осуществлять криптозащиту любой информации независимо от степени ее секретности.

В отличие от рассмотренного выше алгоритма DES в алгоритме ГОСТ 28147-89 используется 256-разрядный ключ, представляемый в виде восьми 32-разрядных чисел, причем расшифровываются данные с помощью того же ключа, посредством второго они были зашифрованы.

Необходимо отметить, что алгоритм ГОСТ 28147-89 полностью соответствует всем требованиям криптографии и обладает всеми достоинствами алгоритма DES, но лишен его недостатков. В частности, за счет использования специально разработанных имитовставок он позволяет обнаруживать как случайные, так и умышленные модификации зашифрованной информации. В качестве недостатка российского алгоритма надо отметить большую сложность его программной реализации и недостаточно высокую скорость работы.

Криптографические алгоритмы электронной подписи

Безбумажная технология резко обострила проблему дистанционной идентификации личности. Возникла необходимость замены рукописной

подписи ее электронным аналогом – электронной цифровой подписью (ЭП). Она может применяться для контроля доступа к особо важным документам, для проверки подлинности документации, контрактов и т. п.

К ЭП предъявляются два основных требования:

- легкость проверки;
- высокая сложность фальсификации.

Несмотря на кажущуюся простоту требований, практическая реализация является достаточно сложной, т. к. не все так гладко, как может показаться на первый взгляд. Дело в том, что, как было установлено в процессе ее эксплуатации, ЭП чрезвычайно подвержена действию "троянских коней" – обобщенного класса программ с преднамеренно заложенными в них потенциально опасными последствиями, активизирующимися при определенных условиях. Например, в момент считывания файла, в котором находится подготовленный к подписи документ, эти программы могут изменить имя подписывающего лица, дату, какие-либо данные (например, сумму платежей) и т. п.

Компьютерная стеганография – современная технология защиты информации

Проблема надежной защиты информации от несанкционированного доступа является одной из древнейших и не решенных до настоящего времени проблем. Способы и методы скрытия секретных сообщений известны с давних времен, причем данная сфера человеческой деятельности получила название стеганография. Это слово происходит от греческих слов steganos (секрет, тайна) и graphy (запись) и таким образом означает буквально "тайнопись", хотя методы стеганографии появились, вероятно, раньше, чем появилась сама письменность (первоначально использовались условные знаки и обозначения).

Для защиты информации используются методы кодирования и криптографии. Как известно, цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений. Стеганография имеет другую задачу, и ее цель – скрыть сам факт существования секретного сообщения. При этом оба способа могут быть объединены и использованы для повышения эффективности защиты информации (например, для передачи криптографических ключей).

На основе анализа открытых информационных источников здесь рассматриваются возможности стеганографии применительно к проблеме защиты информации.

Компьютерная стеганография сегодня

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии, появилось новое направление в области защиты информации – компьютерная стеганография (КС).

Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций. Эти методы, используя естественные неточности устройств оцифровки и избыточность аналогового видео – или аудиосигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). Причем в отличие от криптографии данные методы скрывают сам факт передачи информации.

Основные принципы компьютерной стеганографии и области ее применения

К. Шеннон дал нам общую теорию тайнописи, которая является базисом стенографии как науки. В современной компьютерной стеганографии существует два основных типа файлов: сообщение – файл, который предназначен для скрытия и контейнер – файл, который может быть использован для скрытия в нем сообщения. При этом контейнеры бывают двух типов. Контейнер-оригинал (или "пустой контейнер) – это контейнер, который не содержит скрытой информации. Контейнер-результат (или "заполненный" контейнер) – это контейнер, который содержит скрытую информацию. Под ключом понимается секретный элемент, который определяет порядок занесения сообщения в контейнер.

Основными положениями современной компьютерной стеганографии являются следующие:

- Методы скрытия должны обеспечивать аутентичность и целостность файла
- Предполагается, что противнику полностью известны возможные стеганографические методы.
- Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации – ключа.
- Даже если факт скрытия сообщения стал известен противнику, извлечение самого секретного сообщения должно представлять сложную вычислительную задачу.

Анализ информационных источников компьютерной сети Internet позволяет сделать вывод, что в настоящее время стеганографические системы активно используются для решения следующих основных задач:

- Защита конфиденциальной информации от несанкционированного доступа. Эта область использования КС является наиболее эффективной при решении проблемы защиты конфиденциальной информации. Так, например, только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчета 8 бит в стереорежиме позволяет скрыть за счет замены наименее значимых младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом изменение значений отсчетов составляет менее 1 %. Такое изменение практически не обнаруживается при прослушивании файла большинством людей.
- Преодоление систем мониторинга и управления сетевыми ресурсами. Стенографические методы, направленные на противодействие мониторингу и управлению сетевыми ресурсами системами промышленного шпионажа, позволяют противостоять попыткам контроля информации при ее прохождении через серверы управления локальных и глобальных вычислительных сетей.
- Камуфлирование программного обеспечения. Другой областью использования компьютерной стеганографии в настоящее время является камуфлирование ПО. В тех случаях, когда использование ПО незарегистрированными пользователями является нежелательным, оно может быть закамуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа (например, в звуковом сопровождении компьютерных игр).
- Защита авторского права на некоторые виды интеллектуальной собственности. Еще одной областью использования стеганографии является защита авторских прав. На компьютерные графические изображения наносится специальная метка, которая остается невидимой для глаз, но распознается специальным ПО. Такое программное обеспечение уже используется в компьютерных версиях некоторых журналов. Данное направление стеганографии предназначено не только для обработки изображений, но и для файлов с аудио- и видеоинформацией и призвано обеспечить защиту интеллектуальной собственности.

Обзор известных стеганографических методов

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям:

- Методы, основанные на использовании специальных свойств компьютерных форматов.

- Методы, основанные на избыточности аудио- и визуальной информации.

Первое направление основано на использовании специальных свойств компьютерных форматов представления данных, а не на избыточности самих данных. Специальные свойства форматов выбираются с учетом защиты скрываемого сообщения от непосредственного прослушивания, просмотра или прочтения. Основным направлением компьютерной стеганографии является использование избыточности аудио- и визуальной информации. Цифровые фотографии, цифровая музыка, цифровое видео представляются матрицами чисел. Все эти числа неточны, т. к. неточны устройства оцифровки аналоговых сигналов, а также присутствуют шумы квантования. Младшие разряды цифровых отсчетов содержат мало полезной информации о параметрах звука и визуального образа. Их значения слабо влияют на качество восприятия, что и дает возможность для скрытия дополнительной информации.

Графические цветные файлы со схемой смешения RGB кодируют каждую точку рисунка тремя байтами. Каждая такая точка состоит из аддитивных составляющих: красного, зеленого, синего. Изменение каждого из трех младших битов приводит к изменению менее 1 % интенсивности данной точки. Это позволяет скрывать в стандартной графической картинке объемом 800 Кбайт около 100 Кбайт информации, что не заметно при просмотре изображения.

Краткий обзор стеганографических программ

1. Операционная среда Windows. Stgganos for Win95 является легкой в использовании, но все же мощной программой для шифрования файлов и скрытия их внутри файлов типа BMP, DIB, VOC, WAV, ASCII, HTML. Для удобства использования программа выполнена в виде мастера. Это 32-разрядное приложение содержит собственный Shredder – программу, которая уничтожает файлы на жестком диске. Contraband – программное обеспечение, позволяющее скрывать любые файлы в 24-битовых графических файлах формата BMP.
2. Операционная среда DOS.

Jsteg – программа предназначена для скрытия информации в популярном формате JPG.

FFEncode – интересная программа, которая скрывает данные в текстовом файле. Программа запускается с соответствующими параметрами из командной строки.

StegoDos – пакет программ, позволяющий выбирать изображение, скрывать в нем сообщение, отображать и сохранять изображение в другом графическом формате.

Winstorm – пакет программ, который позволяет шифровать сообщение и скрывать его внутри графического файла PCX-формата.

3. Операционная среда OS/2.

Hide4PGP v 1.1 – программа позволяет прятать информацию в файлах формата BMP, WAV и VOC, при этом для скрытия можно использовать любое число самых младших битов.

Texto – стеганографическая программа, преобразующая данные в английский текст.

Winstorm – аналогична программе для DOS.

4. Для ПК Macintosh.

Stego – позволяет внедрять данные в файлы формата PICT без изменения внешнего вида и размера PICT-файла.

Paranoid – эта программа позволяет шифровать данные по алгоритмам IDEA и DES, а затем скрывать файл в файле.

8.7. Методы сохранения и дублирования информации. Рейд-массивы. Рейд-технология

Первая разработка произошла в 1987 году, когда трое работников Калифорнийского университета – Гибсон (Gibson), Катц (Katz) и Паттэрсон (Patterson) – объявили миру об изобретенной ими технологии Redunand Array of Expensive Discs (Избыточный Массив Недорогих Дисков), или RAID. Спустя год они же представили несколько способов реализации этих массивов – уровней RAID. На сегодняшний день существует восемь уровней дисковых массивов (от 0 до 7), а именно RAID 0, RAID 1, ... , RAID 7.

В стандартном персональном компьютере каждый винчестер видится как независимый диск, обозначенный буквами C, D, E и так далее. В системе RAID несколько жестких дисков помещены в один или несколько массивов. Каждый массив видится как независимый диск, хотя он может объединять два, три, четыре или больше физических дисков.

Организации RAID

Существует два способа организации RAID:

1. Программный. Программный требует наименьших финансовых затрат, так как при помощи программного обеспечения функции RAID-контроллера (стоящего от 20$) выполняет центральный процессор. Причем если разные аппаратные RAID-контролеры поддерживают создание только некоторых уровней RAID, то программно при наличии требуемого количества винчестеров можно реализовать какой угодно массив. Хотя, вообще непонятна польза от использования массивов, реализованных программно. Ведь при программной реализации вся

работа по подготовке информационного потока перекладывается на плечи процессора, загружая его, "благодаря" чему работа всего компьютера замедляется в принципе.

2. Аппаратный. При использовании же аппаратного контроллера всей обработкой данных перед поступлением их на винчестеры и обратно занимается микропроцессор, встроенный в этот контроллер. Тем самым CPU полностью освобождается от лишней работы. Поэтому стараются избегать программного RAID, и используют аппаратные решения. К тому же в аппаратный контроллер встроена кеш-память, в которую временно помещаются последние записанные или последние считанные данные. Таким образом, при запросе одних и тех же файлов часто используемые данные будут считываться из кеша, а не непосредственно с винчестера, что будет существенно разгружать дисковую подсистему.

Материнская плата, как известно, не умеет просто так записывать информацию на диск и считывать ее оттуда. Для осуществления этих операций между материнской платой и дисковым устройством должен находиться контроллер. Дисковых интерфейсов существует как минимум два – SCSI и EIDE. Первый в виду высокого быстродействия и неподъемной цены поддерживающих его устройств является прерогативой лишь серверов и, возможно, некоторых рабочих станций, требующих большого быстродействия. Для всех остальных машин вполне достаточно пусть не таких скоростных, зато заметно менее дорогостоящих EIDE-дисков. В преимущества "скази" (именно так называется SCSI на компьютерном слэнге) можно записать не только повышенное по сравнению с EIDE быстродействие, но и возможность подключать к одному шлейфу более 50 устройств (причем ими не обязательно должны быть винчестеры; можно подключить любое устройство, оснащенное SCSI-разъемом, например принтер или сканер), к тому на длину EIDE-шлейфа накладывается ограничение в 40 см. У SCSI такое ограничение отсутствует, что позволяет размещать созданные дисковые массивы вне корпуса системного блока, имеющего ограниченное для размещения массива пространство. Например, в отдельной стойке, размер которой можно сделать достаточным для размещения массива, а также обеспечить достойную вентиляцию внутри стойки для создания нормального температурного режима дисковым накопителям.

К недостаткам можно отнести вышеупомянутую дороговизну. SCSI-контроллеры встраиваются разве что в какие-то эксклюзивные серверные материнские платы, а вообще повсеместно представляют собой PCI-карты расширения. EIDE же аналоги, напротив, встраиваются сейчас во все современные материнские платы. И хоть и ограничение на длину шлейфа накладывается (если его длина превысит 40 см, скорость обмена данными по

нему резко упадет), и быстродействие EIDE-дисков относительно невысокое, для домашнего компьютера такая дисковая подсистема интерфейса EIDE лучшим решением.

Дисковый массив – это все те же диски, только объединенные особым алгоритмом распределения данных по всем накопителям массива. Каждый алгоритм используется при обработке информации в своем типе массивов. Иными словами, в RAID 0 используется свой алгоритм, в RAID 1 – свой и так далее. Не важно, какие диски – SCSI или EIDE – используются при построении массива. Алгоритм выбранного уровня RAID не будет зависеть от интерфейса дисковых накопителей. К примеру, при построении массива RAID уровня 0 что из SCSI-, что из EIDE-винчестеров, алгоритм RAID 0 не изменится.

Информация на RAID

Идея создания RAID-системы заключается в следующем, из набора обычных дисковых накопителей создается массив, который управляется специальным контроллером и определяется сервером как единый логический диск большой емкости. Высокое быстродействие системы обеспечивается возможностью параллельного выполнения нескольких операций вывода (ввода), а сохранность информации – ее дублированием или вычислением контрольных сумм.

Следует отметить, что применение RAID массивов защищает от потерь данных только в случае физического отказа жестких дисков. Использование RAID массивов не может обезопасить Ваши данные в случаях:

- отказа RAID контроллера;
- сбоев оборудования;
- сбоев программных средств;
- ошибочных действий обслуживающего персонала;
- ошибках или злонамеренных действий пользователей;
- вирусных атаках;
- а также в при возникновении любых иных проблем, не связанных с технической неисправностью накопителей.

Многие организации используют дисковые RAID массивы для защиты от потерь данных при физических отказах дисковых накопителей, а также для ускорения доступа к данным.

Следует учесть, что RAID массивы помогают сохранить данные только в случае отказа дискового накопителя, и больше ни в каких случаях. Так называемые "зеркальные" массивы RAID 1 дублируют данные одновременно на двух различных дисках. При отказе одного из них данные можно будет легко восстановить с другого, уцелевшего диска. Массивы RAID 5 хранят избыточную информацию, позволяющую продолжить работу при отказе одного (но не двух!) из нескольких дисков.

Однако дисковые массивы RAID не помогут Вам при отказе дискового контроллера, вирусном заражении, а также при возникновении фатальных ошибок в прикладном программном обеспечении или операционной системе. Отказы контроллера массива RAID 5 зачастую приводят к наиболее тяжелым повреждениям данных, так как затрагивают область контрольных сумм. В результате содержимое массива превращается в хаотическую мешанину байтов, из которой невозможно обычным способом что-либо извлечь.

Еще одна распространенная причина потерь данных в массивах RAID связана с неумелым использованием утилит администрирования таких массивов, расположенной в BIOS контроллера. Невнимательное выполнение операций, связанных с добавлением новых дисков или изменением текущей конфигурации контроллера RAID может привести к частичной или полной потере данных.

Немало случаев, когда после выхода из строя одного из дисков функционирование неисправного массива либо продолжается, либо предпринимаются попытки немедленного восстановления его работоспособности, без предварительного создания резервной копии имеющихся данных. Последующий отказ еще одного диска или ошибочные действия по горячей замене вышедшего из строя диска приводят к потере информации, которую можно было легко сохранить.

У RAID-массивов всех уровней есть общая особенность – операционная система сервера, к которому они подключены, работает с ними как с единым логическим диском. Это означает, что можно объединить различные RAID-уровни для создания массива массивов, где физические диски заменены. RAID-массивами второго уровня, которые не обязательно должны иметь ту же схему хранения данных, что и массив первого уровня. Объединение массивов позволяет создать системы хранения огромной емкости.

В связи с техническими трудностями восстановления информации в случае сбоя RAID-массивы пятого уровня обычно содержат не более 5-6 дисков, их совокупной емкости может не хватить для хранения всей информации, но создание массива массивов решает эту проблему.

Кроме того, комбинирование RAID-уровней позволяет использовать их преимущества и сглаживать недостатки. Обычно соединение устроено таким образом, что сервер работает с высокопроизводительным RAID-массивом, а низкопроизводительные используются для обеспечения сохранности данных.

- RAID 0. Дисковый массив без отказоустойчивости (Striped Disk Array without Fault Tolerance)
- RAID 1. Дисковый массив с зеркалированием (mirroring)
- RAID 2. Отказоустойчивый дисковый массив с использованием кода Хемминга (Hamming Code ECC)

- RAID 3. Отказоустойчивый массив с параллельной передачей данных и четностью (Parallel Transfer Disks with Parity)
- RAID 4. Отказоустойчивый массив независимых дисков с разделяемым диском четности (Independent Data disks with shared Parity disk)
- RAID 5. Отказоустойчивый массив независимых дисков с распределенной четностью
- RAID 6. Отказоустойчивый массив независимых дисков с двумя независимыми распределенными схемами четности
- RAID 7. Отказоустойчивый массив, оптимизированный для повышения производительности
- JBOD (Just a Bunch Of Drives)
- Комбинированные уровни RAID массивов

RAID 0. Дисковый массив без отказоустойчивости (Striped Disk Array without Fault Tolerance)

Массив дисков без избыточного хранения данных. Информация разбивается на блоки, которые записываются на отдельные диски, что обеспечивает увеличение производительности. Суть его в том, что поток данных разрезается на кусочки равного размера. Этот дисковый массив должен состоять как минимум из двух винчестеров, которые делят между собой этот поток данных. Условно представим, что поток поделен на кусочки "1", "2", "3", "4", "5" и "6". Тогда диски, составляющие RAID 0, возьмут каждый по одному кусочку этого потока. Так, если в массиве есть два харда – "C" и "D", то первый возьмет себе кусочек "1", а второй – кусочек "2". Далее "C" записывает "3", а "D" – "4". И так далее. Необходимо заметить, что я не совсем точно описал процесс записи, так как не сначала записывается "1", затем "2", а после него "3". Совсем не так! Диск "C" непрерывно пишет куски "1", "3", и "5" потока данных, а диск "D" непрерывно записывает "2", "4" и "6". Причем диски записывают эти кусочки одновременно. Чтение записанных данных диски RAID 0 производят также одновременно (параллельно). С одного харда считываются нечетные кусочки, а со второго – четные. Именно за счет параллельности производительность RAID 0 буквально удваивается по сравнению с производительностью одиночного винчестера, потому что запрос чтения или записи, теоретически предназначающийся для одного харда, выполняют сразу два (или более – смотря из скольких дисков, вы построите массив) винчестера. Чем больше дисков в массиве, тем быстрее обработается запрос. Данные способ хранения информации ненадежен (поломка одного диска приводит к потере всей информации), поэтому уровнем RAID как таковым не является. За счет возможности одновременного ввода/вывода с нескольких дисков RAID 0 обеспечивает максимальную скорость передачи данных и максимальную

эффективность использования дискового пространства, так как не требуется места для хранения контрольных сумм. Реализация этого уровня очень проста. В основном RAID 0 применяется в тех областях, где требуется быстрая передача большого объема данных.

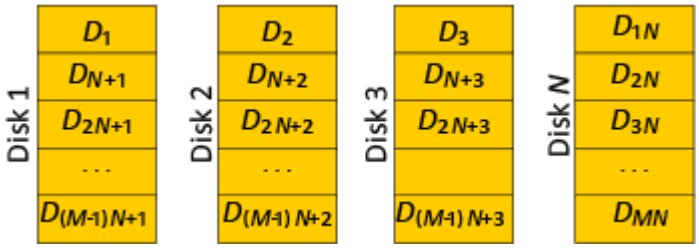


Рисунок 8.1 – RAID 0

Преимущества:

- Наивысшая производительность в приложениях, требующих интенсивной обработки запросов ввода/вывода и данных большого объема;
- Простота реализации;
- Низкая стоимость.

Недостатки:

- Не отказоустойчивое решение;
- Отказ одного диска влечет за собой потерю всех данных массива.

RAID 1. Дисковый массив с зеркалированием (mirroring)

Дисковый массив с дублированием информации, так называемая схема с зеркалированием данных. В простейшем случае два накопителя содержат одинаковую информацию и являются одним логическим диском. То есть сначала кусочки "1", "2", "3", "4", "5" и "6" записываются на диск "C", а затем на "D" (и на все остальные винчестеры массива, если таковые присутствуют). Причем запись происходит последовательно, а именно пока не будет завершена запись на один винчестер, следующий будет ожидать свою очередь. Тем самым обеспечивается самый высокий уровень сохранности данных: при выходе из строя одного диска его функции выполняет другой (что абсолютно прозрачно для пользователя). Кроме того, этот уровень удваивает скорость считывания информации, так как эта операция может выполняться одновременно с двух дисков.

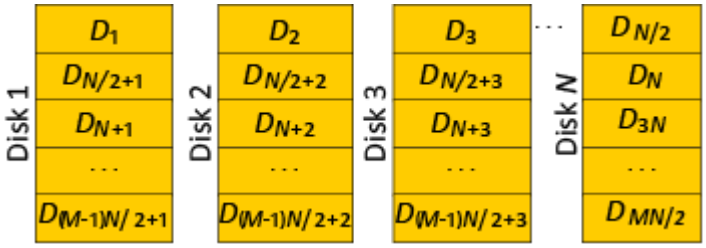


Рисунок 8.2 – RAID 1

Такая схема хранения информации используется в основном в тех случаях, где "цена" безопасности данных намного выше стоимости реализации системы

хранения. Но поскольку цены на диски все время снижаются, RAID 1 становится все популярней. В серверах среднего уровня, где объем хранимой информации не так велик, его применение может быть вполне оправдано. RAID 1 прост в реализации, позволяет создать отказоустойчивую систему всего из двух дисков, самый большой его минус – высокая стоимость.

Преимущества:

- Простота реализации;
- Простота восстановления массива в случае отказа (копирование).

Недостатки:

- Высокая стоимость – 100% избыточность;
- Невысокая скорость передачи данных.

RAID 2. Отказоустойчивый дисковый массив с использованием кода Хемминга (Hamming Code ECC)

Схема резервирования данных с использованием кода Хэмминга (Hamming code) для коррекции ошибок – запатентован компанией Thinking Machines. Поток данных разбивается на слова таким образом, что количество бит в слое равно количеству дисков и при записи слова каждый отдельный бит записывается на свой диск. Для каждого слова вычисляется код коррекции ошибок, который записывается на выделенные диски для хранения контрольной информации. Их число равно количеству бит в слове контрольной суммы.

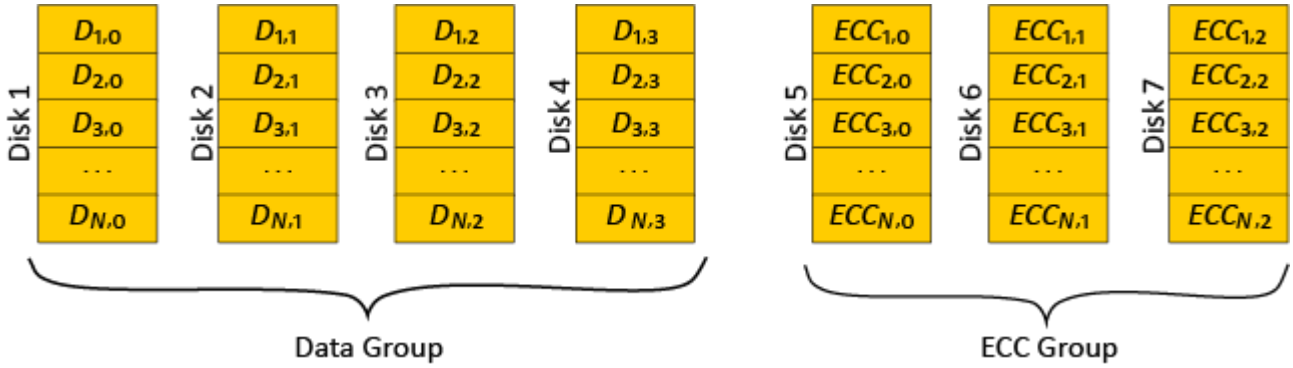


Рисунок 8.3 – RAID 2

Например, если слово состоит из четырех бит, то под контрольную информацию отводится три диска. RAID 2 – один из немногих уровней, позволяющих обнаруживать двойные ошибки и исправлять "на лету" одиночные. При этом он является самым избыточным среди всех уровней с контролем четности. Такая схема хранения подходит для приложений, где требуется передача большого объема данных (за счет параллельного обращения к дискам), но неприменима для задач с большим количеством запросов малого объема (за счет сравнительно большого объема операций, который требуется для перераспределения данных), RAID 2 относительно дорог, но при увеличении количества дисков стоимость реализации снижается. Эта схема хранения данных мало применяется, поскольку плохо справляется с большим

количеством запросов, сложна в организации и имеет незначительные преимущества перед уровнем RAID 3.

Преимущества:

- Достаточно простая реализация;
- Быстрая коррекция ошибок;
- Очень высокая скорость передачи данных;
- При увеличении количества дисков накладные расходы уменьшаются.

Недостатки:

- Низкая скорость обработки запросов;
- Большая стоимость при малом количестве дисков.

RAID 3. Отказоустойчивый массив с параллельной передачей данных и четностью (Parallel Transfer Disks with Parity)

Отказоустойчивый массив с параллельным вводом/выводом и диском контроля четности. Поток данных разбивается на блоки на уровне байт (хотя возможно и на уровне бит) и записывается одновременно на все диски массива, кроме диска, который выделен для хранения контрольных сумм, вычисляемых при записи данных. Поломка любого из дисков массива не приведет к потере информации, которую можно восстановить вычислением операции "исключающее ИЛИ (XOR)", примененной к информации на оставшихся дисках.

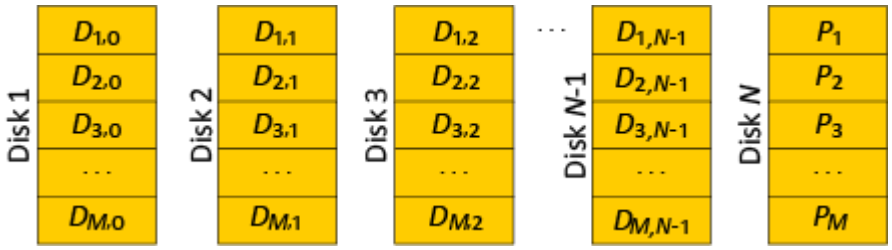


Рисунок 8.4 – RAID 3

Этот уровень имеет намного меньшую избыточность, чем RAID 2, в схеме которого большинство дисков, хранящих контрольную информацию, нужны для определения неисправного разряда. Как правило, RAID-контроллеры могут получить данные об ошибке с помощью механизмов отслеживания случайных сбоев (при помощи расшифровки сигналов от дисков или дополнительного кодирования). Благодаря разбиению данных на блоки RAID 3 имеет высокую производительность. При считывании информации не производится обращения к диску с контрольными суммами (в случае отсутствия сбоя), что происходит всякий раз при операции записи. Поскольку при каждой операции ввода/вывода производится обращение практически ко всем дискам массива, одновременная обработка нескольких запросов невозможна. Этот уровень подходит для приложений с файлами большого объема и малой частотой обращений (в основном это сфера мультимедиа). Использование только одного диска для

хранения контрольной информации объясняет тот факт, что коэффициент использования дискового пространства достаточно высок (и как следствие этого – относительно низкая стоимость). Кроме того, достоинством RAID 3 является незначительное снижение производительности при сбое и быстрое восстановление информации, недостатком – сложность реализации.

Преимущества:

- Очень высокая скорость передачи данных;
- Отказ диска мало влияет на скорость работы массива;
- Очень высокая скорость передачи данных;
- Малые накладные расходы для реализации избыточности.

Недостатки:

- Сложная реализация;
- Низкая производительность при большой интенсивности запросов данных небольшого объем.

RAID 4. Отказоустойчивый массив независимых дисков с разделяемым диском четности (Independent Data disks with shared Parity disk)

Отказоустойчивый массив независимых дисков с общим диском контроля четности, во многом схож с уровнем RAID 3. Поток данных разделяется не на уровне байтов, а на уровне блоков, каждый из которых записывается на отдельный диск. После записи группы блоков вычисляется контрольная сумма, которая записывается на выделенный для этого диск.

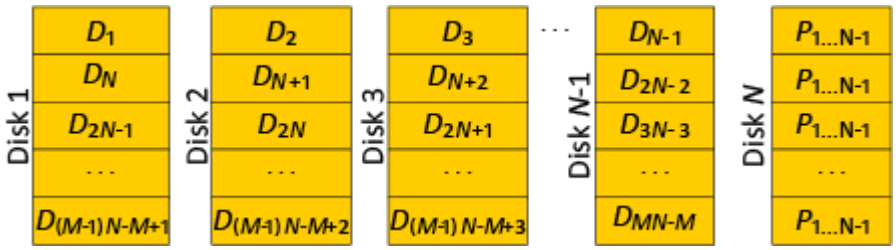


Рисунок 8.5 – RAID 4

Благодаря большему, чем у RAID 3, размеру блока возможно одновременное выполнение нескольких операций чтения. RAID 4 повышает производительность передачи файлов малого объема (за счет распараллеливания операции считывания). Но поскольку при записи должна изменяться контрольная сумма на выделенном диске, одновременное выполнение операций невозможно (налицо асимметричность операций ввода и вывода). Этот уровень имеет все недостатки RAID 3 и не обеспечивает преимущества в скорости при передаче данных большого объема. Схема хранения разрабатывалась для приложений, в которых данные изначально разбиты на небольшие блоки, поэтому нет необходимости разбивать их дополнительно. RAID 4 – неплохое решение для файл-серверов, информация с которых в основном считывается и редко записывается. Эта схема хранения

данных имеет невысокую стоимость, но ее реализация достаточно сложна, как и восстановление данных при сбое.

Преимущества:

- Очень высокая скорость передачи данных;
- Отказ диска мало влияет на скорость работы массива;
- Очень высокая скорость передачи данных;
- Малые накладные расходы для реализации избыточности.

Недостатки:

- Достаточно сложная реализация;
- Очень низкая производительность при записи данных;
- Сложное восстановление данных.

RAID 5. Отказоустойчивый массив независимых дисков с распределенной четностью

Отказоустойчивый массив независимых дисков с распределением контрольных сумм (массив с вращающейся четностью). Самый распространенный уровень. Блоки данных и контрольные суммы циклически записываются на все диски массива, отсутствует выделенный диск для хранения информации о четности: нет асимметричности конфигурации дисков.

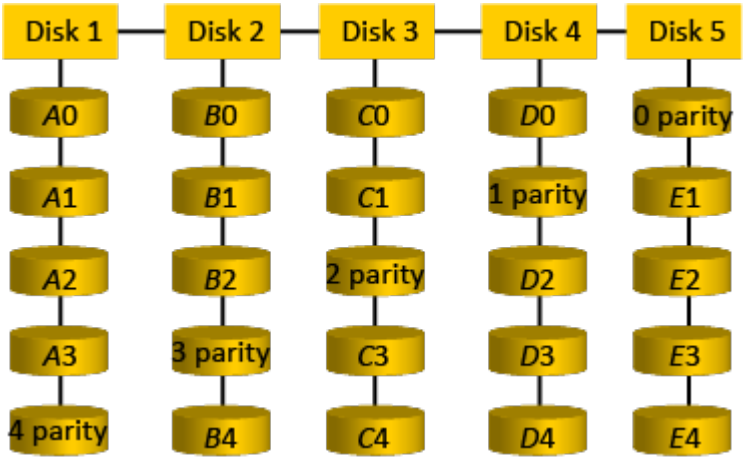


Рисунок 8.6 – RAID 5

В случае RAID 5 все диски массива имеют одинаковый размер, но по одиночки для операционной системы они не видны. На уровне RAID контроллера все диски объединяются в один большой диск. Например, если 3 диска имеют размер 1 Гб, то фактически размер массива составляет 2 Гб, 1 Гб отводится на контрольную информацию. В случае добавления четвертого диска операционная система будет видеть 3 Гб, 1 Гб предназначен для хранения контрольных сумм. Самый большой недостаток уровней RAID от 2-го до 4-го – это наличие отдельного (физического) диска, хранящего информацию о контрольной сумме. Операции считывания не требуют обращения к этому диску, и, как следствие, скорость их выполнения достаточно высока, но при каждой операции записи на нем изменяется информация, поэтому схемы RAID

2-4 не позволяют проводить параллельные операции записи. RAID 5 не имеет этого недостатка, так как контрольные суммы равномерно распределяются по всем дискам массива. Это позволяет выполнять нескольких операций считывания или записи одновременно. Грамотная реализация этого уровня в случае массива из N дисков позволяет одновременно обрабатывать N/2 блоков данных. RAID 5 имеет достаточно высокую скорость записи-считывания (скорость чтения ниже, чем у RAID 4) и малую избыточность, т.е. он экономичен.

Преимущества:

- Высокая скорость записи данных;
- Достаточно высокая скорость чтения данных;
- Высокая производительность при большой интенсивности запросов чтения/записи данных;
- Малые накладные расходы для реализации избыточности.

Недостатки:

- Низкая скорость чтения/записи данных малого объема при единичных запросах;
- Очень низкая производительность при записи данных;
- Достаточно сложная реализация;
- Сложное восстановление данных.

RAID 6. Отказоустойчивый массив независимых дисков с двумя независимыми распределенными схемами четности

Этот термин используют как минимум в трех разных случаях. Как часто бывает при бурном развитии технологии, различные производители компьютерного оборудования разрабатывают свои собственные расширения стандартных архитектур. Названия, которые им присваиваются, происходят иногда от инженерного сленга и представляют реальные технологические улучшения, другие же – плод творчества отдела маркетинга и своего рода попытка привлечь внимание покупателя (маркетинговая уловка).

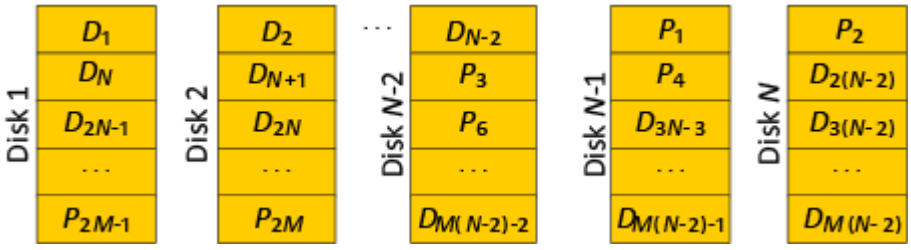


Рисунок 8.7 – RAID 6

Некоторые производители берут массив RAID 5, добавляют избыточные источники питания и, возможно, диск "горячего" резервирования (свободный диск, на который автоматически переносится информация с накопителя, вышедшего из строя, тем самым восстанавливается состояние системы до сбоя)

и называют эту конфигурацию RAID 6. Другие просто несколько изменяют процедуру записи, используемую в RAID 5, добавляют к 5 единицу и получают RAID 6. Но настоящий RAID 6 – это отказоустойчивый массив независимых дисков с распределением контрольных сумм, вычисленных двумя независимыми способами. Этот уровень во многом схож с RAID 5, но наличие двух независимых схем контроля четности позволяет сохранять работоспособность системы при одновременном выходе из строя двух накопителей. Для вычисления контрольных сумм в RAID 6 используется алгоритм, построенный на основе кода Рида-Саломона. При его выполнении применяются специальные таблицы, или он является итерационным процессом, использующим линейные регистры с обратной связью.

Этот уровень имеет очень высокую отказоустойчивость, большую скорость считывания (данные хранятся блоками, нет выделенных дисков для хранения контрольных сумм), но из-за большого объема контрольной информации – низкую скорость записи. Он очень сложен в реализации, характеризуется низким коэффициентом использования дискового пространства (для массива их пяти дисков он составляет всего 60%, но с ростом числа дисков ситуация исправляется).

"Истинный" RAID 6 по многим характеристикам проигрывает другим уровням, поэтому на сегодняшний день не реализован ни одной фирмой, производящей RAID-системы. Все модели RAID 6, которые встречаются на рынке, – небольшие модификации RAID 5.

Преимущества:

- Высокая отказоустойчивость;
- Достаточно высокая скорость обработки запросов;
- Относительно малые накладные расходы для реализации избыточности.

Недостатки:

- Низкая скорость чтения/записи данных малого объема при единичных запросах;
- Очень сложная реализация;
- Сложное восстановление данных;
- Очень низкая скорость записи данных.

RAID 7. Отказоустойчивый массив, оптимизированный для повышения производительности

Является зарегистрированной торговой маркой корпорации Storage Computer. Во многом он похож на RAID 4 с возможностью кэширования данных. В состав RAID 7 входит контроллер с встроенным микропроцессором под управлением операционной системы реального времени (SOS). Она позволяет обрабатывать все запросы на передачу данных (как между отдельными дисками, так и между

массивом и компьютером) асинхронно и независимо. Блок вычисления контрольных сумм интегрирован с блоком буферизации, для хранения информации о четности используется отдельный диск, который может быть размещен на любом канале. RAID 7 имеет высокую скорость передачи данных и обработки запросов, хорошее масштабирование (при увеличении числа дисков повышается скорость записи). Самым большим недостатком этого уровня является стоимость его реализации.

Преимущества:

- Очень высокая скорость передачи данных и высокая скорость обработки запросов (в 1.5-6 раз выше других стандартных уровней RAID);
- Высокая масштабируемость хост-интерфейсов (до 12-ти интерфейсов и до 48-ми дисков;
- Для вычисления четности нет необходимости в дополнительной передаче данных.

Недостатки:

- Сложная реализация;
- Очень высокая стоимость на единицу объема;
- Не может обслуживаться пользователем;
- Нужно использовать блок бесперебойного питания для предотвращения потери данных из кэш-памяти (впрочем, UPS и так практически всегда применяется для питания серверов);
- Короткий гарантийный срок.

JBOD (Just a Bunch Of Drives).

В операционной системе Windows JBOD-массив называется spanned disk. Это не уровень RAID, а дополнительная функция некоторых рейд контроллеров. Применяется в случае, если пользователь хочет использовать суммарную емкость нескольких жестких дисков, имеющих разный объем. Однако, кроме увеличения емкости, от этого способа объединения жестких дисков других существенных преимуществ нет.

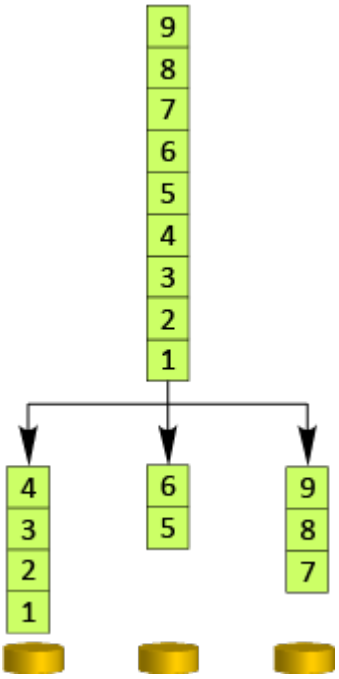


Рисунок 8.8 – Размещение данных на дисках массива организации JBOD

Характеристики JBOD массива:

- Размер массива равен суммарному объему всех дисков.
- Вероятность отказа повышается, так как избыточность не обеспечивается, в случае выхода из строя любого из дисков, массив разрушается.
- Временные характеристики определяют самый медленный и самый быстрый диски. Скорость чтения и записи не выше, чем у самого быстрого диска в массиве и не ниже чем у самого медленного диска.
- Нагрузка на процессор при работе минимальная такая же как при работе с обычным диском.

Особенности JBOD массива:

- Отказ одного диска позволяет восстановить файлы на остальных дисках, если их начало/конец не принадлежат отказавшему диску.
- В ряде случаев возможно обеспечение высокой скорости работы нескольких приложений, если приложения работают данными на разных дисках.
- Рейд может состоять из дисков различной емкости и быстродействия.

Комбинированные уровни RAID массивов

Современные RAID контроллеры позволяют комбинировать различные уровни RAID. Таким образом, можно реализовать системы, которые объединяют в себе достоинства различных уровней, а также системы с большим количеством дисков. Обычно это комбинация нулевого уровня (stripping) и какого либо отказоустойчивого уровня.

RAID 10 (RAID 1+0). Отказоустойчивый массив с дублированием и параллельной обработкой

Комбинация уровней 1 и 0. Каждый физический диск уровня RAID 0 заменяется массивом RAID 1. Это обеспечивает высокую производительность передачи данных, (сервер видит массив как RAID 0) и высокую их сохранность, но значительно ограничивает масштабирование, и коэффициент использования дискового пространства получается очень низким – всего 50%.

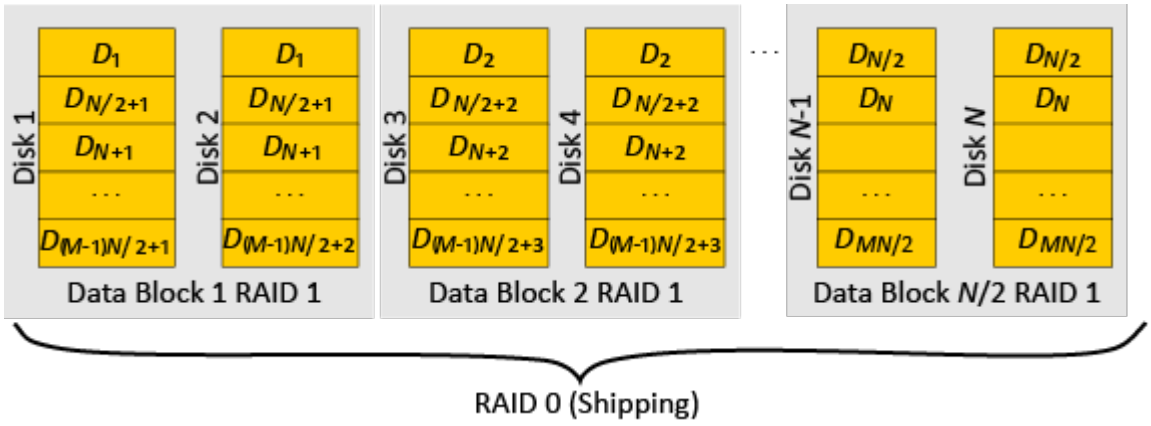


Рисунок 8.9 – RAID 10

Преимущества:

- Очень высокая скорость записи данных при не менее высокой надежности.

Недостатки:

- Очень высокая стоимость;
- Ограниченное масштабирование.

RAID 30 (RAID 3+0). Отказоустойчивый массив с параллельной передачей данных и повышенной производительностью

Массив нулевого уровня, роль дисков которого играют массивы RAID 3, сочетает производительность RAID 0 и отказоустойчивость RAID 3. Поскольку в схеме RAID 3 дисковое пространство используется более рационально, чем в RAID 1, то у массивов RAID 3+0 коэффициент его использования выше, чем у RAID 1+0, и равен 40%. Эта схема имеет ограниченное масштабирование.

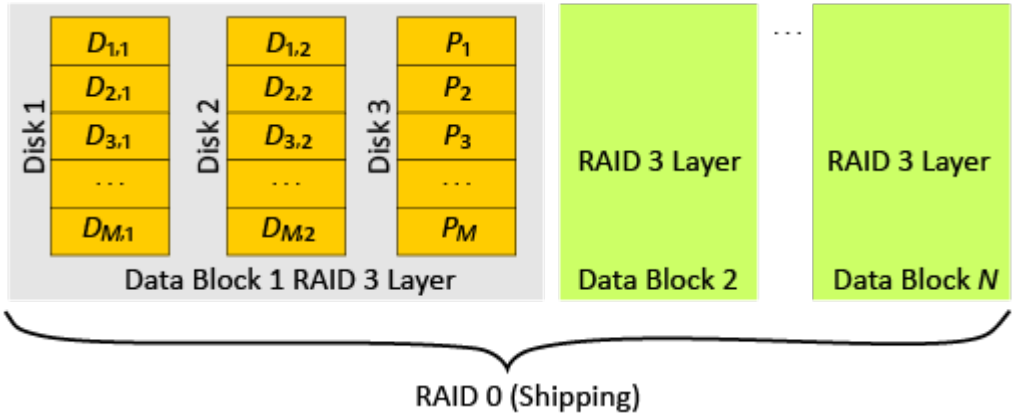


Рисунок 8.10 – RAID 30

RAID 50 (RAID 5+0). Отказоустойчивый массив с распределенной четностью и повышенной производительностью

Массив нулевого уровня, роль дисков которого играют массивы RAID 5. Он объединяет в себе отказоустойчивость и высокую производительность для приложений с большой интенсивностью запросов и высокую скорость передачи данных. RAID 5+0 обладает высокой производительностью и стоимостью. Эта схема тоже имеет ограниченное масштабирование. Возможен еще вариант RAID 5+3, когда физические диски массива RAID 5 заменяются массивами RAID 3.

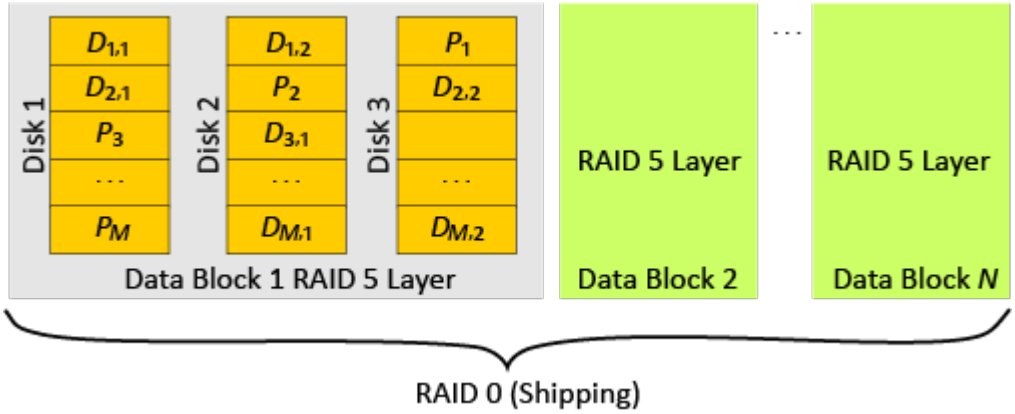


Рисунок 8.11 – RAID 50

Преимущества:

- Высокая отказоустойчивость и производительность;
- Достаточно высокая скорость чтения данных;
- Высокая производительность при большой интенсивности запросов чтения/записи данных;
- Малые накладные расходы для реализации избыточности.

Недостатки:

- Большая стоимость;
- Ограниченное масштабирование.

Восстановление данных RAID массива.

Используемая нами технология восстановления данных RAID – массива гарантирует конфиденциальность информации на Вашем жестком диске. Эта технология также полностью исключает вероятность фатальной ошибки в процессе восстановления данных, что нередко происходит при попытках восстановления RAID – массива непосредственно на самих дисках с поврежденным RAID – массивом. В этих случаях неудачная попытка корректировки приводит к необратимым последствиям – безвозвратной потере всех данных и информации. Чтобы избежать подобных проблем, мы предварительно производим копирование исходных дисков на технологические носители, и вся работа производится с копиями Ваших дисков. Программы, применяемые нами, имеют процедуру контроля допустимости записи на указанный жесткий диск. В этом их основное отличие от программ клонирования, широко распространенных в сети. Программы клонирования,

разработанные в нашей Лаборатории, будут осуществлять запись только на указанный жесткий диск.

Причины потерь данных на RAID массивах

Многие пользователи предпочитают использовать дисковые массивы RAID 5 в целях защиты от потерь данных при физических отказах накопителей, а также для ускорения доступа к информации. Однако не стоит забывать о том, что они помогают сохранить данные только при отказе одного дискового накопителя, и больше ни в каких случаях. Так называемые "зеркальные" массивы RAID 1 осуществляют запись данных на два различных дисках одновременно, следовательно, при отказе одного из дисков данные легко можно восстановить с другого. На массивах же RAID 5 хранится избыточное количество информации, позволяющую продолжить работу только при отказе одного (но не двух!) из дисков. Также следует учитывать, что RAID – массивы не помогут в случаях:

- отказа дискового контроллера;
- поражения вирусами;
- в случае возникновения фатальных ошибок в прикладном программном обеспечении или операционной системе.

При отказах дискового контроллера в массивах RAID 5 происходят наиболее серьезным повреждениям данных, так как в этих случаях оказываются затронуты области контрольных сумм. Как результат – вся информация, содержащаяся на диске, превращается в бессмысленную мешанину байтов, извлечь из которой что-либо не представляется возможным без специальных технологий. Еще одна причина потери данных в массивах RAID 5 – неумелое использование утилиты администрирования подобных массивов, расположенной в BIOS контроллера. Невнимательность при выполнении операций, связанных с добавлением новых дисков или изменением текущей конфигурации контроллера RAID способна привести к полной потере данных и информации. Немало случаев, когда после выхода из строя одного из дисков функционирование неисправного массива либо продолжается, либо предпринимаются попытки немедленного восстановления его работоспособности, без предварительного создания резервной копии имеющихся данных. Последующий отказ еще одного диска или ошибочные действия по горячей замене вышедшего из строя диска приводят к потере информации, которую можно было легко сохранить. Достаточно часто встречаются случаи, когда функционирование неисправного массива после выхода из строя одного из дисков либо продолжается, либо предпринимаются попытки немедленного восстановления его работоспособности, без предварительного создания резервной копии имеющихся данных. Следующий за этим отказ еще одного диска или неверные действия по немедленной замене

вышедшего из строя диска приводят к утере информации, которую можно было с легкостью сохранить с помощью адекватных в этой ситуации действий. Мы не будем давать рекомендаций по восстановлению RAID массивов. Из собственного опыта нам известно, что любые попытки восстановить RAID массивов неспециалистами в этой области, не владеющими тонкостями организации RAID массивов, заканчиваются фатальным разрушением данных RAID массивов. Если Вы все же хотите все же самостоятельно проанализировать состояние отдельных дисков RAID массивов, прислушайтесь к нашему совету: ни в коем случае не просматривайте диски под управлением Windows! Все дело в том, что настройки операционной системы по умолчанию предполагают, что диски имеют четко определенную структуру, и любое отклонение от этой схемы может быть воспринято системой любым из трех нижеследующих способов:

- воспринято как разрушение файловой системы;
- диск может быть воспринят как новый, не размеченный;
- искажение таблицы патриций и загрузочного сектора формально воспринимаются правильно, но не соответствуют действительности.

В первом случае система попытается исправить ошибку автоматическим запуском программы корректировки структуры диска. И если эта процедура не будет прервана Пользователем, структура RAID массива будет распознана системой как структура обычного жесткого диска, что приведет к необратимым разрушениям на диске. Во втором случае система может присвоить сектору MBR начальное значение, в результате исказится значение начального сектора и как следствие этого – исказится значение контрольной суммы первого блока RAID 5. Часто приходится слышать от пользователей жалобы на то, что у них перестал работать RAID, хотя они ничего с ним не делали – только лишь просмотрели диск на другом компьютере.

Тема 9. Построение защищенных экономических информационных систем

9.1. Общие сведения

Internet и информационная безопасность несовместны по самой природе Internet. Она родилась как чисто корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и т.д.), являющиеся, по определению, сетями с ограниченным доступом, но и рядовых пользователей, которые имеют

возможность получить прямой доступ в Internet со своих домашних компьютеров с помощью модемов и телефонной сети общего пользования.

Как известно, чем проще доступ в Сеть, тем хуже ее информационная безопасность, поэтому с полным основанием можно сказать, что изначальная простота доступа в Internet – хуже воровства, так как пользователь может даже и не узнать, что у него были скопированы – файлы и программы, не говоря уже о возможности их порчи и корректировки.

Что же определяет бурный рост Internet, характеризующийся ежегодным удвоением числа пользователей? Ответ прост – "халява", то есть дешевизна программного обеспечения (TCP/IP), легкость и дешевизна доступа в Internet (либо с помощью IP-адреса, либо с помощью провайдера) и ко всем мировым информационным ресурсам.

Платой за пользование Internet является всеобщее снижение информационной безопасности, поэтому для предотвращения несанкционированного доступа к своим компьютерам все корпоративные и ведомственные сети, а также предприятия, использующие технологию intranet, ставят фильтры (fire-wall) между внутренней сетью и Internet, что фактически означает выход из единого адресного пространства. Еще большую безопасность даст отход от протокола TCP/IP и доступ в Internet через шлюзы.

Для решения этих и других вопросов нужно предусмотреть следующее:

1. Во-первых, ликвидировать физическую связь между Internet и корпоративными и ведомственными сетями, сохранив между ними лишь информационную связь через систему World Wide Web.
2. Во-вторых, заменить маршрутизаторы на коммутаторы, исключив обработку в узлах IP-протокола и заменив его на режим трансляции кадров Ethernet, при котором процесс коммутации сводится к простой операции сравнения MAC-адресов.
3. В-третьих, перейти в новое единое адресное пространство на базе физических адресов доступа к среде передачи (MAC-уровень), привязанное к географическому расположению сети, и позволяющее в рамках 48-бит создать адреса для более чем 64 триллионов независимых узлов.

Безопасность данных является одной из главных проблем в Internet. Появляются все новые и новые страшные истории о том, как компьютерные взломщики, использующие все более изощренные приемы, проникают в чужие базы данных. Разумеется, все это не способствует популярности Internet в деловых кругах. Одна только мысль о том, что какие-нибудь хулиганы или, что еще хуже, конкуренты, смогут получить доступ к архивам коммерческих данных, заставляет руководство корпораций отказываться от использования открытых

информационных систем. Специалисты утверждают, что подобные опасения безосновательны, так как у компаний, имеющих доступ и к открытым, и частным сетям, практически равные шансы стать жертвами компьютерного террора.

Каждая организация, имеющая дело с какими бы то ни было ценностями, рано или поздно сталкивается с посягательством на них. Предусмотрительные начинают планировать защиту заранее, непредусмотрительные-после первого крупного “прокола”. Так или иначе, встает вопрос о том, что, как и от кого защищать.

Обычно первая реакция на угрозу-стремление спрятать ценности в недоступное место и приставить к ним охрану. Это относительно несложно, если речь идет о таких ценностях, которые вам долго не понадобятся: убрали и забыли. Куда сложнее, если вам необходимо постоянно работать с ними. Каждое обращение в хранилище за вашими ценностями потребует выполнения особой процедуры, отнимет время и создаст дополнительные неудобства. Такова дилемма безопасности: приходится делать выбор между защищенностью вашего имущества и его доступностью для вас, а значит, и возможностью полезного использования.

Все это справедливо и в отношении информации. Например, база данных, содержащая конфиденциальные сведения, лишь тогда полностью защищена от посягательств, когда она находится на дисках, снятых с компьютера и убранных в охраняемое место. Как только вы установили эти диски в компьютер и начали использовать, появляется сразу несколько каналов, по которым злоумышленник, в принципе, имеет возможность получить к вашим тайнам доступ без вашего ведома. Иными словами, ваша информация либо недоступна для всех, включая и вас, либо не защищена на сто процентов.

Может показаться, что из этой ситуации нет выхода, но информационная безопасность сродни безопасности мореплавания: и то, и другое возможно лишь с учетом некоторой допустимой степени риска.

В области информации дилемма безопасности формулируется следующим образом: следует выбирать между защищенностью системы и ее открытостью. Правильнее, впрочем, говорить не о выборе, а о балансе, так как система, не обладающая свойством открытости, не может быть использована.

В банковской сфере проблема безопасности информации осложняется двумя факторами: во-первых, почти все ценности, с которыми имеет дело банк (кроме наличных денег и еще кое-чего), существуют лишь в виде той или иной информации. Во-вторых, банк не может существовать без связей с внешним миром: без клиентов, корреспондентов и т. п. При этом по внешним связям обязательно передается та самая информация, выражающая собой ценности, с

которыми работает банк (либо сведения об этих ценностях и их движении, которые иногда стоят дороже самих ценностей). Извне приходят документы, по которым банк переводит деньги с одного счета на другой. Вовне банк передает распоряжения о движении средств по корреспондентским счетам, так что открытость банка задана a priori.

Стоит отметить, что эти соображения справедливы по отношению не только к автоматизированным системам, но и к системам, построенным на традиционном бумажном документообороте и не использующим иных связей, кроме курьерской почты. Автоматизация добавила головной боли службам безопасности, а новые тенденции развития сферы банковских услуг, целиком основанные на информационных технологиях, усугубляют проблему.

9.2. Основные технологии построения защищенных экономических информационных систем

Построение защищенных информационных систем связано с решением следующих двух ключевых взаимосвязанных проблем:

- распределение задач администрирования средствами защиты информации между субъектами управления системой;
- использование встроенных механизмов защиты на всех уровнях иерархии системы.

Первая проблема обусловлена иерархическими принципами построения сложной системы – выделяют уровень платформы (операционная система), общесистемный уровень (СУБД и другие системные средства), уровень приложений. Каждый уровень требует своего администрирования. В информационной системе выделяются следующие задачи администрирования:

- системное администрирование (настройка операционной системы, конфигурация и маршрутизация сетевого трафика и т. п.);
- администрирование СУБД и других общесистемных средств;
- администрирование прикладных приложений. При этом на уровне системного администрирования в сложных системах может присутствовать разделение задач по функциональному назначению объектов – рабочие станции, файл-серверы и серверы приложений, серверы доступа к внешним сетям и др.

В иерархии задач администрирования в сложной системе вводятся соответствующие администраторы, каждый из которых отвечает за свою компоненту управления.

В сложных защищенных информационных системах, предназначенных для обработки конфиденциальной информации, выделяется самостоятельная компонента управления – управление информационной безопасностью

системы. Возникает проблема включения данной компоненты в исходную схему администрирования, связанная с тем, что администратором каждого уровня иерархии управления решаются задачи администрирования информационной безопасностью в рамках соответствующего уровня иерархии. Возникают вопросы. Каким образом распределить данные задачи при включении в схему администратора безопасности, какими его функциями делегировать? Какие функции администрирования информационной безопасностью возложить на остальных администраторов системы?

Другая проблема состоит в использовании встроенных средств защиты, распределении задач между встроенными и добавочными средствами защиты. Проблема осложнена тем, что, с одной стороны, невозможно в полной мере доверять встроенным в системы иностранного производства средствам защиты, с другой – нельзя и отказываться от этих механизмов в полном объеме. Иначе для всех видов операционных систем, СУБД и т.д. потребуется разрабатывать добавочные средства защиты, а это невозможно реализовать или приведет к существенному усложнению системы.

Подходы к решению задач

Используются следующие подходы для решения указанных проблем:

1. Все задачи администрирования информационной безопасности системы возложить на администратора безопасности. Это невозможно. Во-первых, задача администрирования становится недопустимо сложной и требует для решения чрезвычайно высокой квалификации администратора безопасности. Во-вторых, для использования такого решения необходимо разграничивать функции администрирования на всех уровнях иерархии системы, что возможно только с реализацией защиты на всех уровнях добавочными средствами.
2. Задачи администрирования информационной безопасности системы распределить между соответствующими администраторами на соответствующих уровнях иерархии. В этом случае не ясны задачи и функции администратора безопасности центрального звена управления информационной безопасности сложной защищенной системы. Обеспечить какую-либо безопасность системы при распределенном решении данной задачи невозможно в принципе.

Наиболее широко используется компромиссное решение рассматриваемой проблемы, реализуемое с использованием метода уровневого контроля целостности списков санкционированных событий.

Суть метода заключается в следующем: все ресурсы системы делятся на уровни (по функциональному признаку). Текущая конфигурация каждого уровня заносится в соответствующий эталонный список, хранящийся в системе

защиты информации и недоступный никому, кроме администратора безопасности, целостность которого контролируется с малым периодом (малая величина списка). Случай обнаружения расхождений текущего и эталонного списка является признаком НСД. В качестве реакции на НСД система защиты информации, помимо восстановления изначальной конфигурации, может выполнить дополнительные реакции. В контролируемых списках могут находиться – списки зарегистрированных пользователей, списки их паролей, списки разрешенных к запуску процессов, настройки операционной системы (например, ключи реестра для MS Windows), собственные настройки системы защиты информации и т.д.

Все настройки системы защиты информации на соответствующих уровнях иерархии задаются соответствующим администратором – системным администратором, администратором приложений, администратором СУБД. Эти администраторы контролируются администратором безопасности, реализованным организационными мероприятиями. По завершении настроек они сохраняются администратором безопасности в эталонных списках системы защиты информации, к которым имеет доступ только администратор безопасности. В процессе функционирования системы данные списки непрерывно контролируются и автоматически восстанавливаются системой защиты информации из эталонных копий в случае обнаружения их искажений.

Компромисс предлагаемого решения состоит в следующем. Администраторы уровней иерархии сами реализуют требования разграничительной политики доступа к ресурсам при непосредственном контроле со стороны администратора безопасности. Система защиты информации обеспечивает невозможность изменения заданных настроек без участия администратора безопасности, в том числе и остальным администраторам системы. Данный подход позволяет разделить задачи администраторов без использования добавочных средств защиты, и в полном объеме использовать встроенные механизмы защиты на всех уровнях иерархии системы.

Основной проблемой остается распределение функций системного администратора и администратора безопасности. Для экономии финансовых средств функции этих администраторов в сложной информационной системе следует совмещать. При этом могут быть в полной мере использованы и механизмы защиты, встроенные в операционную систему. Разделение функций системного администратора и администратора безопасности возможно при условии, что система разграничения доступа к ресурсам на уровне операционной системы будет реализована как добавочное средство защиты. В противном случае системный администратор получит доступ к эталонным спискам событий, хранящимся в системе защиты информации.

Преимуществом данного метода является возможность разделения задач администрирования при максимальном использовании встроенных средств защиты на всех уровнях иерархии сложной системы. Однако появляется другая проблема – проблема доверия встроенным механизмам защиты, которые могут содержать как ошибки, так и закладки, что при определенных условиях позволит злоумышленнику их преодолеть. Решение этой проблемы возможно с помощью рассмотренного ранее метода уровневого контроля целостности списков санкционированных событий, а также метода противодействия ошибкам и закладкам в средствах информационной системы, сущность которого состоит в следующем.

При доступе санкционированного пользователя либо злоумышленника к информации должен произойти ряд событий:

- авторизация пользователя, должен быть запущен некоторый процесс (программа) на исполнение;
- при доступе к информации (файлу, таблице) должны быть проверены права доступа пользователя, при этом собственно операционная система и СУБД должны обладать некоторым набором заданных администраторами свойств и т.д.

Далее система защиты информации создает эталонные копии списков контролируемых событий и осуществляет их непрерывный контроль в процессе функционирования системы. При искажении исходного списка вырабатывается реакция системы защиты информации (например, восстановление исходного списка, выключение компьютера и т.д.).

Если доступ к информации осуществляет санкционированный пользователь и не нарушает своих прав в рамках заданной администратором безопасности разграничительной политики, он получает доступ к информации. В противном случае нарушителю необходимо осуществить какое-либо изменение контролируемого события при доступе к информации. Иначе нарушитель не получит доступ к данным. В этом случае системой защиты информации будет оказано противодействие НСД. Особенностью данного подхода является то, что для системы защиты информации неважно, за счет чего злоумышленником осуществляется попытка модификации контролируемого события при доступе к информации, в том числе и за счет использования им ошибки либо закладки. Фиксируется не причина попытки изменения события, а сам факт подобного изменения.

Применение этого метода позволяет повысить доверие к встроенным механизмам защиты информационной системы и, как следствие, рассматривать их как основные средства защиты при построении сложной защищенной информационной системы.

Преимуществом рассмотренных принципов реализации системы защиты информации является ее реализация на прикладном уровне, т. е. практически инвариантна к типу используемых в информационных системах операционной системе, СУБД и приложений, и ее применение практически не приводит к снижению надежности функционирования системы.

9.3. Информационная безопасность и информационные технологии

На раннем этапе автоматизации внедрение банковских систем (и вообще средств автоматизации банковской деятельности) не повышало открытость банка. Общение с внешним миром, как и прежде, шло через операционистов и курьеров, поэтому дополнительная угроза безопасности информации проистекала лишь от возможных злоупотреблений со стороны работавших в самом банке специалистов по информационным технологиям.

Положение изменилось после того, как на рынке финансовых услуг стали появляться продукты, само возникновение которых было немыслимо без информационных технологий. В первую очередь – это пластиковые карточки. Пока обслуживание по карточкам шло в режиме голосовой авторизации, открытость информационной системы банка повышалась незначительно, но затем появились банкоматы, POS-терминалы, другие устройства самообслуживания-то есть средства, принадлежащие к информационной системе банка, но расположенные вне ее и доступные посторонним для банка лицам.

Повысившаяся открытость системы потребовала специальных мер для контроля и регулирования обмена информацией: дополнительных средств идентификации и аутентификации лиц, которые запрашивают доступ к системе (PIN-код, информация о клиенте на магнитной полосе или в памяти микросхемы карточки, шифрование данных, контрольные числа и другие средства защиты карточек), средств криптозащиты информации в каналах связи и т. д.

Еще больший сдвиг баланса "защищенность-открытость" в сторону последней связан с телекоммуникациями. Системы электронных расчетов между банками защитить относительно несложно, так как субъектами электронного обмена информацией выступают сами банки. Тем не менее, там, где защите не уделялось необходимое внимание, результаты были вполне предсказуемы. Наиболее кричащий пример-к сожалению, наша страна. Использование крайне примитивных средств защиты телекоммуникаций в 1992 г. привело к огромным потерям на фальшивых авизо.

Общая тенденция развития телекоммуникаций и массового распространения вычислительной техники привела в конце концов к тому, что на рынке банковских услуг во всем мире появились новые, чисто телекоммуникационные продукты, и в первую очередь системы Home Banking (отечественный аналог-"клиент-банк"). Это потребовало обеспечить клиентам круглосуточный доступ к автоматизированной банковской системе для проведения операций, причем полномочия на совершение банковских транзакций получил непосредственно клиент. Степень открытости информационной системы банка возросла почти до предела. Соответственно, требуются особые, специальные меры для того, чтобы столь же значительно не упала ее защищенность.

Наконец, грянула эпоха "информационной супермагистрали": взрывообразное развитие сети Internet и связанных с нею услуг. Вместе с новыми возможностями эта сеть принесла и новые опасности. Казалось бы, какая разница, каким образом клиент связывается с банком: по коммутируемой линии, приходящей на модемный пул банковского узла связи, или по IP-протоколу через Internet? Однако в первом случае максимально возможное количество подключений ограничивается техническими характеристиками модемного пула, во втором же-возможностями Internet, которые могут быть существенно выше. Кроме того, сетевой адрес банка, в принципе, общедоступен, тогда как телефонные номера модемного пула могут сообщаться лишь заинтересованным лицам. Соответственно, открытость банка, чья информационная система связана с Internet, значительно выше, чем в первом случае. Все это вызывает необходимость пересмотра подходов к обеспечению информационной безопасности банка. Подключаясь к Internet, следует заново провести анализ риска и составить план защиты информационной системы, а также конкретный план ликвидации последствий, возникающих в случае тех или иных нарушений конфиденциальности, сохранности и доступности информации.

На первый взгляд, для нашей страны проблема информационной безопасности банка не столь остра: до Internet ли нам, если в большинстве банков стоят системы второго поколения, работающие в технологии "файл-сервер". К сожалению, и у нас уже зарегистрированы "компьютерные кражи". Положение осложняется двумя проблемами. Прежде всего, как показывает опыт общения с представителями банковских служб безопасности, и в руководстве, и среди персонала этих служб преобладают бывшие оперативные сотрудники органов внутренних дел или госбезопасности. Они обладают высокой квалификацией в своей области, но в большинстве своем слабо знакомы с информационными технологиями. Специалистов по информационной безопасности в нашей стране вообще крайне мало, потому что массовой эта профессия становится только сейчас.

Вторая проблема связана с тем, что в очень многих банках безопасность автоматизированной банковской системы не анализируется и не обеспечивается всерьез. Очень мало где имеется тот необходимый набор организационных документов (анализ риска, план защиты и план ликвидации последствий), о котором говорилось выше. Более того, безопасность информации сплошь и рядом просто не может быть обеспечена в рамках имеющейся в банке автоматизированной системы и принятых правил работы с ней.

Тем не менее, наши банки уделяют информационным технологиям много внимания, и достаточно быстро усваивают новое. Сеть Internet и финансовые продукты, связанные с ней, войдут в жизнь банков России быстрее, чем это предполагают скептики, поэтому уже сейчас необходимо озаботиться вопросами информационной безопасности на другом, более профессиональном уровне, чем это делалось до сих пор.

Некоторые рекомендации

1. Необходим комплексный подход к информационной безопасности.

   Информационная безопасность должна рассматриваться как составная часть общей безопасности банка-причем как важная и неотъемлемая ее часть. Разработка концепции информационной безопасности должна обязательно проходить при участии управления безопасности банка. В этой концепции следует предусматривать не только меры, связанные с информационными технологиями (криптозащиту, программные средства администрирования прав пользователей, их идентификации и аутентификации, "брандмауэры" для защиты входов-выходов сети и т. п.), но и меры административного и технического характера, включая жесткие процедуры контроля физического доступа к автоматизированной банковской системе, а также средства синхронизации и обмена данными между модулем администрирования безопасности банковской системы и системой охраны.
2. Необходимо участие сотрудников управления безопасности на этапе выбора-приобретения-разработки автоматизированной банковской системы.

   Это участие не должно сводиться к проверке фирмы-поставщика. Управление безопасности должно контролировать наличие надлежащих средств разграничения доступа к информации в приобретаемой системе.

Отсюда следует третья практическая рекомендация: относиться сугубо осторожно к любым сертификатам и отдавать предпочтение тем продуктам, надежность которых подтверждена успешным использованием в мировой финансовой практике. Безопасность в сети Internet.

9.4. Средства защиты информации

Одним из наиболее распространенных механизмов защиты от интернетовских бандитов – "хакеров" является применение межсетевых экранов – брэндмауэров (firewalls).

Стоит отметить, что в следствии непрофессионализма администраторов и недостатков некоторых типов брэндмауэров порядка 30% взломов совершается после установки защитных систем.

Не следует думать, что все изложенное выше – "заморские диковины". Всем, кто еще не уверен, что Россия уверенно догоняет другие страны по числу взломов серверов и локальных сетей и принесенному ими ущербу, следует познакомиться с тематической подборкой материалов российской прессы и материалами Hack Zone (Zhurnal.Ru).

Не смотря на кажущийся правовой хаос в расматриваемой области, любая деятельность по разработке, продаже и использованию средств защиты информации регулируется множеством законодательных и нормативных документов, а все используемые системы подлежат обязательной сертификации Государственой Технической Комисией при президенте России.

Технология работы в глобальных сетях Solstice FireWall-1

В настоящее время вопросам безопасности данных в распределенных компьютерных системах уделяется очень большое внимание. Разработано множество средств для обеспечения информационной безопасности, предназначенных для использования на различных компьютерах с разными ОС. В качестве одного из направлений можно выделить межсетевые экраны (firewalls), призванные контролировать доступ к информации со стороны пользователей внешних сетей.

В настоящем документе рассматриваются основные понятия экранирующих систем, а также требования, предъявляемые к ним. На примере пакета Solstice FireWall-1 рассматривается несколько типичных случаев использования таких систем, особенно применительно к вопросам обеспечения безопасности Internet-подключений. Рассмотрено также несколько уникальных особенностей Solstice FireWall-1, позволяющих говорить о его лидерстве в данном классе приложений.

Назначение экранирующих систем и требования к ним

Проблема межсетевого экранирования формулируется следующим образом. Пусть имеется две информационные системы или два множества информационных систем. Экран (firewall) – это средство разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве.

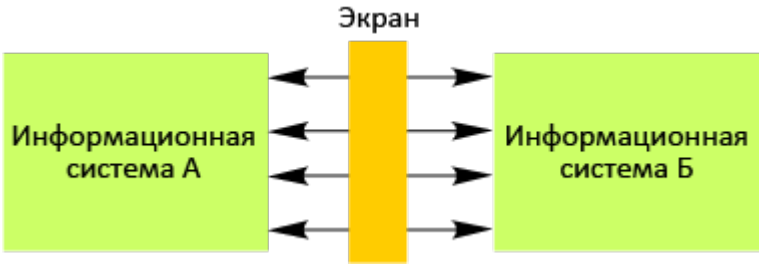


Рисунок 9.1 – Экран FireWall

Экран выполняет свои функции, контролируя все информационные потоки между этими двумя множествами информационных систем, работая как некоторая "информационная мембрана". В этом смысле экран можно представлять себе как набор фильтров, анализирующих проходящую через них информацию и, на основе заложенных в них алгоритмов, принимающих решение: пропустить ли эту информацию или отказать в ее пересылке. Кроме того, такая система может выполнять регистрацию событий, связанных с процессами разграничения доступа, в частности, фиксировать все "незаконные" попытки доступа к информации и, дополнительно, сигнализировать о ситуациях, требующих немедленной реакции, то есть поднимать тревогу.

Обычно экранирующие системы делают несимметричными. Для экранов определяются понятия "внутри" и "снаружи", и задача экрана состоит в защите внутренней сети от "потенциально враждебного" окружения. Важнейшим примером потенциально враждебной внешней сети является Internet.

Рассмотрим более подробно, какие проблемы возникают при построении экранирующих систем. При этом мы будем рассматривать не только проблему безопасного подключения к Internet, но и разграничение доступа внутри корпоративной сети организации.

1. Первое, очевидное требование к таким системам, это обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи.
2. Во-вторых, экранирующая система должна обладать мощными и гибкими средствами управления для простого и полного воплощения в жизнь политики безопасности организации и, кроме того, для обеспечения простой реконфигурации системы при изменении структуры сети.
3. В-третьих, экранирующая система должна работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий.
4. В-четвертых, экранирующая система должна работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик в "пиковых" режимах. Это необходимо для того, чтобы firewall нельзя было, образно говоря, "забросать" большим количеством вызовов, которые привели бы к нарушению ее работы.

5. Пятое. Система обеспечения безопасности должна быть сама надежно защищена от любых несанкционированных воздействий, поскольку она является ключом к конфиденциальной информации в организации.
6. Шестое. В идеале, если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах, система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики безопасности.
7. Седьмое. Система Firewall должна иметь средства авторизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки, и в процессе работы им, тем немение, требуется доступ, по крайней мере, к некоторым ресурсам внутренней компьютерной сети организации. Система должна уметь надежно распознавать таких пользователей и предоставлять им необходимый доступ к информации.

Структура системы solstice firewall-1

Классическим примером, на котором хотелось бы проиллюстрировать все вышеизложенные принципы, является программный комплекс Solstice FireWall-1 компании Sun Microsystems. Данный пакет неоднократно отмечался наградами на выставках и конкурсах. Он обладает многими полезными особенностями, выделяющими его среди продуктов аналогичного назначения.

Рассмотрим основные компоненты Solstice FireWall-1 и функции, которые они реализуют (см. рисунок 9.2).

Центральным для системы FireWall-1 является модуль управления всем комплексом. С этим модулем работает администратор безопасности сети. Следует отметить, что продуманность и удобство графического интерфейса модуля управления отмечалось во многих независимых обзорах, посвященных продуктам данного класса.

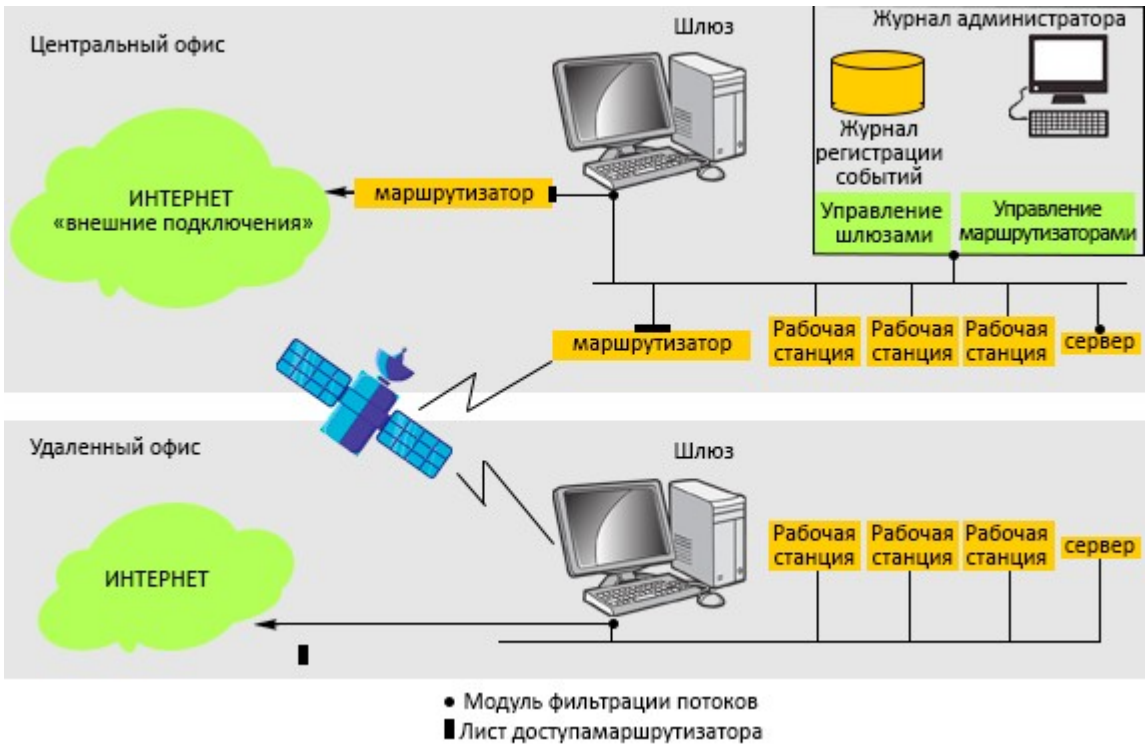


Рисунок 9.2 – Основные компоненты Solstice FireWall-1

Администратору безопасности сети для конфигурирования комплекса FireWall-1 необходимо выполнить следующий ряд действий:

- Определить объекты, участвующие в процессе обработки информации. Здесь имеются в виду пользователи и группы пользователей, компьютеры и их группы, маршрутизаторы и различные подсети локальной сети организации.
- Описать сетевые протоколы и сервисы, с которыми будут работать приложения. Впрочем, обычно достаточным оказывается набор из более чем 40 описаний, поставляемых с системой FireWall-1.
- Далее, с помощью введенных понятий описывается политика разграничения доступа в следующих терминах: "Группе пользователей А разрешен доступ к ресурсу Б с помощью сервиса или протокола С, но об этом необходимо сделать пометку в регистрационном журнале". Совокупность таких записей компилируется в исполнимую форму блоком управления и далее передается на исполнение в модули фильтрации.

Модули фильтрации могут располагаться на компьютерах – шлюзах или выделенных серверах – или в маршрутизаторах как часть конфигурационной информации. В настоящее время поддерживаются следующие два типа маршрутизаторов: Cisco IOS 9.x, 10.x, а также BayNetworks (Wellfleet) OS v.8.

Модули фильтрации просматривают все пакеты, поступающие на сетевые интерфейсы, и, в зависимости от заданных правил, пропускают или отбрасывают эти пакеты, с соответствующей записью в регистрационном журнале. Следует отметить, что эти модули, работая непосредственно с

драйверами сетевых интерфейсов, обрабатывают весь поток данных, располагая полной информацией о передаваемых пакетах.

9.5. Пример реализации политики безопасности

Рассмотрим процесс практической реализации политики безопасности организации с помощью программного пакета FireWall-1. (см. рисунок 9.3).

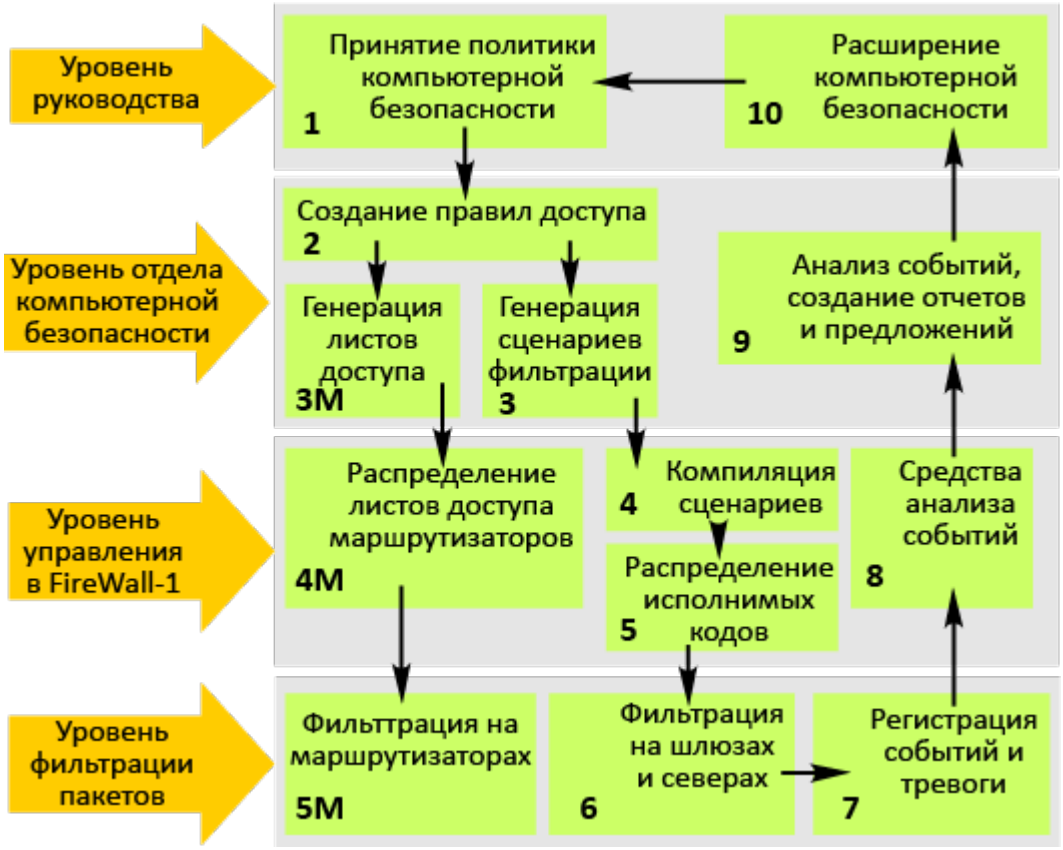


Рисунок 9.3 – Реализация политики безопасности FireWall

1. Прежде всего, как уже отмечалось, разрабатываются и утверждаются на уровне руководства организации правила политики безопасности.
2. После утверждения эти правила надо воплотить в жизнь. Для этого их нужно перевести в структуру типа откуда, куда и каким способом доступ разрешен или, наоборот, запрещен. Такие структуры, как мы уже знаем, легко переносятся в базы правил системы FireWall-1.
3. Далее, на основе этой базы правил формируются списки доступа для маршрутизаторов и сценарии работы фильтров на сетевых шлюзах. Списки и сценарии далее переносятся на физические компоненты сети, после чего правила политики безопасности "вступают в силу".
4. В процессе работы фильтры пакетов на шлюзах и серверах генерируют записи обо всех событиях, которые им приказали отслеживать, а, также, запускают механизмы "тревоги", требующие от администратора немедленной реакции.

5. На основе анализа записей, сделанных системой, отдел компьютерной безопасности организации может разрабатывать предложения по изменению и дальнейшему развитию политики безопасности.

Рассмотрим простой пример реализации следующих правил:

1. Из локальных сетей подразделений, возможно удаленных, разрешается связь с любой локальной сетью организации после аутентификации, например, по UNIX-паролю.
2. Всем запрещается доступ к сети финансового департамента, за исключением генерального директора и директора этого департамента.
3. Из Internet разрешается только отправлять и получать почту. Обо всех других попытках связи необходимо делать подробную запись.

Все эти правила естественным образом представляются средствами графического интерфейса Редактора Правил FireWall-1 (см. рисунок 9.4).

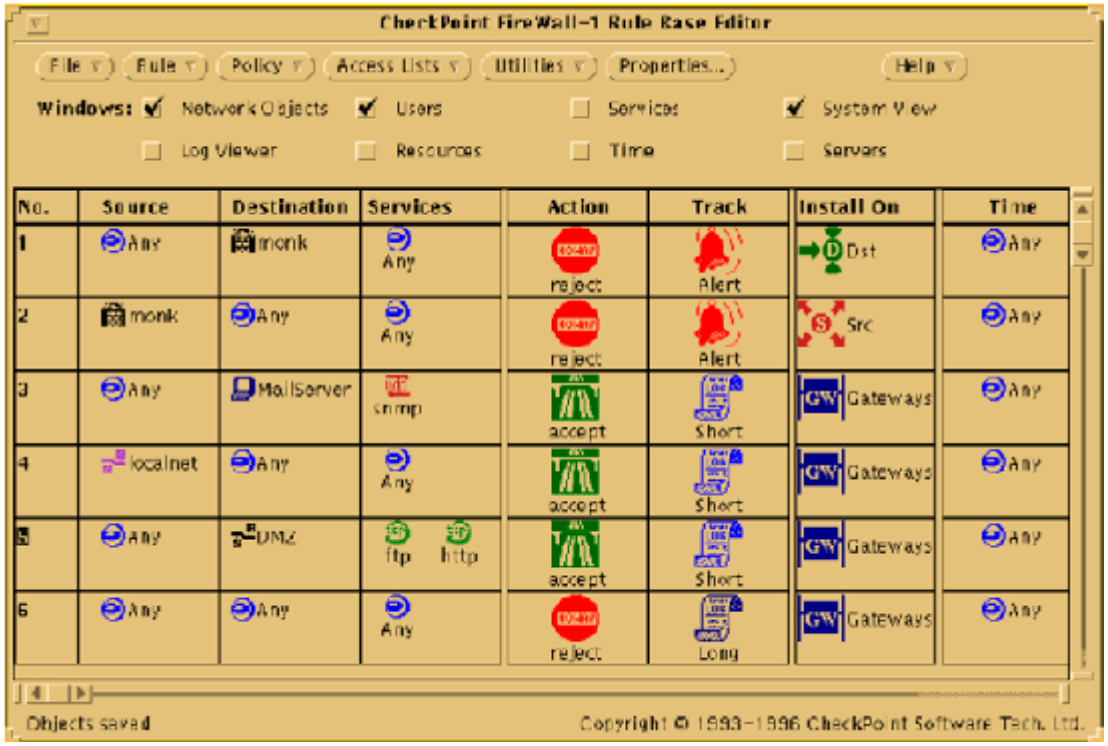


Рисунок 9.4 – Графический интерфейс Редактора Правил FireWall-1

После загрузки правил, FireWall-1 для каждого пакета, передаваемого по сети, последовательно просматривает список правил до нахождения элемента, соответствующего текущему случаю.

Важным моментом является защита системы, на которой размещен административно-конфигурационный модуль FireWall-1. Рекомендуется запретить средствами FireWall-1 все виды доступа к данной машине, или по крайней мере строго ограничить список пользователей, которым это разрешено, а также принять меры по физическому ограничению доступа и по защите обычными средствами ОС UNIX.

Управление системой firewall-1

На рисунке 9.5 показаны основные элементы управления системой FireWall-1.

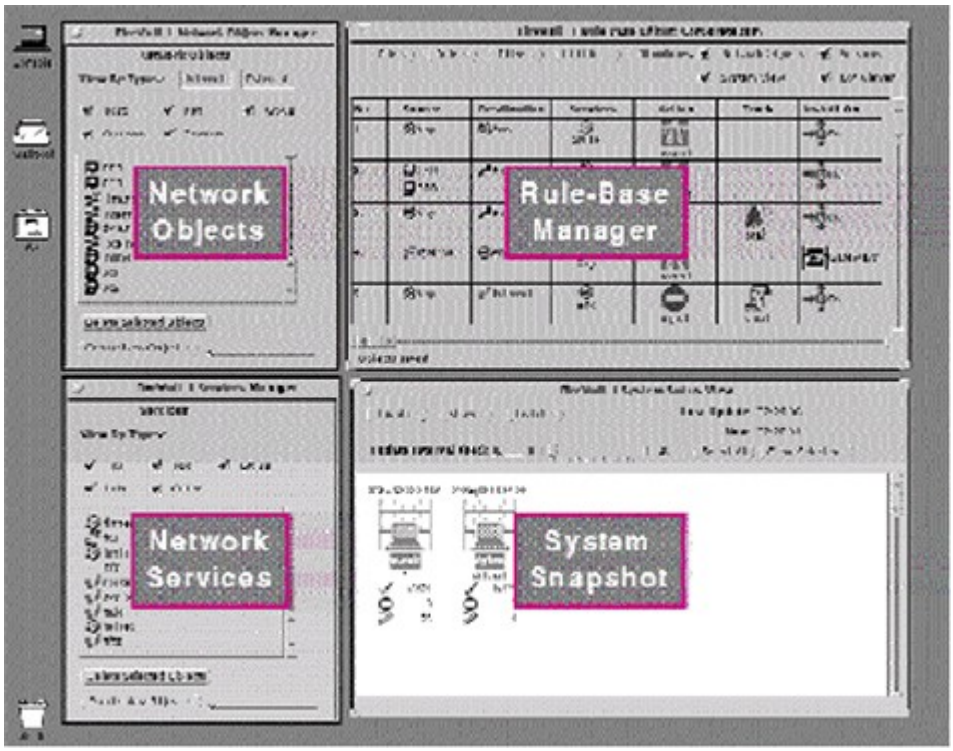


Рисунок 9.5 – Основные элементы управления системой FireWall-1

Слева расположены редакторы баз данных об объектах, существующих в сети и о протоколах или сервисах, с помощью которых происходит обмен информацией. Справа вверху показан редактор правил доступа.

Справа внизу располагается интерфейс контроля текущего состояния системы, в котором для всех объектов, которые занес туда администратор, отображаются данные о количестве разрешенных коммуникаций (галочки), о количестве отвергнутых связей (знак "кирпич") и о количестве коммуникаций с регистрацией (иконка карандаш). Кирпичная стена за символом объекта (компьютера) означает, что на нем установлен модуль фильтрации системы FireWall-1.

Рассмотрим теперь случай, когда первоначальная конфигурация сети меняется, а вместе с ней меняется и политика безопасности.

Пусть мы решили установить у себя в организации несколько общедоступных серверов для предоставления информационных услуг. Это могут быть, например, серверы World Wide Web, FTP или другие информационные серверы. Поскольку такие системы обособлены от работы всей остальной сети организации, для них часто выделяют свою собственную подсеть, имеющую выход в Internet через шлюз (см. рисунок 9.6).

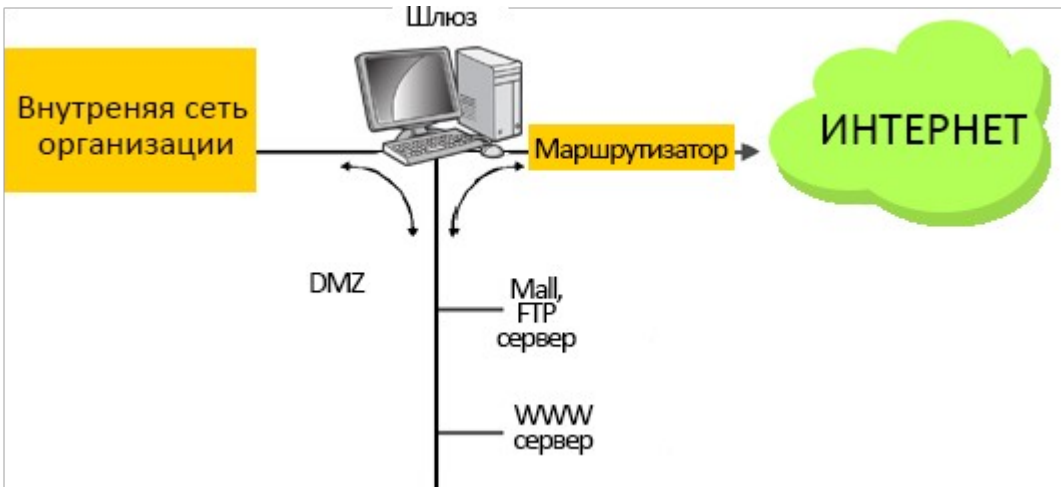


Рисунок 9.6 – Схема шлюза Internet

Поскольку в предыдущем примере локальная сеть была уже защищена, то все, что нам надо сделать, это просто разрешить соответствующий доступ в выделенную подсеть. Это делается с помощью одной дополнительной строки в редакторе правил, которая здесь показана. Такая ситуация является типичной при изменении конфигурации FireWall-1. Обычно для этого требуется изменение одной или небольшого числа строк в наборе правил доступа, что, несомненно, иллюстрирует мощь средств конфигурирования и общую продуманность архитектуры FireWall-1.

Аутенфикация пользователей при работе с ftp

Solstice FireWall-1 позволяет администратору установить различные режимы работы с интерактивными сервисами FTP и telnet для различных пользователей и групп пользователей. При установленном режиме аутентификации, FireWall-1 заменяет стандартные FTP и telnet демоны UNIX на свои собственные, располагая их на шлюзе, закрытом с помощью модулей фильтрации пакетов. Пользователь, желающий начать интерактивную сессию по FTP или telnet (это должен быть разрешенный пользователь и в разрешенное для него время), может сделать это только через вход на такой шлюз, где и выполняется вся процедура аутентификации. Она задается при описании пользователей или групп пользователей и может проводиться следующими способами:

- Unix-пароль;
- программа S/Key генерации одноразовых паролей;
- карточки SecurID с аппаратной генерацией одноразовых паролей.

Гибкие алгоритмы фильтрации udp-пакетов, динамическое экранирование

UDP-протоколы, входящие в состав набора TCP/IP, представляют собой особую проблему для обеспечения безопасности. С одной стороны на их основе создано множество приложений. С другой стороны, все они являются протоколами "без состояния", что приводит к отсутствию различий между запросом и ответом, приходящим извне защищаемой сети.

Пакет FireWall-1 решает эту проблему созданием контекста соединений поверх UDP сессий, запоминая параметры запросов. Пропускаются назад только ответы внешних серверов на высланные запросы, которые однозначно отличаются от любых других UDP-пакетов (читай: незаконных запросов), поскольку их параметры хранятся в памяти FireWall-1.

Следует отметить, что данная возможность присутствует в весьма немногих программах экранирования, распространяемых в настоящий момент.

Заметим также, что подобные механизмы задействуются для приложений, использующих RPC, и для FTP сеансов. Здесь возникают аналогичные проблемы, связанные с динамическим выделением портов для сеансов связи, которые FireWall-1 отслеживает аналогичным образом, запоминая необходимую информацию при запросах на такие сеансы и обеспечивая только "законный" обмен данными.

Данные возможности пакета Solstice FireWall-1 резко выделяют его среди всех остальных межсетевых экранов. Впервые проблема обеспечения безопасности решена для всех без исключения сервисов и протоколов, существующих в Internet.

Система Solstice FireWall-1 имеет собственный встроенный обьектно-ориентированный язык программирования, применяемый для описания поведения модулей – Фильтров системы. Собственно говоря, результатом работы графического интерфейса администратора системы является сгенерированный сценарий работы именно на этом внутреннем языке. Он не сложен для понимания, что допускает непосредственное программирование на нем. Однако на практике данная возможность почти не используется, поскольку графический интерфейс системы и так позволяет сделать практически все, что нужно.

FireWall-1 полностью прозрачен для конечных пользователей. Еще одним замечательным свойством системы Solstice FireWall-1 является очень высокая скорость работы. Фактически модули системы работают на сетевых скоростях передачи информации, что обусловлено компиляцией сгенерированных сценариев работы перед подключением их непосредственно в процесс фильтрации.

Solstice FireWall-1 – эффективное средство защиты корпоративных сетей и их сегментов от внешних угроз, а также от несанкционированных взаимодействий локальных пользователей с внешними системами.

Solstice FireWall-1 обеспечивает высокоуровневую поддержку политики безопасности организации по отношению ко всем протоколам семейства TCP/IP.

Solstice FireWall-1 характеризуется прозрачностью для легальных пользователей и высокой эффективностью.

По совокупности технических и стоимостных характеристик Solstice FireWall-1 занимает лидирующую позицию среди межсетевых экранов.

Законодательный уровень

В настоящее время наиболее подробным законодательным документом в области информационной безопасности является Уголовный кодекс, точнее говоря, его новая редакция, вступившая в силу в мае 1996 года.

В разделе IX ("Преступления против общественной безопасности") имеется глава 28 – "Преступления в сфере компьютерной информации". Она содержит три статьи – 272 ("Неправомерный доступ к компьютерной информации"), 273 ("Создание, использование и распространение вредоносных программ для ЭВМ") и 274 – "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети".

Уголовный кодекс стоит на страже всех аспектов информационной безопасности – доступности, целостности, конфиденциальности, предусматривая наказания за "уничтожение, блокирование, модификацию и копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети".

Весьма энергичную работу в области современных информационных технологий проводит Государственная техническая комиссия (Гостехкомиссия) при Президенте Российской Федерации. В рамках серии руководящих документов (РД) Гостехкомиссии подготовлен проект РД, устанавливающий классификацию межсетевых экранов (firewalls, или брандмауэров) по уровню обеспечения защищенности от несанкционированного доступа (НСД). Это принципиально важный документ, позволяющий упорядочить использование защитных средств, необходимых для реализации технологии Intranet.

9.6. Разработка сетевых аспектов политики безопасности

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

- невозможность миновать защитные средства;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;

- разнообразие защитных средств;
- простота и управляемость информационной системы;
- обеспечение всеобщей поддержки мер безопасности.

Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Применительно к межсетевым экранам данный принцип означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через экран. Не должно быть “тайных” модемных входов или тестовых линий, идущих в обход экрана.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

1. Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.
2. Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.
3. Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.
4. Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом и, как последний рубеж, – протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.
5. Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение

разнообразными и, по возможности, несовместимыми между собой навыками (например умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

6. Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.
7. Последний принцип – всеобщая поддержка мер безопасности – носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Анализ рисков – важнейший этап выработки политики безопасности. При оценке рисков, которым подвержены Intranet-системы, нужно учитывать следующие обстоятельства:

- новые угрозы по отношению к старым сервисам, вытекающие из возможности пассивного или активного прослушивания сети. Пассивное прослушивание означает чтение сетевого трафика, а активное – его изменение (кражу, дублирование или модификацию передаваемых данных). Например, аутентификация удаленного клиента с помощью пароля многократного использования не может считаться надежной в сетевой среде, независимо от длины пароля;
- новые (сетевые) сервисы и ассоциированные с ними угрозы.

Как правило, в Intranet-системах следует придерживаться принципа “все, что не разрешено, запрещено”, поскольку “лишний” сетевой сервис может предоставить канал проникновения в корпоративную систему. В принципе, ту же мысль выражает положение “все непонятное опасно”.

Процедурные меры

В общем и целом Intranet-технология не предъявляет каких-либо специфических требований к мерам процедурного уровня. На наш взгляд, отдельного рассмотрения заслуживают лишь два обстоятельства:

- описание должностей, связанных с определением, наполнением и поддержанием корпоративной гипертекстовой структуры официальных документов;
- поддержка жизненного цикла информации, наполняющей Intranet.

При описании должностей целесообразно исходить из аналогии между Intranet и издательством. В издательстве существует директор, определяющий общую направленность деятельности. В Intranet ему соответствует Web-администратор, решающий, какая корпоративная информация должна присутствовать на Web-сервере и как следует структурировать дерево (точнее, граф) HTML-документов.

В многопрофильных издательствах существуют редакции, занимающиеся конкретными направлениями (математические книги, книги для детей и т.п.). Аналогично, в Intranet целесообразно выделить должность публикатора, ведающего появлением документов отдельных подразделений и определяющего перечень и характер публикаций.

У каждой книги есть титульный редактор, отвечающий перед издательством за свою работу. В Intranet редакторы занимаются вставкой документов в корпоративное дерево, их коррекцией и удалением. В больших организациях “слой” публикатор/редактор может состоять из нескольких уровней.

Наконец, и в издательстве, и в Intranet должны быть авторы, создающие документы. Подчеркнем, что они не должны иметь прав на модификацию корпоративного дерева и отдельных документов. Их дело – передать свой труд редактору.

Кроме официальных, корпоративных, в Intranet могут присутствовать групповые и личные документы, порядок работы с которыми (роли, права доступа) определяется, соответственно, групповыми и личными интересами.

Переходя к вопросам поддержки жизненного цикла Intranet-информации, напомним о необходимости использования средств конфигурационного управления. Важное достоинство Intranet-технологии состоит в том, что основные операции конфигурационного управления – внесение изменений (создание новой версии) и извлечение старой версии документа – естественным образом вписываются в рамки Web-интерфейса. Те, для кого это необходимо, могут работать с деревом всех версий всех документов, подмножеством которого является дерево самых свежих версий.

Управление доступом путем фильтрации информации

Мы переходим к рассмотрению мер программно-технического уровня, направленных на обеспечение информационной безопасности систем, построенных в технологии Intranet. На первое место среди таких мер мы поставим межсетевые экраны – средство разграничения доступа, служащее для защиты от внешних угроз и от угроз со стороны пользователей других сегментов корпоративных сетей.

Отметим, что бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС – это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для получения нелегальных привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений (как и врач, не ведающий всех побочных воздействий рекомендуемых лекарств). Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.).

Как указывалось выше, единственный перспективный путь связан с разработкой специализированных защитных средств, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран – это полупроницаемая мембрана, которая располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети) и контролирует все информационные потоки во внутреннюю сеть и из нее (см. рисунок 9.7). Контроль информационных потоков состоит в их фильтрации, то есть в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.

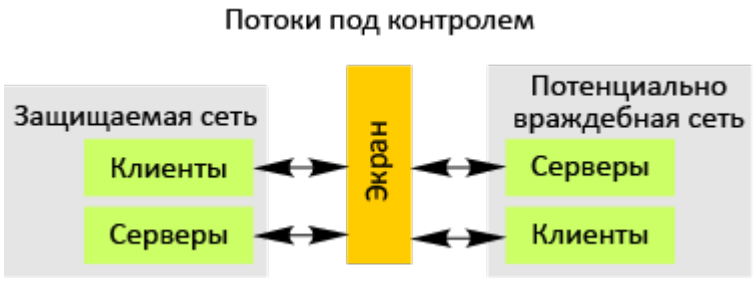


Рисунок 9.7 – Межсетевой экран как средство контроля информационных потоков

Целесообразно разделить случаи, когда экран устанавливается на границе с внешней (обычно общедоступной) сетью или на границе между сегментами одной корпоративной сети. Соответственно, мы будет говорить о внешнем и внутреннем межсетевых экранах.

Как правило, при общении с внешними сетями используется исключительно семейство протоколов TCP/IP. Поэтому внешний межсетевой экран должен учитывать специфику этих протоколов. Для внутренних экранов ситуация сложнее, здесь следует принимать во внимание помимо TCP/IP по крайней мере протоколы SPX/IPX, применяемые в сетях Novell NetWare. Иными словами, от внутренних экранов нередко требуется многопротокольность.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, является, скорее, исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования (см. рисунок 9.8). В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

Рисунок 9.8 – Экранирование корпоративной сети, состоящей из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. Межсетевые экраны также целесообразно классифицировать по тому, на каком уровне производится фильтрация – канальном, сетевом, транспортном или прикладном. Соответственно, можно говорить об экранирующих концентраторах (уровень 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7). Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

При принятии решения “пропустить/не пропустить”, межсетевые экраны могут использовать не только информацию, содержащуюся в фильтруемых потоках, но и данные, полученные из окружения, например текущее время.

Таким образом, возможности межсетевого экрана непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует экран, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее экран может быть сконфигурирован. В то же время фильтрация на каждом из перечисленных выше уровней обладает своими достоинствами, такими как дешевизна, высокая эффективность или прозрачность для пользователей. В силу этой, а также некоторых других причин, в большинстве случаев используются смешанные конфигурации, в которых объединены разнотипные экраны. Наиболее типичным является сочетание экранирующих маршрутизаторов и прикладного экрана.

Приведенная конфигурация называется экранирующей подсетью. Как правило, сервисы, которые организация предоставляет для внешнего применения (например “представительский” Web-сервер), целесообразно выносить как раз в экранирующую подсеть.

Помимо выразительных возможностей и допустимого количества правил качество межсетевого экрана определяется еще двумя очень важными характеристиками – простотой применения и собственной защищенностью. В плане простоты использования первостепенное значение имеют наглядный интерфейс при задании правил фильтрации и возможность централизованного администрирования составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил фильтрации и проверки набора правил на непротиворечивость. Важен и централизованный сбор и анализ регистрационной информации, а также

получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. При выполнении централизованного администрирования следует еще позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность.

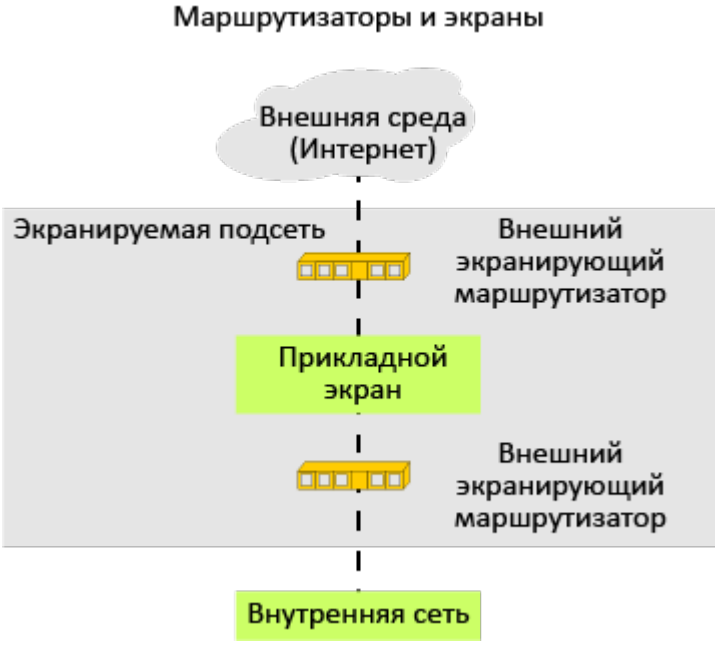


Рисунок 9.9 – Сочетание экранирующих маршрутизаторов и прикладного экрана

Природа экранирования (фильтрации), как механизма безопасности, очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Так, прикладной экран может осуществлять действия от имени субъектов внутренней сети, в результате чего из внешней сети кажется, что имеет место взаимодействие исключительно с межсетевым экраном (см. рисунок 9.10). При таком подходе топология внутренней сети скрыта от внешних пользователей, поэтому задача злоумышленника существенно усложняется.

Рисунок 9.10 – Истинные и кажущиеся информационные потоки

Более общим методом сокрытия информации о топологии защищаемой сети является трансляция “внутренних” сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый видит лишь то, что ему положено.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, в частности таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация баз данных.

9.7. Безопасность программной среды

Идея сетей с так называемыми активными агентами, когда между компьютерами передаются не только пассивные, но и активные исполняемые данные (то есть программы), разумеется, не нова. Первоначально цель состояла в том, чтобы уменьшить сетевой трафик, выполняя основную часть обработки там, где располагаются данные (приближение программ к данным). На практике это означало перемещение программ на серверы. Классический пример реализации подобного подхода – это хранимые процедуры в реляционных СУБД.

Для Web-серверов аналогом хранимых процедур являются программы, обслуживающие общий шлюзовый интерфейс (Common Gateway Interface – CGI).

CGI-процедуры располагаются на серверах и обычно используются для динамического порождения HTML-документов. Политика безопасности организации и процедурные меры должны определять, кто имеет право помещать на сервер CGI-процедуры. Жесткий контроль здесь необходим, поскольку выполнение сервером некорректной программы может привести к сколь угодно тяжелым последствиям. Разумная мера технического характера состоит в минимизации привилегий пользователя, от имени которого выполняется Web-сервер.

В технологии Intranet, если заботиться о качестве и выразительной силе пользовательского интерфейса, возникает нужда в перемещении программ с Web-серверов на клиентские компьютеры – для создания анимации, выполнения семантического контроля при вводе данных и т.д. Вообще, активные агенты – неотъемлемая часть технологии Intranet.

В каком бы направлении ни перемещались программы по сети, эти действия представляют повышенную опасность, т.к. программа, полученная из ненадежного источника, может содержать непреднамеренно внесенные ошибки или целенаправленно созданный зловредный код. Такая программа потенциально угрожает всем основным аспектам информационной безопасности:

- доступности (программа может поглотить все наличные ресурсы);
- целостности (программа может удалить или повредить данные);
- конфиденциальности (программа может прочитать данные и передать их по сети).

Java

Проблему ненадежных программ осознавали давно, но, пожалуй, только в рамках системы программирования Java впервые предложена целостная концепция ее решения.

Java предлагает три оборонительных рубежа:

- надежность языка;
- контроль при получении программ;
- контроль при выполнении программ.

Впрочем, существует еще одно, очень важное средство обеспечения информационной безопасности – беспрецедентная открытость Java-системы. Исходные тексты Java-компилятора и интерпретатора доступны для проверки, поэтому велика вероятность, что ошибки и недочеты первыми будут обнаруживать честные специалисты, а не злоумышленники.

В концептуальном плане наибольшие трудности представляет контролируемое выполнение программ, загруженных по сети. Прежде всего, необходимо определить, какие действия считаются для таких программ допустимыми. Если исходить из того, что Java – это язык для написания клиентских частей приложений, одним из основных требований к которым является мобильность, загруженная программа может обслуживать только пользовательский интерфейс и осуществлять сетевое взаимодействие с сервером. Программа не может работать с файлами хотя бы потому, что на Java-терминале их, возможно, не будет. Более содержательные действия должны производиться на серверной стороне или осуществляться программами, локальными для клиентской системы.

Safe-Tcl

Интересный подход предлагают специалисты компании Sun Microsystems для обеспечения безопасного выполнения командных файлов. Речь идет о среде Safe-Tcl (Tool Comman Language, инструментальный командный язык). Sun предложила так называемую ячеечную модель интерпретации командных

файлов. Существует главный интерпретатор, которому доступны все возможности языка.

Если в процессе работы приложения необходимо выполнить сомнительный командный файл, порождается подчиненный командный интерпретатор, обладающий ограниченной функциональностью (например, из него могут быть удалены средства работы с файлами и сетевые возможности). В результате потенциально опасные программы оказываются заключенными в ячейки, защищающие пользовательские системы от враждебных действий. Для выполнения действий, которые считаются привилегированными, подчиненный интерпретатор может обращаться с запросами к главному. Здесь, очевидно, просматривается аналогия с разделением адресных пространств операционной системы и пользовательских процессов и использованием последними системных вызовов. Подобная модель уже около 30 лет является стандартной для многопользовательских ОС.

Защита web-серверов

Наряду с обеспечением безопасности программной среды (см. предыдущий раздел), важнейшим будет вопрос о разграничении доступа к объектам Web-сервиса. Для решения этого вопроса необходимо уяснить, что является объектом, как идентифицируются субъекты и какая модель управления доступом – принудительная или произвольная – применяется.

В Web-серверах объектами доступа выступают универсальные локаторы ресурсов (URL – Uniform (Universal) Resource Locator). За этими локаторами могут стоять различные сущности – HTML-файлы, CGI-процедуры и т.п.

Как правило, субъекты доступа идентифицируются по IP-адресам и/или именам компьютеров и областей управления. Кроме того, может использоваться парольная аутентификация пользователей или более сложные схемы, основанные на криптографических технологиях.

В большинстве Web-серверов права разграничиваются с точностью до каталогов (директорий) с применением произвольного управления доступом. Могут предоставляться права на чтение HTML-файлов, выполнение CGI-процедур и т.д.

Для раннего выявления попыток нелегального проникновения в Web-сервер важен регулярный анализ регистрационной информации.

Разумеется, защита системы, на которой функционирует Web-сервер, должна следовать универсальным рекомендациям, главной из которых является максимальное упрощение. Все ненужные сервисы, файлы, устройства должны быть удалены. Число пользователей, имеющих прямой доступ к серверу, должно быть сведено к минимуму, а их привилегии – упорядочены в соответствии со служебными обязанностями.

Еще один общий принцип состоит в том, чтобы минимизировать объем информации о сервере, которую могут получить пользователи. Многие серверы в случае обращения по имени каталога и отсутствия файла index.HTML в нем, выдают HTML-вариант оглавления каталога. В этом оглавлении могут встретиться имена файлов с исходными текстами CGI-процедур или с иной конфиденциальной информацией. Такого рода “дополнительные возможности” целесообразно отключать, поскольку лишнее знание (злоумышленника) умножает печали (владельца сервера).

Аутентификация в открытых сетях

Методы, применяемые в открытых сетях для подтверждения и проверки подлинности субъектов, должны быть устойчивы к пассивному и активному прослушиванию сети. Суть их сводится к следующему.

- Субъект демонстрирует знание секретного ключа, при этом ключ либо вообще не передается по сети, либо передается в зашифрованном виде.
- Субъект демонстрирует обладание программным или аппаратным средством генерации одноразовых паролей или средством, работающим в режиме “запрос-ответ”. Нетрудно заметить, что перехват и последующее воспроизведение одноразового пароля или ответа на запрос ничего не дает злоумышленнику.
- Субъект демонстрирует подлинность своего местоположения, при этом используется система навигационных спутников.

Виртуальные частные сети

Одной из важнейших задач является защита потоков корпоративных данных, передаваемых по открытым сетям. Открытые каналы могут быть надежно защищены лишь одним методом – криптографическим.

Отметим, что так называемые выделенные линии не обладают особыми преимуществами перед линиями общего пользования в плане информационной безопасности. Выделенные линии хотя бы частично будут располагаться в неконтролируемой зоне, где их могут повредить или осуществить к ним несанкционированное подключение. Единственное реальное достоинство – это гарантированная пропускная способность выделенных линий, а вовсе не какая-то повышенная защищенность. Впрочем, современные оптоволоконные каналы способны удовлетворить потребности многих абонентов, поэтому и указанное достоинство не всегда облечено в реальную форму.

Любопытно упомянуть, что в мирное время 95% трафика Министерства обороны США передается через сети общего пользования (в частности через Internet). В военное время эта доля должна составлять “лишь” 70%. Можно предположить, что Пентагон – не самая бедная организация. Американские военные полагаются на сети общего пользования потому, что развивать

собственную инфраструктуру в условиях быстрых технологических изменений – занятие очень дорогое и бесперспективное, оправданное даже для критически важных национальных организаций только в исключительных случаях.

Представляется естественным возложить на межсетевой экран задачу шифрования и дешифрования корпоративного трафика на пути во внешнюю сеть и из нее. Чтобы такое шифрование/дешифрование стало возможным, должно произойти начальное распределение ключей. Современные криптографические технологии предлагают для этого целый ряд методов.

После того как межсетевые экраны осуществили криптографическое закрытие корпоративных потоков данных, территориальная разнесенность сегментов сети проявляется лишь в разной скорости обмена с разными сегментами. В остальном вся сеть выглядит как единое целое, а от абонентов не требуется привлечение каких-либо дополнительных защитных средств.

Важнейшим аспектом информационной безопасности является управляемость системы. Управляемость – это и поддержание высокой доступности системы за счет раннего выявления и ликвидации проблем, и возможность изменения аппаратной и программной конфигурации в соответствии с изменившимися условиями или потребностями, и оповещение о попытках нарушения информационной безопасности практически в реальном времени, и снижение числа ошибок администрирования, и многое, многое другое.

Наиболее остро проблема управляемости встает на клиентских рабочих местах и на стыке клиентской и серверной частей информационной системы. Причина проста – клиентских мест гораздо больше, чем серверных, они, как правило, разбросаны по значительно большей площади, их используют люди с разной квалификацией и привычками. Обслуживание и администрирование клиентских рабочих мест – занятие чрезвычайно сложное, дорогое и чреватое ошибками. Технология Intranet за счет простоты и однородности архитектуры позволяет сделать стоимость администрирования клиентского рабочего места практически нулевой. Важно и то, что замена и повторный ввод в эксплуатацию клиентского компьютера могут быть осуществлены очень быстро, поскольку это “клиенты без состояния”, у них нет ничего, что требовало бы длительного восстановления или конфигурирования.

На стыке клиентской и серверной частей Intranet-системы находится Web-сервер. Это позволяет иметь единый механизм регистрации пользователей и наделения их правами доступа с последующим централизованным администрированием. Взаимодействие с многочисленными разнородными сервисами оказывается скрытым не только от пользователей, но и в значительной степени от системного администратора.

Задача обеспечения информационной безопасности в Intranet оказывается более простой, чем в случае произвольных распределенных систем, построенных в архитектуре клиент/сервер. Причина тому – однородность и простота архитектуры Intranet. Если разработчики прикладных систем сумеют в полной мере воспользоваться этим преимуществом, то на программно-техническом уровне им будет достаточно нескольких недорогих и простых в освоении продуктов. Правда, к этому необходимо присовокупить продуманную политику безопасности и целостный набор мер процедурного уровня.

9.8. Правила при работе с компьютерной сетью

Правило первое

Крайне осторожно относитесь к программам и документам Word/Excel, которые получаете из глобальных сетей. Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте их на наличие вирусов.

Используйте специализированные антивирусы – для проверки "на-лету" всех файлов, приходящих по электронной почте (и по Internet в целом). К сожалению, на сегодняшний день мне неизвестны антивирусы, которые достаточно надежно ловят вирусы в приходящих из Internet файлах, но не исключено, что такие антивирусы появятся в ближайшем будущем.

Правило второе – защита локальных сетей

Для уменьшения риска заразить файл на сервере администраторам сетей следует активно использовать стандартные возможности защиты сети: ограничение прав пользователей; установку атрибутов "только на чтение" или даже "только на запуск" для всех выполняемых файлов (к сожалению, это не всегда оказывается возможным) и т.д.

Используйте специализированные антивирусы, проверяющие "на лету" файлы, к которым идет обращение. Если это по какой-либо причине невозможно, регулярно проверяйте сервер обычными антивирусными программами.

Значительно уменьшается риск заражения компьютерной сети при использовании бездисковых рабочих станций.

Желательно также перед тем, как запустить новое программное обеспечение, попробовать его на тестовом компьютере, не подключенном к общей сети.

Правило третье

Лучше покупать дистрибутивные копии программного обеспечения у официальных продавцов, чем бесплатно или почти бесплатно копировать их из других источников или покупать пиратские копии. При этом значительно снижается вероятность заражения, хотя известны случаи покупки инфицированных дистрибутивов.

Как следствие из этого правила вытекает необходимость хранения дистрибутивных копий программного обеспечения (в том числе копий

операционной системы), причем копии желательно хранить на защищенных от записи дискетах.

Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов, хотя это не всегда спасает (например, на WWW-сервере Microsoft довольно долгое время находился документ, зараженный макро-вирусом "Wazzu"). По-видимому, единственными надежными с точки зрения защиты от вирусов являются BBS/ftp/WWW антивирусных фирм-разработчиков.

Правило четвертое

Старайтесь не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Желательно использовать только программы, полученные из надежных источников. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.

Если даже ни один антивирус не среагировал на файл, который был снят с BBS или электронной конференции – не торопитесь его запускать. Подождите неделю, если этот файл вдруг окажется заражен новым неизвестным вирусом, то скорее всего кто-либо "наступит на грабли" раньше вас и своевременно сообщит об этом.

Желательно также, чтобы при работе с новым программным обеспечением в памяти резидентно находился какой-либо антивирусный монитор. Если запускаемая программа заражена вирусом, то такой монитор поможет обнаружить вирус и остановить его распространение.

Все это приводи к необходимости ограничения круга лиц, допущенных к работе на конкретном компьютере. Как правило, наиболее часто подвержены заражению "многопользовательские" персональные компьютеры.

Правило пятое

Пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т.д.). Периодически сравнивайте информацию, хранящуюся в подобной базе данных, с реальным содержимым винчестера, так как практически любое несоответствие может служить сигналом о появлении вируса или "троянской" программы.

Правило шестое

Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа. Такие резервные копии носят название backup-копий. Затраты на копирование файлов, содержащих исходные тексты программ, базы данных,

документацию, значительно меньше затрат на восстановление этих файлов при проявлении вирусом агрессивных свойств или при сбое компьютера.
При наличии стримера или какого-либо другого внешнего носителя большого объема имеет смысл делать backup всего содержимого винчестера. Но поскольку времени на создание подобной копии требуется значительно больше, чем на сохранение только рабочих файлов, имеет смысл делать такие копии реже.

Прочие правила

Поставьте в BIOS Setup порядок загрузки "сначала – C:, потом – A:". Это надежно защитит компьютер от загрузочных вирусов.
Не обольщайтесь встроенной в BIOS защитой от вирусов, многие вирусы "обходят" ее при помощи различных приемов.
То же верно для систем антивирусной защиты, встроенных в Word и Excel MS Office. Они также могут быть отключены вирусом (или самим пользователем, поскольку эти системы могут сильно мешать в работе).

9.9. Место информационной безопасности экономических систем в национальной безопасности страны

В современном мире информационная безопасность становится жизненно необходимым условием обеспечения интересов человека, общества и государства и важнейшим, стержневым, звеном системы национальной безопасности страны.
Доктрина национальной безопасности страны рассматривает всю работу в информационной сфере на основе и в интересах Концепции национальной безопасности РФ.
Доктрина выделяет четыре основные составляющие национальных интересов России в информационной сфере.
Первая составляющая включает соблюдение конституционных прав и свобод человека и гражданина в области получения и пользования информацией, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.
Для ее реализации необходимо:

1. повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа страны;

2. усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала России;
3. обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
4. обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
5. укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
6. гарантировать свободу массовой информации и запрет цензуры;
7. не допускать пропаганды и агитации, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
8. обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов в информационной сфере включает информационное обеспечение государственной политики страны, связанное с доведением до российской и международной общественности достоверной информации о ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам. Для этого требуется:

1. укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
2. интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов в информационной сфере включает развитие современных информационных технологий, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение

потребностей внутреннего рынка этой продукцией и выход ее на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Для достижения результата на этом направлении необходимо:

1. развивать и совершенствовать инфраструктуру единого информационного пространства России;
2. развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
3. развивать производство в стране конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
4. обеспечить государственную поддержку фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов в информационной сфере включает защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

В этих целях требуется:

1. повысить безопасность информационных систем (включая сети связи), прежде всего первичных сетей связи и информационных систем органов государственной власти, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
2. интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля их эффективности;
3. обеспечить защиту сведений, составляющих государственную тайну;
4. расширять международное сотрудничество России в области безопасного использования информационных ресурсов, противодействия угрозе противоборства в информационной сфере.

9.10. Концепция информационной безопасности

Концепция защиты информации – инструментально-методологическая база, обеспечивающая практическую реализацию стратегий защиты (оборонительной, наступательной, упреждающей), при ее оптимизации и минимальности затрат.

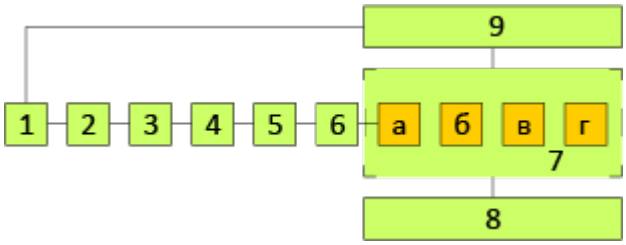


Рисунок 9.11 – Структура концепции защиты информации

На рисунке 9.11 приведена структура концепции защиты информации, где:

- 1 – концепции, задающие ситуацию защиты;
- 2 – методология описания ситуации защиты;
- 3 – система показателей уязвимости (защищенности) информации;
- 4 – система дестабилизирующих факторов, влияющих на уязвимость (защищенность) информации; 5 – методология оценки уязвимости (защищенности) информации;
- 6 – методология определения требований к защите информации;
- 7 – система концептуальных решений по защите информации:
  - а) функции защиты,
  - б) задачи защиты,
  - в) средства защиты,
  - г) система защиты;
- 8 – требования к концептуальным решениям;
- 9 – условия, способствующие повышению эффективности защиты.

Концепции, задающие ситуацию защиты

Ситуацию защиты формируют концепции построения и использования автоматизированных систем обработки данных (АСОД) и условия их функционирования. АСОД предназначены для оптимального управления информационным обеспечением деятельности современных объектов (предприятий, учреждений и т. п.) на регулярной основе.

Решениями данной концепции являются формирование на каждом специальном объекте информационного кадастра, построение унифицированной технологии автоматизированной обработки информации и разработка методологии организации информационного обеспечения деятельности объектов.

Унифицированная технология автоматизированной обработки информации представлена в таблице 9.1.

Таблица 9.1 – Унифицированная технология автоматизированной обработки информации

Наименование участков	**Характеристики участков**		
	Содержание обработки данных	**Данные, используемые в процессе обработки**	**Данные, полученные в процессе обработки**
Прием входных потоков информации	1. Прием и размещение в буферных запоминающих	1. Поступающие по каналам связи	1. Подготовленные для последующей обработки

Наименование участков	Характеристики участков		
	Содержание обработки данных	**Данные, используемые в процессе обработки**	**Данные, полученные в процессе обработки**
	устройствах поступающих документов и данных. 2. Контроль поступивших документов и данных. 3. Регистрация поступивших документов и данных. 4. Подготовка принятых документов и данных для последующей обработки. 5. Передача документов и данных на обработку.	сообщения: быстроменяющейся информации; медленноменяюшейся фактографической информации: постоянной информации. 2. Поступающая входящая корреспонденция. 3. Поступающая техническая документация. 4. Поступающая другая документальная информация.	все виды поступившей информации. 2. Данные для регистрации всех видов поступившей информации. 3. Данные об обнаруженных ошибках в поступивших сообщениях и документах.
Обработка быстроменяющейся информации в реальном масштабе времени	1. Разделение потока быстроменяющейся информации по категориям срочности сообщений. 2. Обеспечение немедленной обработки весьма срочных сообщений. 3. Периодическая обработка массива срочных сообщений. 4. Табельная обработка всего массива сообщений. 5. Информационно-вычислительное обеспечение текущей работы диспетчерских служб. 6. Передача всех поступивших данных на базовую обработк.	1. Поступающие сообщения быстроменяющейся информации. 2. Ранее накопленные массивы быстроменяющейся информации. 3. Массивы нормативно-правовой информации.	1. Сигналы о поступлении весьма срочных сообщений. 2. Информационные сообщения выдаваемые на устройства отображения. 3. Результаты решения задачи распознавания ситуации. 4. Табельные документы оперативно-диспетчерской службы. 5. Данные, выдаваемые по нерегламентным запросам. 6. Сообщения и документы, помещаемые в массивы для последуюшего использования. 7. Сообщения, передаваемые на базовую обработку.
Формирование текущих массивов входной информации	1. Проверка правильности приема и регистрации поступивших данных и документов. 2. Определение назначения поступивших сообщений и документов и распределение их по массивам.	1. Сообщения и документы входных потоков, поступившие в соответствующий интервал времени. 2. Массивы нормативно-справочных данных.	1. Массивы сообщений, подготовленные для базовой обработки фактографической информации. 2. Массивы документов, подготовленные для базовой обработки документальной информации.
Базовая обработка входных потоков	1. Обработка по стандартному алгоритму: фактографической	1. Массивы сообщений, подготовленные на	1. Данные, извлекаемые специалистами в процессе

Наименование участков	Характеристики участков		
	Содержание обработки данных	**Данные, используемые в процессе обработки**	**Данные, полученные в процессе обработки**
информации	информации; поступившей входящей корреспонденции, технической документации; другой документальной информации. 2. Обеспечение ввода данных в массивы исходных данных. 3. Формирование массивов описаний документов. 4. Подготовка и передача в фонды оригиналов документов.	предыдущем этапе. 2. Массивы документов, подготовленные на предыдущем этапе. 3. Массивы нормативно-справочных данных.	базовой обработки и помещаемые в персональные массивы. 2. Массивы картотеки входящей корреспонденции. 3. Массивы описаний документов.
Формирование массивов исходных данных	1. Организация ввода и ввод данных в запоминающее устройство. 2. Проверка правильности исходных данных. 3. Размещение исходных данных в массивах в соответствии с их назначением и принадлежностью. 4. Поддержание массивов исходных данных в рабочем состоянии. 5. Обеспечение целостности и безопасности информации в массивах исходных данных	1. Данные, извлекаемые пользователями в процессе базовой обработки. 2. Массивы ранее накопленных исходных данных. 3. Массивы нормативно-справочных данных.	1. Упорядоченные, организованные, поддерживаемые в рабочем состоянии и защищаемые массивы исходных данных
Аналитико-синтетическая обработка информации	1. Формирование перечня обновляемых и впервые получаемых регламентных данных. 2. Организация процесса обработки. 3. Организация многоаспектного поиска в массивах исходных и регламентных данных. 4. Логико-аналитическая обработка данных по запросуи в диалоговом режиме. 5. Организация экспертизы с количественными оценками параметров. 6. Организация экспертных оценок на уровне лингвистических оценок экспертов и по методологии "мозгового штурма". 7. Организация и поддержание сеансов психоинтеллектуальной генерации.	1. Массивы исходных данных. 2. Массивы регламентных данных. 3. Массивы нормативно-справочных данных. 4. Массивы вспомогательных данных	1. Регламентные данные, подготовленные для ввода в массивы. 2. Массивы вспомогательных данных (результаты).
Введение баз регламентных данных	1. Формирование списков вводимых регламентных данных	1. Формирование списков вводимых	1. Обновленные и пополненные массивы

Наименование участков	Характеристики участков		
	Содержание обработки данных	**Данные, используемые в процессе обработки**	**Данные, полученные в процессе обработки**
информационного кадастра	при обновлении и пополнении данных кадастра. 2. Организация процесса ввода данных. 3. Формирование регламентных данных для ввода и контроль правильности их формирования. 4. Передача пакета данных администрации кадастра. 5. Документальное и юридическое оформление передачи пакета данных. 6. Ввод пакета данных в массивы регламентных данных. 7. Контроль правильности ввода. 8. Документальное оформление акта ввода данных в массивы кадастра. 9. Поддержание массивов данных в рабочем состоянии и организация их защиты. Организация контроля массивов кадастра. 10. Оптимизация структуры массивов кадастра.	регламентных данных при обновлении и пополнении данных кадастра. 2. Организация процесса ввода данных. 3. Формирование регламентных данных для ввода и контроль правильности их формирования. 4. Передача пакета данных администрации кадастра. 5. Документальное и юридическое оформление передачи пакета данных. 6. Ввод пакета данных в массивы регламентных данных. 7. Контроль правильности ввода. 8. Документальное оформление акта ввода данных в массивы кадастра. 9. Поддержание массивов данных в рабочем состоянии и организация их защиты. Организация контроля массивов кадастра. 10. Оптимизация структуры массивов кадастра.	информационного кадастра. 2. Записи в журналах учета передачи, регистрации обновления, пополнения и учета результатов контроля
Переработка данных	1. Ввод (формирование) запросов на переработку информации. 2. Формирование процедуры (алгоритма) переработки информации в соответствии с запросом. 3. Определение перечня данных, необходимых для выполнения сформированной процедуры. 4. Выполнение процедуры по сформированному алгоритму. 5. Выдача результатов переработки в соответствии с запросом. 6. Запись (при необходимости)	1. Массивы регламентных данных. 2. Регистрационные журналы. 3. Массивы нормативно-справочных данныхю	1. Результаты переработки данных в соответствии с алгоритмической процедурой. 2. Записи в массивах результатов. 3. Записи в регистрационных журналах

Наименование участков	Характеристики участков		
	Содержание обработки данных	**Данные, используемые в процессе обработки**	**Данные, полученные в процессе обработки**
	результатов переработки в массив результатов. 7 Контроль записи. 8. Регистрация записи в журнале. 9. Поддержание массивов в рабочем состоянии. 10. Защита массивов результатов. 11. Оптимизация структуры массивов результатов		
Выдача данных	1. Формирование списка подлежащих выдаче регламентных документов. 2. Организация процедуры обработки документов. 3. Компоновка формы обрабатываемого документа. 4. Формирование списка данных, необходимых для обработки документа. 5. Поиск и выборка необходимых данных. 6. Обработка выбранных данных в соответствии с формой и содержанием документа. 7. Выдача документа. 8. Запись документа в массив выданных документов. 9. Регистрация выдачи документа и записи его в массив. 10. Ввод запросов на нерегламентную выдачу данных. 11. Формирование списка данных, необходимых для удовлетворения запроса. 12. Поиск и выборка необходимых данных. 13. Обработка выбранных данных. 14. Выдача данных. 15. Запись (при необходимости) выданных данных в массив. 16. Регистрация (при необходимости) выдачи данных и записи их в массив. 17. Поддержание массивов в рабочем состоянии. 18. Защита массивов. 19. Оптимизация структуры массивов выданных документов.	1. Табель выдачи регламентных документов. 2. Массивы форм документов. 3. Массивы информационного кадастра. 4. Результаты обработки данных.	1. Регистрационные данные о выдаче регламентных документов. 2. Регистрационные данные о поступивших нерегламентных запросах и выданных по ним данным.

Методология описания ситуации защиты

Описание ситуации защиты необходимо проводить в строго формальном представлении архитектуры и процессов функционирования рассматриваемой системы. Одной из наиболее характерных особенностей ситуаций является повышенное влияние случайных факторов, что затрудняет формальное описание системы.

Система показателей уязвимости (защищенности) информации

Под показателем уязвимости информации понимается мера потенциально возможного негативного воздействия на защищаемую информацию. Величина, дополняющая меру уязвимости до максимально возможного значения представляет собою меру защищенности информации.

Система дестабилизирующих факторов, влияющих на уязвимость (защищенность) информации

Под дестабилизирующим фактором понимается событие или явление, которое может произойти в АСОД или системе защиты, и содержащее в себе потенциальную возможность такого негативного воздействия на информацию, результатом которого может быть повышение значений каких-либо показателей уязвимости защищаемой информации и соответственно – снижение показателей ее защищенности. Для реализации оборонительной стратегии защиты достаточно иметь сведения об уже известных и наиболее опасных угрозах. Для наступательной стратегии необходимы сведения обо всех когда-либо проявлявшихся угрозах. Для реализации упреждающей стратегии необходимы сведения обо всех потенциально возможных угрозах как в существующих, так и в перспективных системах защиты информации.

Методология оценки уязвимости (защищенности) информации.

Данная методология должна содержать методы, модели и инструментальные средства определения текущих и прогнозирования будущих значений каждого из системы показателей уязвимости (защищенности) информации под воздействием каждой из потенциально возможных угроз и любой их совокупности.

Методология определения требований к защите информации

Данный компонент определяет подходы, средства и методы практической организации защиты. По возможности требования к любым параметрам создаваемых систем должны быть выражены в количественном эквиваленте. С повышенным влиянием на систему различных неопределенностей, требования к системе защиты определяются эвристическими и теоретико-эмпирическими методами. Построение системы необходимо проводить во взаимосвязи с задачами оптимизации и стандартизации.

Система концептуальных решений по защите информации

Под концептуальным решением понимается решение, которое создает объективные предпосылки для формирования инструментальных средств, необходимых и достаточных для эффективного решения всей совокупности задач по защите информации на регулярной основе и в соответствии с требованиями к их решению. Требования к решению задач определяются целями функционирования системы защиты. Концептуальные решения должны быть научно обоснованными и оптимальными. Принятие решений относится к слабоструктурированным задачам, и методики их решения должны основываться на эвристических методах.

Требования к концептуальным решениям

Данный компонент концепции защиты заключается в обосновании таких требований к каждому из концептуальных решений, которые обеспечивали бы достижение целей их принятия наиболее рациональным способом.

Условия, способствующие повышению эффективности защиты

Данный компонент защиты информации заключается в формировании и обосновании перечней и содержания условий, соблюдение которых будет существенно способствовать повышению уровня защиты при расходовании выделенных для этих целей средств, обеспечивающих требуемый уровень защиты.

Целями защиты информации является:

- предупреждение возникновения условий, благоприятствующих порождению дестабилизирующих факторов;
- предупреждение непосредственного проявления дестабилизирующих факторов в конкретных условиях функционирования системы защиты;
- обнаружение проявившихся дестабилизирующих факторов;
- предупреждение воздействия дестабилизирующих факторов на защищаемую информацию;
- обнаружение воздействия дестабилизирующих факторов на информацию;
- локализация (ограничение) воздействия дестабилизирующих факторов на информацию;
- ликвидация последствий воздействия дестабилизирующих факторов на информацию.

Для реализации целей защиты информации сформированы 10 классов задач:

1. Введение избыточности элементов системы. Включение в состав системы дополнительных компонентов сверх минимума, который необходим для выполнения ими всего множества своих функций. Избыточные элементы функционируют одновременно с основными. Это позволяет создавать системы, устойчивые относительно внешних и внутренних дестабилизирующих воздействий. Избыточность подразделяют на

организационную (введение дополнительной численности людей), аппаратную (введение дополнительных технических устройств), программно-алгоритмическую (введение дополнительных алгоритмов и программ), информационную (создание дополнительных информационных массивов), временную (выделение дополнительного времени для проведения обработки информации).

2. Резервирование элементов системы. Вместо введения в активную работу дополнительных элементов, часть элементов выводится из работы и держится в резерве на случай непредвиденных ситуаций. Различают два вида резервирования – горячее и холодное. При горячем резервировании выводимые в резерв элементы находятся в рабочем состоянии и способны включаться в работу сразу без проведения дополнительных операций включения и подготовки. При холодном резервировании элементы находятся в таком состоянии, что для перевода их в рабочее состояние требуются дополнительные процедуры.
3. Регулирование доступа к элементам системы. Доступ на объект будет предоставлен лишь при условии предъявления некоторой заранее обусловленной идентифицирующей информации.
4. Регулирование использования элементов системы. Осуществление запрашиваемых операций производится лишь при условии предъявления некоторых заранее обусловленных полномочий.
5. Маскировка информации. Защищаемые данные преобразуются или маскируются таким образом, что они в явном виде могут быть доступными лишь при предъявлении некоторой специальной информации, называемой ключом преобразования.
6. Контроль элементов системы. Совокупность проверок – соответствие элементов системы заданному их составу, текущего состояния элементов системы, работоспособности элементов системы, правильности функционирования элементов системы и т. д.
7. Регистрация сведений. Фиксация всех тех сведений о фактах, событиях и ситуациях, относящихся к защите информации.
8. Уничтожение информации. Осуществление процедур своевременного уничтожения тех элементов информации, которые больше не нужны для функционирования системы защиты и дальнейшее нахождение которых может отрицательно сказаться на защищенности информации. Одной из разновидностей уничтожения информации является аварийное уничтожение, осуществляемое при явной угрозе злоумышленного доступа к информации повышенной важности.

9. Сигнализация. В системе управления должна быть обратная связь, по которой поступает информация (сигналы) о состоянии управляемых объектов и процессов. Процедуры генерирования, передачи и отображения (выдачи) этих сигналов и составляют содержание рассматриваемого класса задач.
10. Реагирование. Наличие возможностей реагирования на проявление дестабилизирующих факторов с целью предотвращения или снижения степени их воздействия на информацию.

Основы защиты информации:

1. Защита информации должна быть комплексной и предусматривать обеспечение физической и логической целостности информации, предупреждение несанкционированной ее модификации, предотвращение несанкционированного получения и несанкционированного размножения.
2. Комплексная защита информации будет эффективной при условии системно-концептуального подхода к изучению и решению всех вопросов, связанных с защитой:
    - исследование и разработка всей совокупности вопросов защиты информации с единых методологических позиций;
    - рассмотрение в едином комплексе всех видов защиты информации;
    - системный учет всех факторов, оказывающих влияние на защищенность информации;
    - комплексное использование всех имеющихся средств защиты информации.
3. На базе системно-концептуального подхода может быть разработана унифицированная концепция защиты информации.
4. Работы по защите информации должны проводится непрерывно.
5. Создание эффективных механизмов защиты, их поддержания и обеспечения должно осуществляться профессионально подготовленными специалистами.

Заключение

Проблема обеспечения, информационной безопасности широка и многогранна. За внешней тривиальностью, заключающейся в обеспечении трех составляющих информационной безопасности (доступности, целостности и конфиденциальности информации) скрывается значительный перечень мероприятий: от общих решений, принимаемых в интересах всего общества и государства, до частных решений применительно к отдельному носителю информации.

На сегодняшний день в нашей стране в целом сформирована единая политика в сфере обеспечения информационной безопасности. Для этого принят целый ряд основополагающих законов, также разработаны ключевые оценочные стандарты средств автоматизированной обработки, хранения, отображения и обмена информацией.

Опыт ведущих развитых стран показывает, что по мере все большей автоматизации и информатизации общественной жизни проблема информационной безопасности будет все больше обостряться.

Наличие проблем с обеспечением защищенности информации и поддерживающей ее инфраструктуры на сегодняшний день сдерживает развитие таких перспективных экономических направлений, как электронная коммерция, электронный бизнес, безбумажный документооборот и др., которые могут реально повысить эффективность функционирования целых отраслей производства и сферы сервисных услуг.

В нашей стране все более востребованными становятся услуги специалистов, занимающихся вопросами защиты информации. На этом фоне появляются крупные компании, оказывающие подобные услуги, разрабатывающие специализированные аппаратно-программные комплексы защиты информации, что дополнительно подтверждает актуальность проблемы обеспечения информационной безопасности.

В связи с этим можно отметить, что современный человек, хоть как-то связанный с информационными технологиями и средствами автоматизации обработки информации, должен представлять основные источники и угрозы информационной безопасности, а самое главное, должен знать основные приемы безопасной работы. Именно с этой точки зрения излагался материал данного пособия. Пользователи, у которых данный материал вызвал дополнительный интерес, могут воспользоваться литературой, приведенной в конце каждого раздела. Наиболее актуальную информацию по проблеме обеспечения информационной безопасности можно найти в периодических изданиях, а также в глобальной сети Интернет.

Глоссарий

А

Авторское право – один из институтов гражданского права, регулируемые им имущественные и личные неимущественные отношения связаны с созданием и с использованием произведений литературы, науки и искусства.

Антивирусная программа – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Антивирусные блокировщики – это резидентные программы, перехватывающие "вирусоопасные" ситуации и сообщающие об этом пользователю.

Аудит – это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день).

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Б

Безопасность – это состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз.

В

Вакцины или **иммунизаторы** – это резидентные программы, предотвращающие заражение файлов.

Г

Государственная тайна – защищаемые государством сведения, создаваемые в условиях секретности в соответствии с законодательством РФ.

Д

Домен – группа узлов сети (хостов), объединенных общим именем, которое для удобства несет определенную смысловую нагрузку.

Доменное имя – это уникальный алфавитно-цифровой идентификатор узла (состоит из символов ASCII-кода – букв от A до Z латинского алфавита и цифр от 0 до 9, также допускается дефис "-").

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

З

Запугивание – это воздействие на сотрудника фирмы посредством угрозы взрыва, поджога квартиры, склада офиса, гаража, автомобиля и другого физического воздействия, которое приводит к подчинению данного лица замыслу злоумышленника.

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

Защищенность – способность противостоять НСД к конфиденциальной информации, ее искажению или разрушению.

Злоумышленник (противник) - субъект, осуществляющий преднамеренный НСД к данным.

Злоумышленные бедствия - связаны главным образом с несанкционированным доступом к ресурсам ИВС.

И

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Идентификация (аутентификация) – ввод имени при входе в систему, стандартное средство проверки пользователя (аутентификация) – пароль.

Интеллектуальная собственность – это результат творческой деятельности личности.

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

Информационная безопасность РФ – это состояние страны, в которой гражданам, объединениям и общественным группам граждан, обществу и государству не может быть нанесен существенный ущерб путем оказания воздействия на информационную сферу страны.

Информационная безопасность государства – это состояние государства, в котором ему не может быть нанесен существенный ущерб путем оказания воздействия на информационную сферу государства.

Информационная безопасность личности – это состояние человека, в котором его личности не может быть нанесено существенного ущерба путем оказания воздействия на окружающее человека информационное пространство.

Информационная безопасность общества – это состояние общества, в котором ему не может быть нанесен существенный ущерб путем воздействия на информационную сферу общества.

Информационная война – действия, принимаемые для достижения информационного превосходства в интересах национальной военной стратегии, осуществляемые путем влияния на информацию и информационные системы противника при одновременной защите собственной информации своих информационных систем. На следующем рисунке представлены направления и цели защиты информации и их взаимосвязь.

Информационная угроза – это угроза объекту путем оказания воздействия на его информационную сферу.

Информационные продукты (продукция) – документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребителей пользователей

Информационные ресурсы – это отдельные документы и массивы документов в библиотеках, архивах, фондах, банках данных и других информационных системах.

Информационные услуги – действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами.

Информационный терроризм – это особая форма насилия, представляющая собой сознательное и целенаправленное информационное воздействие или угрозу применения такого воздействия для принуждения правительства к реализации политических, экономических, религиозных и иных целей террористической организацией или отдельными террористами, сопровождаемое эмоциональным воздействием на общество для возбуждения в нем страха, панических настроений, потери доверия к власти и создание политической нестабильности.

Информация как объект гражданских правоотношений – произведения науки и литературы, другие формы, отображающие информацию (например, карты, фотографии и т.п.), а также информация, содержащаяся в документах, закрепляющих авторские права на изобретения, полезные модели, промышленные образцы (патенты, свидетельства).

Информация о гражданах – (персональные данные) создаются самими гражданами в их повседневной деятельности, в том числе связанной с реализацией прав и свобод (права на труд, на жилище, на отдых, медицинское обслуживание, пенсионное обеспечение, на свободу слова и многое другое) и выполнением обязанностей (например, воинской обязанности) и представляется как сведения о себе (персональные данные) разным субъектам. Документированной информацией здесь являются анкеты, истории болезни, декларации о доходах, банковские записи и т.п.

К

Код – совокупность символов, соответствующих элементам информации или ее характеристикам.

Коммерческая тайна (информация, составляющая коммерческую тайну) – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, включая ноу-хау. Режим защиты такой информации устанавливается законом.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Концепция защиты информации – инструментально-методологическая база, обеспечивающая практическую реализацию стратегий защиты (оборонительной, наступательной, упреждающей), при ее оптимизации и минимальности затрат.

Копирование – представляет собой точный список, точное воспроизведение, повторение чего-либо.

Криптографические методы защиты информации – преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на то полномочия.

Л

Лицензия – специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении требований и условий, выданная юридическому лицу или индивидуальному предпринимателю.

М

Маршрутизатор – это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями.

Маскировка – метод защиты информации в каналах телекоммуникаций путем ее криптографического закрытия.

Массовая информация – информация, содержащая сообщения информационного характера, подготавливаемая и распространяемая СМИ и (или) через Интернет с целью информирования населения, в том числе реклама деятельности физических и юридических лиц, производимых продуктов и предоставляемых услуг, предлагаемых потребителям.

Межсетевой экран – программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации.

Механизм подотчетности (протоколирования) – доверенная система должна фиксировать все события, касающиеся безопасности.

Н

Нарушитель - субъект, осуществляющий несанкционированный доступ к данным к данным.

Научно-юридическая информация – сведения, содержащиеся в юридических монографиях, статьях, справочниках, комментариях, докладах на юридические темы и т.п.

Национальная безопасность России – это гарантированная конституционными, законодательными и практическими мерами защищенность и обеспеченность ее национальных интересов.

Национальные интересы России – это совокупность сбалансированных интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других сферах.

Несанкционированный доступ к данным (НСД) - злоумышленное или случайное действие, нарушающее технологическую схему обработки данных и ведущее к получению, модификации или уничтожению данных. НСД к данным может быть пассивным (несанкционированное получение или размножение информации) и активным (модификация, уничтожение информации).

О

Обязательно представляемая документированная информация – обязательные контрольные экземпляры документов, информация в учетных документах, данные документов, представляемых в органы статистики, налоговая, регистрационная и другая такого типа информация. Такая информация создается юридическими и физическими лицами в порядке учета и отчетности и направляется в обязательном порядке разным органам и организациям в соответствии с действующим законодательством.

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

Отказ - это нарушение работоспособности какого-либо элемента ИВС, приводящее к невозможности выполнения им своих функций.

Официальные документы – законы, судебные решения, иные тексты законодательного, административного и судебного характера, а также их официальные переводы. Эта информация создается в порядке законотворческой или иной правовой деятельности.

Ошибка (вид) - неправильное (одноразовое или систематическое) выполнение элементом ИВС одной или нескольких функций, происходящее вследствие специфического его состояния.

П

Побочные явления - электромагнитные излучения устройств ИВС, паразитные наводки, внешние электромагнитные излучения, вибрации, внешние атмосферные условия и т.д.

Побуждение – такой метод защиты, который побуждает пользователя и персонал системы не нарушать установленных за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и "неписаных").

Подозрительная активность – поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Подсеть (subnetwork) – (в терминологии Internet) совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

Полиморфные вирусы – вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

Преднамеренные воздействия – это целенаправленные действия злоумышленника.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.).

Прерывание – реакция системы на некоторое событие, при котором временно прекращается исполнение программы и используется процедура обработки прерывания, после чего управление передается в основную программу.

Принуждение – такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Программная закладка – программа, которая способна выполнить ряд разрушающих операций.

Протокол сетевого обмена информацией можно определить как перечень форматов передаваемых блоков данных, а также правил их обработки и соответствующих действий.

Р

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Режим военного положения – это функционирование системы национальной безопасности при наличии угроз национальным интересам России, требующих отражения и уничтожения.

Режим мирного времени – это нормальное функционирование системы национальной безопасности в условиях отсутствия угроз национальным интересам России или их практической нейтрализации.

Режим повышенной готовности – это функционирование системы национальной безопасности при наличии угроз, требующих их пресечения.

Режим чрезвычайного положения – это функционирование системы национальной безопасности при наличии угроз национальным интересам России, требующих локализации и устранения.

С

Сбой - это временное нарушение работоспособности какого–либо элемента ИВС, следствием чего может быть неправильное выполнение им в этот момент своих функций.

Сегмент сети – физическое объединение хостов.

Секретность – это понятие, которое употребляется по отношению к отдельным лицам. Это есть право лица решать какую информацию он желает разделить с другими, а какую хочет скрыть от других.

Система защиты информации – совокупность органов и (или) исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации (ГОСТ Р 50922-96 "Защита информации. Основные термины и определения").

Система национальной безопасности – это совокупность органов управления, сил и средств, законодательных актов ориентированных на

обеспечение безопасности и защиты жизненно важных интересов государства и общества от внешних и внутренних угроз.

Стихийные бедствия - пожары, наводнения, стихийные бедствия, взрывы и т.д.

Стойкость шифра – это способность противостоять попыткам постороннего лица восстановить (дешифровать) открытый текст по перехваченному шифртексту.

Субъект атаки (или источник атаки) – это атакующая программа или злоумышленник, непосредственно осуществляющие воздействие.

Т

Технический канал утечки информации (ТКУИ) – это совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.

Типовая удаленная атака – это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной сети.

У

Угроза информации – это потенциальная возможность определенным образом нарушить информационную безопасность.

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи.

Управление доступом – метод защиты информации регулированием использования всех ресурсов системы (элементов баз данных, программных и технических средств).

Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС. Он показывает, насколько корректны механизмы, отвечающие за политику безопасности.

Ф

Федеральные критерии безопасности информационных технологий – первый стандарт информационной безопасности, в котором определяются три независимые группы требований: функциональные требования к средствам защиты, требования к технологии разработки и к процессу квалификационного анализа.

Х

Хищение – это преступное, противоправное присвоение чужого имущества, средств, документов, материалов и информации.

Ц

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Ш

Шантаж – это неблаговидное действие, угроза разоблачения, разглашения компрометирующих сведений с целью вымогательства, а также вообще угроза, запугивание чем-нибудь с целью создать выгодную для себя обстановку.

Шифр – это множество обратимых преобразований формы сообщения с целью его защиты от несанкционированного прочтения.

Шпионаж в бизнесе – это деятельность по выведыванию, собиранию или похищению сведений, составляющих конфиденциальную информацию с целью использования в своих интересах или с целью передачи ее другим заинтересованным сторонам.

Э

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.