МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Кафедра информационной безопасности

Составители
Е. В. Прокопенко
И. В. Чичерин

ЗАЩИТА ИНФОРМАЦИИ

Методические материалы

Рекомендованы учебно-методической комиссией специальности
10.05.03 Информационная безопасность автоматизированных систем
в качестве электронного издания для использования
в образовательном процессе

Кемерово 2018

Рецензенты
Стенин Д. В.– кандидат технических наук, доцент, директор ИИТМА
Сыркин И. С. – кандидат технических наук, доцент кафедры информационных и автоматизированных производственных систем

Прокопенко Евгения Викторовна
Чичерин Иван Владимирович

Защита информации методические материалы [Электронный ресурс]: для обучающийся специальности 10.05.03 Информационная безопасность автоматизированных систем очной формы обучения / сост. Е. В. Прокопенко, И. В. Чичерин; КузГТУ. – Кемерово, 2018. – Систем. требования: Pentium IV; ОЗУ 8 Мб; Windows XP; мышь. – Загл. с экрана.

Защита информации в телекоммуникационных системах.

Появление общего программного обеспечения в ЭВМ относят к 1953 г., когда в СССР появилась одна из первых теоретических работ по автоматизации программирования для цифровых ЭВМ (А.П. Ершов), а в Массачусетсом технологическом институте (США) была создана экспериментальная "операционная система", применявшаяся в учебных целях. Затем появились специализированные операционные системы (ОС) для обслуживания оборонных вычислительных систем реального времени. Однако эти разработки имели экспериментальный, исследовательский характер и широкого распространения в то время не получили. Тем не менее, потребности практического использования ЭВМ в различных предметных областях, необходимость более эффективного использования ЭВМ. повышение производительности труда разработчиков программного обеспечения, а также стремление расширить рынок сбыта ЭВМ вызвали стремительный прогресс в создании теории и инструментальных средств общего программного обеспечения вычислительных систем.

Построение вычислительных машин основано на трех принципах:

1. Принцип цифрового представления данных (чисел, команд, обозначение операции, букв, слов и т.д.). Единицами данных в ЭВМ являются бит, байт, слово и т.п.

2. Принцип адресности данных – все данные и любые объекты программы хранятся в ячейках памяти, имеющих адрес.

3. Принцип программного управления (Ч. Беббндж, 1834 г.) – управление вычислительным процессом осуществляется с помощью программы, находящейся в памяти ЭВМ.

Все универсальные вычислительные машины, в том числе и персональные компьютеры, имеют структуру, показанную на рис. 1.

Впервые такую структуру вычислительных машин предложил Джон фон Нейман в 1945 г. поэтому ЭВМ с такой структурой называют машинами фон Неймана.

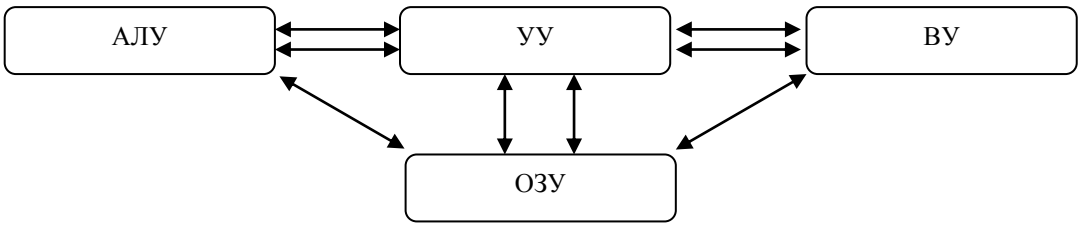

Рис. 1. Общая структура универсальной ЭВМ: АЛУ – арифметико-логическое устройство; УУ – устройство управления; ВУ – внешние устройства; ОЗУ – оперативное запоминающее устройство

Конкретная аппаратурная реализация схемы изменялась от поколения к поколению ЭВМ. Например, в современных компьютерах АЛУ и УУ объединены в единое устройство – *центральный процессор.* Кроме того, в ЭВМ ввели *систему прерываний.* Появились многопроцессорные ЭВМ, позволяющие осуществлять параллельную обработку данных в компьютере. Тем не менее, функциональная структура существующих компьютеров в основном соответствует структуре машины фон Неймана.

Архитектура вычислительной системы – общая логическая организация цифровой вычислительной системы, определяющая процесс обработки данных в конкретной вычислительной системе и включающая методы кодирования данных, состав, назначение, принципы взаимодействия технических средств и программного обеспечения.

Большинство из выпускаемых сейчас компьютеров выполнено в соответствии с принципом открытой архитектуры, впервые примененном в персональной ЭВМ IBM PC (фирма IBM, 1981 г.).

Классификация программных средств

Программное обеспечение вычислительных систем принято делить на следующие виды:

1) общее (системное) программное обеспечение (ОПО):

2) специальное программное обеспечение (СПО). Введем ряд определений.

В состав общего программного обеспечения вычислительных систем входят:

• программные средства управления обработкой данных, включая операционные системы;

• обслуживающие (сервисные) программы (утилиты):

• инструментальные программные средства.

Специальное ПО делят на следующие виды:

• прикладные программы (приложение) общего назначения;

• прикладные программы пользователя.

Прикладные программы общего назначения можно разделить на следующие группы:

- программа офисного назначения;
- программа экономического назначения;
- издательские системы:
- компьютерная графика, видео, анимация и звук;
- системы управления базами данных;
- прочие прикладные программы общего назначения.

Можно видеть, что современные компьютеры и их программное обеспечение глубоко внедрилось практически во все сферы человеческой деятельности: науку, производство, экономику, право и т.д.

Функционирование прикладных программ любого назначения происходит под управлением и при участии программ, относящихся к категории системного программного обеспечения.

Место и функции системного программного обеспечения

Системное ПО играет роль "прослойки" между пользователем и техническими средствами вычислительной системы. На различных этапах работы с компьютером в качестве такой "прослойки" выступают разные программы и пакеты программ системного ПО, выполняя при этом отличающиеся назначением функции.

Основой системного ПО является операционная система.

Операционная система (ОС) цифровой вычислительной системы – система программ, предназначенная для обеспечения определенного уровня эффективности цифровой вычислительной системы за счет автоматизированного управления ее работой и предоставляемого пользователям набора услуг.

Основными функциями ОС являются:

1) автоматическое выполнение действий по запуску задач в обработку и их завершению;

2) диспетчеризация (планирование обработки задач);

3) распределение памяти между различными задачами;

4) управление ходом выполнения задач в вычислительной системе;

5) распределение задачам необходимых ресурсов ВС;

6) синхронизация выполнения задач;

7) поддержка выполнения операции ввода/вывода данных;

8) ведение учета работы системы (при необходимости).

Выполнение своих функции ОС осуществляется с помощью соответствующих программных комплексов управления, которые носят название супервизорных программ (супервизоров или менеджеров).

Супервизорная программа – машинная программа, являющаяся обычно частью операционной системы, которая управляет выполнением других машинных программ и регулирует поток работ в системе управления данными.

Супервизор – часть управляющей программы, координирующая распределение ресурсов вычислительной системы.

В целом современные операционные системы представляют собой иерархическую структуру (рис. 2).

В основе иерархии находится аппаратура вычислительной машины, называемая иногда "чистой машиной" или "голым железом". На следующем уровне иерархии (иногда на следующих нескольких уровнях) находятся некоторые функции ядра операционной системы. В совокупности с этими функциями ядра (называемыми еще "примитивами") компьютер становится *расширенной машиной,* т.е. машиной, которая представляет для операционной системы и пользователей не только свой машинный язык, но и ряд дополнительных возможностей.

Выше над ядром расположены программы ОС для обеспечения выполнения задач пользователя (управления внешними устройствами, обслуживание операций ввода/вывода и т.п.). На вершине иерархии находятся программы пользователя. В подобных иерархических системах принято, как правило, следующее ограничение: допускается обращение только сверху вниз в иерархии, т.е. средства каждого уровня могут обращаться только

к тем функциям, которые находятся на ближайшем нижележащем уровне.

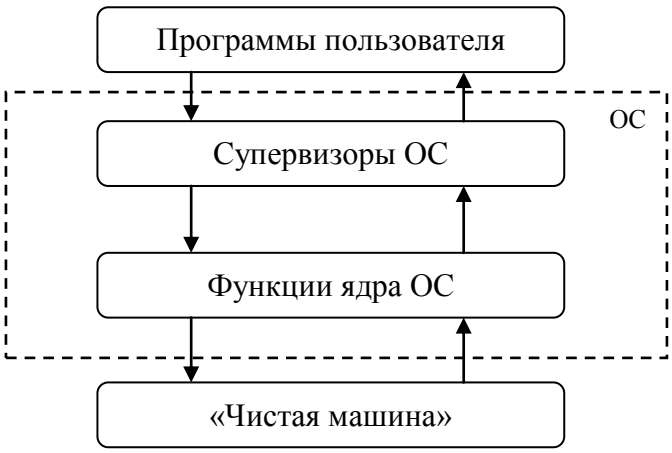

Рис. 2. Структура операционной системы

Обслуживающие (сервисные) программы (утилиты) предназначены для выполнения различных вспомогательных функций и разделяются на следующие типы: про граммы-упаковщики (архиваторы); антивирусные программы; программы резервирования; программы диагностики компьютера; программы оптимизации дисков; программы динамического сжатия дисков.

Инструментальные программные средства, называемые также средствами разработки приложений и системами программирования, являются орудием автоматизации разработок программного обеспечения ЭВМ. обеспечивающим повышение производительности труда разработчиков и надежности ПО.

К инструментальным программным средствам относятся:

- компиляторы и интерпретаторы;
- автономные отладчики (дебагеры. от англ. Debug "удаление насекомых");
- интегрированные оболочки;
- средства создания приложений типа клиент-сервер и т.п.

Существующие инструментальные программные средства обеспечивают разработчиков ПО всем необходимым набором функций для создания мощного программного обеспечения решения прикладных задач любой мощности для практически всех предметных областей.

Принципы работы вычислительной системы

Всякая вычислительная система создается для решения некоторого множества вычислительных или информационных задач, которые в совокупности называются задачами обработки данных. Для успешного решения любой задачи в вычислительной системе необходимо иметь:

1) программу, реализующую алгоритм решения задачи;

2) аппаратные средства ВС для ввода программы, выполнения программы, получения дополнительной информации и вывода результатов:

3) дополнительные программные средства, необходимые для решения прикладной задачи (стандартные программы).

Существует три вида систем обработки данных (СОД), отличающихся друг от друга требованиями к скорости получения результатов решения задач:

1) системы реального времени (СРВ), в которых требования к скорости обработки информации очень высокие из-за необходимости решения задач в темпе реального времени (примером являются системы навигации и управления летательными аппаратами);

2) системы оперативной обработки (СОО), в которых планирование заданий на обработку данных осуществляется, исходя из требования минимальности времени выполнения каждого полученного задания. Примером такого вида систем является система обработки данных для персонала боевых расчетов пунктов управления;

3) системы пакетной обработки (СПО), в которых основным требованием является минимизация простоя оборудования при решении поставленных задач.

Запуск прикладной программы в работу, предоставление ей необходимых аппаратных мощностей и программных средств осуществляется операционной системой.

Режимы работы операционных систем

Режимы обработки данных

Порядок представления прикладной программе перечисленных средств определяется режимов обработки данных, реализованных в операционной системе ЭВМ. Различают однопро-

граммные и мультипрограммные режимы обработки данных и, соответственно, работы ОС.

К однопрограммным режимам относятся:

– режим непосредственного доступа (РНД):

– пакетный однопрограммный режим (ПШ). Мультипрограммными режимами обработки данных являются:

– пакетный мультипрограммный режим (ПМП);

– режим разделения времени (РРВ).

Однопрограммные режимы обработки данных

Режим непосредственного доступа широко применялся в ЭВМ первого поколения и используется при работе с современными персональными компьютерами. РНД характерен тем, что ЭВМ предоставляется только одному пользователю, который осуществляет взаимодействие с машиной посредством пульта управления (сейчас – клавиатура, мыши и дисплеи). Время решения каждой задачи в РНД складывается из времени $7"_{вв}$ ввода программы и данных в ЭВМ, времени T_p работы процессора над решением задачи, времени $T_{ву}$ обмена данными с внешними устройствами (включая вывод результатов и обработки), времени $T_{оп}$ обслуживания ЭВМ и задачи оператором ЭВМ при ее подготовке к запуску и по окончании решения задачи:

$$T_{НД} = T_{ВВ} + T_{ЦП} + T_{ВУ} + T_{ОП}.$$

Коэффициент загрузки процессора при одной задаче составляет

$$\eta_{НД} = T_{ЦП} / T_{НД}.$$

Полное время решения N задач и коэффициент загрузки:

$$T_{НД}(N) = \sum_{i=1}^{N} [T_{ВВ}(i) + T_{ЦП}(i) + T_{ВУ}(i) + T_{ОП}(i)];$$

$$\eta_{НД}(N) = \left[\sum_{i=1}^{N} T_{ЦП}(i) \right] \Big/ T_{НД},$$

где i – номер задачи.

В РНД наличие ОС не обязательно. Недостатками РНД являются:

1) аппаратура и программы ЭВМ используются не эффективно:

2) велики затраты времени программиста на управление машиной;

3) предъявляются высокие требования к подготовке пользователя как оператора вычислительной машины.

Пакетный однопрограммный режим применяется в ВС, начиная с ЭВМ второго поколения. Несколько заданий для решения задач обработки собираются в один пакет, называемый пакет заданий (ПЗ). Пакет гаданий оператор ЭВМ вводит в ЭВМ, где ПЗ сначала записывается во внешнюю память (магнитные диски, магнитные барабаны и т.п.). Затем операционная система машины последовательно считывает задания, входящие в ПЗ. и осуществляет выполнение необходимых в соответствиями с заданиями действий для решения задач пользователей. После завершения очередного задания происходит обращение к ОС. которая активирует начато выполнения следующего. После завершения последнего задания пакета оператор ЭВМ загружает в машину новый пакет заданий.

Режим П1П обладает следующими положительными чертами:

1) более высокая пропускная способность;

2) отсутствие специальных требований к аппаратуре ЭВМ;

3) возможна его реализация на любой ЭВМ.

К недостаткам режима П1П относятся:

1) необходимо наличие операционной системы;

2) пользователь физически отделен от ЭВМ и решаемой им задачи;

3) увеличивается реакция пользователя на полученные результаты решения;

4) последовательный порядок выполнения заданий пакетов не позволяет увеличить загрузку оборудования вычислительной системы.

Многопрограммные режимы обработки данных

Пакетный мультипрограммный режим широко применяется в ЭВМ третьего и последующих поколении. ПМП является режимом классического мультипрограммирования, при котором в вычислительной системе находятся в обработке сразу несколько заданий. На входе в систему формируется набор пакетов

гаданий, которые оператор ЭВМ загружает в систему. После окончания ввода первого ПЗ операционная система начинает его обработку, не дожидаясь ввода второго и последующих ПЗ. Задания, принадлежащие одному пакету*, выполняются последовательно (т.е. в режиме П1П). Задания, принадлежащие разным пакетам, выполняются параллельно. Первым начинает выполняться первое задание первого пакета. По мере освобождения ресурсов ОС активизирует выполнение заданий из других пакетов в порядке их следования внутри ПЗ.

Пакетный мультипрограммный режим обеспечивает наивысшую пропускную способность вычислительной системы, что достигается при наличии в ЭВМ следующих аппаратных средств:

1) автономно управляемые внешние устройства:

2) развитая система прерывания программ;

3) средства защиты памяти от взаимного влияния программ.

Основным недостатком режима ПМП является практически полное устранение пользователя из системы и, как следствие, отсутствие связи пользователя со своей задачей.

Режим разделения бремени существенно отличается от классического мультипрограммирования, реализованного в ПМП, и является в настоящее время основным режимом функционирования операционных систем. Главное в режиме разделения времени – это предоставление каждой задаче (или пользователю, работающему в диалоге с машиной) ресурсов ЭВМ на некоторый ограниченный интервал времени (квант). По истечении кванта времени данная программа свертывается операционной системой, развертывается следующая по очереди программа (или подключается следующий терминал пользователя), которой предоставляются ресурсы ЭВМ. и т.д.

Режимы и дисциплины обслуживания

Порядок обслуживания заданий (заявок на работу) в операционных системах с мультипрограммированием, т.е. реализующих режимы ПМП или РРВ. определяются принятыми в них режимами обслуживания и дисциплинами обслуживания,

Режимы обслуживания

Режимом обслуживания называется правило отбора заявок на обслуживание. Режимы обслуживания делятся на три вида:

1) режим одиночного отбора заявок:

2) режим группового отбора, когда на обслуживание отбирается вся очередь заявок определенного типа:

3) смешанный режим отбора, когда для одних классов заявок производится одиночный отбор, а для других групповой.

Дисциплины обслуживания

Дисциплиной обслуживания называется правило отбора заявок на обслуживание при заданном режиме обслуживания. Для каждого из режимов обслуживания может быть применен один из следующих видов дисциплин обслуживания:

- бесприоритетное обслуживание:
- обслуживание с приоритетом;
- обслуживание по расписанию.

Разновидности дисциплины беспрноритетного обслуживания:

1) ОПП – обслуживание в порядке поступления ("первый пришел – первый обслужен". FIFO);

2) ООП – обслуживание в обратном порядке ("первый пришел – последний обслужен", LIFO);

3) ОСП – обслуживание в случайном порядке.

При бесприоритетном обслуживании считается, что все заявки имеют равное право на обслуживание. Если требуется, чтобы заявки некоторого типа имели преимущества перед другими на их обслуживание операционной системой, то применяется дисциплина обслуживания с приоритетами:

1) ДОП – дисциплина обслуживания с относительными приоритетами, когда приоритет заявки влияет только на ее место в очереди заявок на обслуживание;

2) ДАП – дисциплина с абсолютными приоритетами, когда высоко приоритетная заявка получает преимущества не только перед заявками, стоящими в очереди, но и перед заявкой, получающей обслуживание;

3) ДСП – дисциплина со смешанными приоритетами, при которой к одним группам заявок применяются относительные приоритеты, а к другим – абсолютные:

4) ДДП – дисциплина обслуживания с динамическими приоритетами, когда значение приоритетов заявок может изменяться (расти) по мере их нахождения в очереди, обеспечивая тем самым первоочередное обслуживание заявок, долго находящихся в системе.

Дисциплина обслуживания по расписанию обеспечивает заданный пользователем порядок обработки задании независимо от очередности их поступления в систему. Она применяется в тех случаях, когда результаты решения одной задачи являются входными данными для другой.

Защита информации

Информационная безопасность – сравнительно молодая, быстро развивающаяся область информационных технологий. Под *информационной безопасностью* будем понимать защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействии естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

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

С методологической точки зрения правильный подход к проблемам информационной безопасности начинается с выявления *субъектов информационных отношении* и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Информационная безопасность – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход. Для решения данной проблемы рассматриваются меры *законодательного, административного, процедурного и программно-технического уровня.*

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение *доступности, целостности* и *конфиденци-*

альности информационных ресурсов и поддерживающей инфраструктуры.

Предмет защиты информации

Успех практически любой деятельности в немалой степени зависит от умения распоряжаться такой ценностью, как информация. В законе РФ "Об информации, информатизации и защите информации" определено:

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

Информация имеет ряд особенностей:

- *не материальна;*
- *хранится и передается с помощью материальных носителей;*
- *любой материальный объект содержит информацию о самом себе либо о другом объекте. Информации присущи следующие свойства:*

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

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

Своевременность информации, т.е. соответствие ценности и достоверности определенному временному периоду, может быть выражена формулой

$$C(t) = C_0 e^{-2,3t/\tau},$$

где C_0 – ценность информации в момент ее возникновения; t – время от момента возникновения информации до момента определения ее стоимости; т – время от момента возникновения информации до момента ее устаревания.

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

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

Объект защиты информации

Объектом зашиты информации является компьютерная (информационная) система или автоматизированная система обработки информации (АСОИ).

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

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

Информационная безопасность достигается проведением соответствующего уровня политики информационной безопасности.

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

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

Основные положения безопасности информационных систем

Что касается подходов к реализации защитных мероприятий по обеспечению безопасности информационных систем, то сложилась трехэтапная (трехстадийная) разработка таких мер. Первая стадия – *выработка требовании* – включает:

- *определение состава средств информационной системы;*
- *анализ уязвимых элементов ИС;*
- *оценка угроз (выявление проблем, возникающих при наличия уязвимых мест);*
- *анализ риска (прогноз возможных последствий, вызывающих эти проблемы).*

Вторая стадия – *определение способов зашиты* – включает ответы на следующие вопросы: Какие угрозы должны быть устранены и в какой мере? Какие ресурсы системы должны быть защищаемы и в какой степени? С помощью каких средств должна быть реализована защита?

Какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз? Третья стадия – *определение функций* процедур и средств безопасности, реализуемых в виде некоторых механизмов зашиты.*

Основные принципы обеспечения информационной безопасности в АС

Для зашиты АС на основании руководящих документов Гостехкомиссии могут быть сформулированы следующие положения.

1. Информационная безопасность АС основывается на положениях требованиях существующих законов, стандартов и нормативно-методических документов.

2. Информационная безопасность АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3. Информационная безопасность АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

4. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

5. Неотъемлемой частью работ по ИБ является опенка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

6. Защита АС должна предусматривать контроль эффективности средств зашиты. Этот контроль может быть периодическим либо инициироваться по мере необходимости пользователем АС или контролирующим органом.

Рассмотренные подходы могут быть реализованы при обеспечении следующих основных принципов: *Принцип системности.* Системный подход к защите информационных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

- *при всех видах информационного проявления и деятельности;*
- *во всех структурных элементах;*

- *при всех режимах функционирования;*
- *на всех этапах жизненного цикла;*
- *с учетом взаимодействия объекта защиты с внешней средой.*

Система защиты должна строиться не только с учетом всех известных каналов проникновения, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип комплексности. В распоряжении специалистов по компьютерной безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем (современные СВТ, ОС, инструментальные и прикладные программные средства, обладающие теми или иными встроенными элементами защиты). Комплексное их использование предполагает согласование разнородных средств при построении целостной системы зашиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Пришит непрерывности зашиты. Защита информации – это не разовое мероприятие и даже не конкретная совокупность уже проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС. Разработка системы зашиты должна вестись параллельно с разработкой самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, позволит создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы. Большинству физических и технических средств зашиты для эффективного выполнения своих функций необходима постоянная организационная поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

Разумная достаточность. Создать абсолютно непреодолимую систему защиты принципиально невозможно, при достаточных времени и средствах можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов ИС и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

Гибкость системы защиты. Часто приходится создавать систему защиты в условиях большой неопределенности. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень зашиты. Для обеспечения возможности варьирования уровнем защищенности средства зашиты должны обладать определенной гибкостью. Особенно важно это свойство в тех случаях, когда средства зашиты необходимо устанавливать на работающую систем}', нарушая процесс ее нормального функционирования.

Открытость алгоритмов и механизмов защиты. Суть принципа открытости алгоритмов и механизмов зашиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы зашиты не должно давать возможности ее преодоления. Но это вовсе не означает, что информация конкретной системы зашиты должна быть общедоступна – необходимо обеспечивать защиту от угрозы раскрытия параметров системы.

Принцип простоты применения средств защиты. Механизмы зашиты должны быть интуитивно понятны и просты в использовании, применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действии, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных непонятных ему операции (ввод нескольких паролей и имен и т.д.).

Анализ угроз информационной безопасности

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Угроза – это потенциально возможно событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угрозой информационной безопасности АС называется возможность реализации воздействия на информацию, обрабатываемую АС, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС. приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

Попытка реализации угрозы называется *атакой,* а тот, кто предпринимает такую попытку, – *злоумышленником.* Потенциальные злоумышленнике называются *источниками угрозы.*

Чаще всего угроза является следствием наличия *уязвимых* мест в защите информационных систем (таких как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется *окном опасности,* ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда – недель), поскольку за это время должны произойти следующие события:

– должно стать известно о средствах использования пробела в защите;

– должны быть выпущены соответствующие заплаты:

– заплаты должны быть установлены в защищаемой ИС.

Новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда суще-

ствуют окна опасности, и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат – как можно более оперативно.

Некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов, они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Рассмотрение наиболее распространенных угроз, которым подвержены современные информационные системы, дает представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Угрозы, как и все в ИБ. зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым). Задание возможных угроз информационной безопасности проводится с целью определения полного перечня требований к разрабатываемой системе защиты. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе зашиты АС. Кроме выявления возможных угроз, должен быть проведен их анализ на основе классификационных признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. При этом угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Угрозы можно классифицировать но нескольким критериям:

1) *по аспекту информационной безопасности* (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

2) *по компонентам информационных систем*, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура):

3) *по способу осуществления* (случайные /преднамеренные действия природного/техногенного характера):

4) *по расположению источника угроз* (внутри/вне рассматриваемой ИС).

Необходимость классификации угроз ИБ АС обусловлена тем, что архитектура современных средств автоматизированной обработки информации, организационное, структурное и функциональное построение информационно-вычислительных систем и сетей, технологии и условия автоматизированной обработки информации такие, что накапливаемая, хранимая и

обрабатываемая информация подвержена случайным влияниям чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Как следствие, для защищаемой системы определяют не полный перечень угроз, а перечень классов угроз.

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

1. *По природе возникновения.*

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

2) *Искусственные угрозы* – угрозы информационной безопасности АС, вызванные деятельностью человека.

2. По степени преднамеренности проявления.

1) *Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала.* Например:

- проявление ошибок программно-аппаратных средств АС;

- некомпетентное использование, настройка или неправомерное отключение средств зашиты персоналом службы безопасности;

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т. п.);

- неправомерное включение оборудования или изменение режимов работы устройств и программ;

- неумышленная порча носителей информации;

- пересылка данных по ошибочному адресу абонента (устройства);

- ввод ошибочных данных;

- неумышленное повреждение каналов связи.

2) *Угрозы преднамеренного действия* (например, угрозы действий злоумышленника для хищения информации).

3. *По непосредственному источнику угроз.*

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

2) *Угрозы, источником которых является человек:*

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

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

- угроза несанкционированного копирования секретных данных пользователем АС;

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

3) *Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства:*

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

- возникновение отказа в работе операционной системы.

4) *Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства:*

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

- заражение компьютера вирусами с деструктивными функциями.

4. *По положению источника угроз.*

1) *Угрозы, источник которых расположен вне контролируемой зоны территории {помещения), на которой находится АС:*

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

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

- дистанционная фото- и видеосъемка.

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

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

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

- применение подслушивающих устройств.

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

4) *Угрозы, источник которых расположен в АС:*

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

- некорректное использование ресурсов АС.

5. *По степени зависимости от активности АС.*

1) *Угрозы, которые могут проявляться независимо от активности АС:*

- вскрытие шифров криптозащиты информации;

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

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

6. По степени воздействия на АС.

1) *Пассивные угрозы,* которые при реализации ничего не меняют в структуре и содержании АС (угроза копирования секретных данных).

2) *Активные угрозы,* которые при воздействии вносят изменения в структуру и содержание АС:

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

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

- угроза умышленной модификации информации.

7. *По пианам доступа пользователей или программ к ресурсам АС.*

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

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

8. *По способу доступа к ресурсам АС.*

1) *Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС:*

- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы и т.д.)

с последующей маскировкой под зарегистрированного пользователя ("маскарад");

- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.

2) *Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС:*

- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);

- угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС.

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

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

2) *Угрозы доступа к информации в оперативной памяти:*

– чтение остаточной информации из оперативной памяти;

– чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой зашиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных АС и систем программирования;

– угроза доступа к системной области оперативной памяти со сторон прикладных программ.

3) *Угрозы доступа к информации, циркулирующей в линиях связи:*

– незаконное подключение к линиям связи с целью работы во время пауз в действиях законного пользователя от его имени с вводом ложных сообщений или модификацией передаваемых сообщений;

– незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений;

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

4) *Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере* (например, угроза записи отображаемой информации на скрытую видеокамеру). Вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие свойства информации систем ее обработки.

В качестве основного критерия будем использовать аспект ИБ. привлекая при необходимости остальные.

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

Доступность информации – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующаяся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда возникает в этом необходимость.

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются *непреднамеренные ошибки* штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих ИС. Эти ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе), иногда они создают уязвимые места, которые используют злоумышленники (по данным до 65 % потерь – от непреднамеренных ошибок).

Другие *угрозы доступности* классифицируем по *компонентам ИС,* на которые нацелены угрозы:

- отказ пользователей;

- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно, применительно к *пользователям,* рассматриваются следующие угрозы: нежелание работать с информационной системой; невозможность работать с системой в силу отсутствия соответствующей подготовки; невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными *источниками внутренних отказов* являются: отступление 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 (пере) конфигурировании системы; отказы программного и аппаратного обеспечения; разрушение данных; разрушение или повреждение аппаратуры.

По *отношению к поддерживающей инфраструктуре* рекомендуется рассматривать следующие угрозы: нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования: разрушение или повреждение помещений; невозможность или нежелание обслуживающего персонала или пользователей выполнять свои обязанности.

Приведем некоторые примеры угроз и программных атак на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться *агрессивное потребление ресурсов* (обычно – полосы пропускания сетей, вычислительных возможностей процессоров или ОЗУ). По расположению источника угрозы такое *потребление* подразделяется на *локальное* и *удаленное.* При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме – как скоординированные распределенные атаки, когда на сервер с множества разных адресов

с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую, в том числе н несанкционированное изменение информации при случайных ошибках программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, периодическая запланированная коррекция некоторой базы данных).

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

Существует различие между *статической* и *динамической целостностью.* С целью нарушения статической целостности злоумышленник может: ввести неверные данные, изменить данные.

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить *"неотказуемость",* компьютерные данные не могут рассматриваться в качестве доказательства.

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

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

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает

полномочиями доступа к ней. В связи с данной угрозой используется термин "утечка".

Конфиденциа1ьность информации – субъективно определяемая (приписываемая) характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доспи к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочии доступа к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты их законных интересов от других субъектов информационных отношений.

Конфиденциальную информацию 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.

Многим субъектам приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. II дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей: рекомендации по их регулярной смене только усугубляют положение, заставляя применять несложные схемы чередования или стараться свести дело к двум-трем легко запоминаемым паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая зашита. Угроза же состоит в том, что кто-то не откажется угнать секреты, которые сами просятся в руки. 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 – получить 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.

Опасной нетехнической угрозой конфиденциальности являются *методы морально-психологического воздействия,* такие как *маскарад* – выполнение действий под видом лица, обладающего полномочиями для доступа к данным

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.

Таковы основные угрозы, которые наносят наибольший ущерб субъектам информационных отношений.

На современном этапе развития информационных технологий подсистемы или функции защиты являются неотъемлемой частью комплекса по обработке информации. Информация не представляется "в чистом виде", на пути к ней имеется хотя бы какая-нибудь система защиты, и поэтому чтобы угрожать, атакующая сторона должна преодолеть эту систему. Однако не существует абсолютно стойкой системы защиты, вопрос лишь во времени и средствах, требующихся на ее преодоление. Исходя из данных условий, примем следующую модель: *защита информационной системы считается преодоленной, если в ходе ее иссле-*

дования определены все уязвимости системы. Поскольку преодоление защиты также представляет собой угрозу, для защищенных систем будем рассматривать ее четвертый вид – *угрозу раскрытия параметров АС,* включающей в себя систему защиты. С точки зрения практики любое проводимое мероприятие предваряется этапом разведки, в ходе которого определяются основные параметры системы, ее характеристики, в результате чего уточняется поставленная задача и выбираются оптимальные технические средства.

Угрозу раскрытия можно рассматривать как опосредованную. Последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность реализоваться первичным или непосредственным угрозам, перечисленным выше. Введение данного вида угроз позволяет описывать с научно-методологической точки зрения отличия защищенных информационных систем от открытых. Для последних угроза разведки параметров системы считается реализованной.

Методы обеспечения информационной безопасности

При рассмотрении вопросов зашиты АС целесообразно использовать четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой АС информации, которая поможет систематизировать как возможные угрозы, так и меры по их нейтрализации и парированию, т.е. может систематизировать и обобщить весь спектр методов обеспечения зашиты, относящихся к информационной безопасности:

1) уровень носителей информации;
2) уровень средств взаимодействия с носителем;
3) уровень представления информации;
4) уровень содержания информации.

Данные уровни были введены исходя из того, что, во-первых, информация для удобства манипулирования чаше всего фиксируется на некотором материальном носителе, которым может быть бумага, дискета, CD-диск и т.п. Во-вторых, если способ представления информации таков, что она не может быть непосредственно воспринята человеком, возникает необходимость в преобразованиях информации в доступный для человека способ представления. Например, для чтения информации с дискеты не-

обходим компьютер, оборудованный дисководом соответствующего типа. В-третьих, информация может быть охарактеризована способом своего представления. Язык жестов, язык символов и другие – все это способы представления информации. В-четвертых, человеку должен быть доступен смысл представленной информации (семантика).

Защита носителей информации должна обеспечивать парирование всех возможных угроз, направленных как на сами носители, так и на зафиксированную на них информацию, представленную в виде изменения состояний отдельных участков, блоков, полей носителя. Применительно к АС защита носителей информации в первую очередь подразумевает защиту машинных носителей. Вместе с тем, необходимо учитывать, что носителями информации являются также каналы связи, документальные материалы, получаемые в ходе эксплуатации АС, и т.п. Защита средств взаимодействия с носителем охватывает спектр методов защиты программно-аппаратных средств, входящих в состав АС. таких как средства вычислительной техники, операционная система, прикладные программы. В основном защита на данном уровне рассматривается как защита от несанкционированного доступа, обеспечивающая разграничение доступа пользователей к ресурсам системы. Защита представления информации, т.е. некоторой последовательности символов, обеспечивается средствами криптографической зашиты. Защита содержания информации обеспечивается семантической зашитой данных.

Классификация злоумышленников

Возможности осуществления вредительских воздействий зависят от статуса злоумышленника по отношению к ИВС. Злоумышленником может быть:

• *разработчик ЛВС* (владеет наиболее полной информацией о программных и аппаратных средствах ИВС и имеет возможность внедрения "закладок" на этапах создания и модернизации систем, но не получает доступа на эксплуатируемые объекты ИВС):

• *сотрудник из числа обслуживающего персонала* (работники службы безопасности информации, системные и прикладные программисты, инженерно-технический персонал):

• *пользователь* (имеет общее представление о структуре ИВС и механизмах ее зашиты, но может осуществлять сбор информации методами традиционного шпионажа и попытками несанкционированного доступа);

• *постороннее лицо* (дистанционные методы шпионажа и диверсионная деятельность).

Основные направления и методы реализации угроз информационной безопасности

К *основным направлениям* реализации злоумышленником информационных угроз относятся:

• непосредственное обращение к объектам доступа;

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

• модификация средств зашиты, позволяющая реализовать угрозы ИБ:

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

Программно-технический уровень информационной безопасности

Программно-технические меры, т.е. меры, направленные на контроль компьютерных сущностей – оборудования, программ и/или данных – образуют последний и самый важный рубеж информационной безопасности. Напомним, что ущерб наносят в основном действия легальных пользователей, по отношению к которым процедурные регуляторы малоэффективны. Главные враги – некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

В связи с этим именно компьютер (особенно находящийся в составе сети) следует в первую очередь рассматривать в качестве объекта защиты, а конечного пользователя – в качестве ее наиболее вероятного потенциального нарушителя. Как следствие, под сомнение ставится обоснованность концепции реализованной системы защиты в современных универсальных ОС. Эта система зашиты заключается в построении распределенной схемы адми-

нистрирования механизмов зашиты, элементами которой, помимо администратора, выступают пользователи, имеющие возможность назначать и изменять права доступа к создаваемым ими файловым объектам.

На практике сегодня существует два подхода к обеспечению компьютерной безопасности:

1) использование только встроенных в ОС и приложения средств защиты;

2) применение, наряду со встроенными, дополнительных механизмов защиты. Этот подход заключается в использовании так называемых технических средств добавочной зашиты – программных, либо программно-аппаратных комплексов, устанавливаемых на защищаемые объекты.

Существующая статистика ошибок, обнаруженных в ОС, а также сведения о недостаточной эффективности встроенных в ОС и приложения механизмов зашиты, заставляет специалистов сомневаться в достижении гарантированной защиты от НС Д, при использовании встроенных механизмов, и все большее внимание уделять средствам добавочной зашиты информации.

Таким образом, важнейшим условием защищенности компьютерной информации является квалификация администраторов безопасности и сотрудников эксплуатирующих служб, которая, по крайней мере, не должна уступать квалификации злоумышленников, в противном случае не помогут никакие средства защиты.

Центральным для программно-технического уровня является понятие *сервиса безопасности*

Далее рассмотрим следующие *основные* и *вспомогательные* сервисы:

- *идентификация* и *аутентификация.*
- *управление доступом:*
- *протоколирование* и *аудит:*
- *шифрование:*
- *контроль целостности:*
- *экранирование:*
- *анализ защищенности:*
- обеспечение *отказоустойчивости:*
- обеспечение *безопасного восстановления:*

• *туннелирование:*

• *управление.*

Совокупность перечисленных выше сервисов безопасности называют полным набором. Считается, что его, в принципе, достаточно для построения надежной зашиты на программно-техническом уровне, правда, при соблюдении целого ряда дополнительных условий (отсутствие уязвимых мест, безопасное администрирование и т.д.).

Для проведения классификации сервисов безопасности и определения их места в обшей архитектуре меры безопасности можно разделить на следующие виды:

- *превентивные,* препятствующие нарушениям ИБ;
- меры *обнаружения нарушений:*
- *локализующие,* сужающие зону воздействия нарушений;
- меры по *выявлению нарушителя:*
- меры *восстановления* режима безопасности.

Большинство сервисов безопасности попадает в число превентивных. Аудит и контроль целостности способны помочь в обнаружении нарушений: активный аудит, кроме того, позволяет запрограммировать реакцию на нарушение с целью локализации и/или прослеживания. Направленность сервисов отказоустойчивости и безопасного восстановления очевидна. Управление играет инфраструктурную роль, обслуживая все аспекты ИС.

Идентификацию и *аутентификацию* можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация – это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и *двусторонней* (вза-

имной). Пример односторонней аутентификации – процедура входа пользователя в систему.

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

- что служит *аутентификатором* (т.е. используется для подтверждения подлинности субъекта):

- как организован (и защищен) обмен данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив, по крайней мере, одну из следующих сущностей:

- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);

- нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);

- нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., т.е. свои биометрические характеристики).

В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, т.е. от *перехвата, изменения* шили *воспроизведения* данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

Надежная идентификация и аутентификация затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно угнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора – с другой. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. *Единый вход в сеть* – это, в первую очередь, требование удобства для

пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Парольная аутентификация – проста и уже давно встроена в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организации уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности. Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы. Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Пароль можно угадать "методом грубой силы", используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

- *наложение технических ограничении* (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);

- *управление сроком действия паролей,* их периодическая смена;

- ограничение доступа к файлу паролей;

- ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");

- обучение пользователей;

- использование программных *генераторов паролей* (программа, основываясь на несложных правилах, порождает только благозвучные и. следовательно, запоминающиеся пароли).

Рассмотренные выше *пароли можно назвать многоразовыми;* их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются *одноразовые пароли.*

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты. Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

Биометрическая аутентификация представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации доста-

точно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

На наш взгляд, к биометрии следует относиться весьма осторожно. Необходимо учитывать, что она подвержена тем же угрозам, что и другие методы аутентификации. Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти. Во-вторых, биометрические методы не более надежны, чем база данных шаблонов. В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в "полевых" условиях, когда, например к устройству сканирования роговицы могут поднести муляж и т.п. В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Но главная опасность состоит в том, что любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.[i]

Защита информации в сети Интернет

Проблемы и риски информационной безопасности Источников, из которых может исходить угроза или несанкционированный доступ к вашим данным, существует несколько. Первые – это источники антропогенного характера. Сюда относятся действия различных субъектов. Они могут быть преднамеренными либо случайными. Они разделяются на внешний и внутренний типы. Первый означает незаконное вторжение постороннего лица из внешней сети общего назначения. Второй подразумевает собой действие изнутри, то есть со стороны сотрудника компании, к примеру. Все, что приводит к сбою или отказу работать программного и технического средства, относится к техногенным источникам. Здесь могут быть виноваты банальные ошибки про-

граммного обеспечения, устаревшие устройства или системы, сбои оборудования (кабельная или дисковая система, проблемы с сервером, рабочей станцией). Всегда следует делать поправку и на какие-то чрезвычайные обстоятельства, поэтому выделяют стихийные источники. К ним относятся как любые случаи форс-мажорного характера, так и всяческие природные катаклизмы.

Причин, по которым могут происходить утечка информации и осуществляться несанкционированный доступ к ней в сетях, достаточно много:

1. Она может быть перехвачена;
2. Модификация информации (изменение исходного документа или сообщения либо его абсолютная подмена с последующей отсылкой адресату);
3. Фальсификация авторства (если посылают любые данные от вашего имени);
4. К серверу аппаратуры или линии связи может быть осуществлено незаконное подключение;
5. Кто-то может замаскироваться под авторизованного пользователя и присвоить себе его данные и полномочия;
6. Вводятся новые пользователи;
7. После преодоления мер защиты носители информации и файлы могут быть скопированы;
8. Неправильное хранение архивных данных;
9. Некорректная работа обслуживающего персонала или пользователей;
10. Внедрение компьютерного вируса;
11. Недостатки вашей операционной системы или прикладных программных средств могут быть использованы против вас.

Когда вы передаете в сетях какие-то данные, то, прежде чем они достигнут адресата, им нужно пройти через множество других серверов и маршрутизаторов. Никакого отслеживания или контроля по пути при этом нет. Поэтому с информацией может произойти что угодно. Интернет по своей архитектуре дает возможность злоумышленникам полную свободу действий. Система интернет зарождалась как абсолютно корпоративная. Но получилось так, что со временем она стала оперировать не только сетями образовательного, коммерческого, государственного, ведомственного, военного характера, что сами по себе подразумевают

некий ограниченный доступ, но и простыми пользователями, которые легко получают прямой доступ в интернет с любого домашнего компьютера с помощью обычного модема и телефонной сети общего пользования. При этом используются единый стек протоколов TCP/IP и единое адресное пространство. Такая простота доступа в интернет негативным образом сказывается на безопасности информации в сетях. А хуже всего то, что вы можете даже и не узнать, что ваши файлы или программы были скопированы, не говоря уже о возможности их порчи и корректировки. Защита информации в интернете является одной из главных проблем любой крупной компании или организации. Те, кто более предусмотрителен, планируют, как должна осуществляется защита заблаговременно. Остальные задумываются об этом уже после первой неприятности.

Кому нужна система защиты информации? Любая организация или компания, которая хранит и обрабатывает данные в информационных системах, нуждается в средствах защиты информации: Финансово-кредитные организации; Коммерческие и государственные организации, у которых есть подключения в сетях общего пользования; Территориально-распределенные компании; Организации, которые вынуждены предоставлять внешний доступ к своим ресурсам информации; Операторы связи. Конечно, это далеко не весь перечень. И компании, которые вынуждены обезопасить свои информационные данные, становятся перед проблемой выбора между тем, насколько эффективной будет их работа в сетях, и необходимым уровнем защиты. Очень часто пользователи или потребители могут расценить такие меры безопасности как ограничение доступа либо снижение эффективности. Поэтому подбор средств для защиты информации каждая организация осуществляет индивидуально.

Классификация и обзор средств защиты.

Из-за того, что проблемы с безопасностью, как и источники угроз, бывают разными, возникла необходимость в создании различных видов ее обеспечения. Их классифицируют на несколько групп: Средства аппаратного (или технического) характера; Программные меры защиты; Средства, которые относят к смешанному виду; Меры организационного или административного характера. К первой группе относятся разные устройства. Они могут

быть электронными, механическими или электромеханическими, но специфика их работы предполагает защиту информации посредством аппаратных средств. Применение этих устройств позволит воспрепятствовать физическому проникновению или замаскировать данные, если доступ все же был открыт. Технические средства надежны, независимы от субъективных факторов и обладают высокой устойчивостью к модификации. Но у них есть и свои недостатки. В первую очередь это достаточно высокая цена. Также они недостаточно гибкие и практически всегда обладают большими массой и объемом. Второй вид оперирует разнообразными программами, для того чтобы контролировать доступ, проводить идентификацию пользователей, тестировать контроль системы защиты информации. Кроме того, средства, относящиеся к этой группе, могут шифровать данные и удалять рабочую (остаточную) информацию (вроде временных файлов). Если система использует программные средства для защиты, она получает массу преимуществ. Они гибкие и надежные, универсальные и достаточно просты в установке, а еще способны к модификации и предполагают определенное развитие. Однако этот вид средств очень чувствителен к случайным и преднамеренным изменениям. К другим недостаткам программной защиты можно отнести использование части ресурсов файл-сервера и рабочих станций, ограниченную функциональность сети и то, что ее средства могут зависеть от типа компьютера и его аппаратных средств. Третья группа сочетает в себе свойства первой и второй. В последний вид входят средства защиты информации организационно-технического и организационно-правового характера. Сюда можно отнести: Контроль доступа в помещения, их подготовку и оснащение; Разработку стратегий безопасности компании; Подборку и изучение национальных законодательств с последующим их применением; Учреждение правил работы и контроль их соблюдения. Полноценная защита информации в интернете может быть достигнута при использовании всех этих средств в комплексе.

Наиболее эффективные методы программных средств.

Для того чтобы обеспечить необходимую секретность, часто обращаются за помощью к специалистам по криптографии или шифрованию информации. При создании зашифрованных дан-

ных используют определенный алгоритм или устройство, которое его реализует. Изменяющийся код ключа осуществляет управление шифрованием. Именно с его помощью вы сможете извлечь информацию. Среди классических алгоритмов, которые используются, выделяют несколько основных: *Подстановка*. Она может быть как самой простой, одноалфавитной, так и многоалфавитной сложной (однопетлевой и многопетлевой); Перестановка. Различают простую и усложненную; *Гаммирование*. Речь идет о смешивании, в котором могут использовать длинную, короткую, неограниченную маски. В первом случае исходный алфавит заменяется альтернативными. Это самый легкий способ шифрования. Данные, зашифрованные алгоритмом перестановки, будут более защищенными, ведь в нем используются цифровые ключи или эквивалентные слова. Система, отдавшая предпочтение гаммированию, получит гарантию надежности и безопасности информации, потому что для осуществления этого способа шифрования будет проведена серьезная криптографическая работа. Для защиты используются нелинейные преобразования данных, методы рассечения-разнесения, компьютерная стеганография и прочее. К тому же существует различие между симметричным и несимметричным шифрованием. Первое означает, что для шифровки и дешифровки берутся одинаковые ключи (это называется система с закрытыми ключами). Тогда как система с открытыми ключами подразумевает собой использование открытого ключа для шифра и закрытого – для его расшифровки.

Если же вы хотите обезопасить себя от возможных модификаций или подмены информации, тогда стоит воспользоваться электронной цифровой подписью. Так называется тоже зашифрованное сообщение, только для его шифровки берется закрытый ключ. Еще стоит проводить аутентификацию. Это означает, что должна быть установлена подлинность каждого пользователя, который представил идентификатор, либо осуществлена проверка. Ведь сообщить этот идентификатор может и совсем другое устройство (лицо), а не тот пользователь, за которого оно себя выдает. В этих целях обычно используются пароли, секретные вопросы. Эффективной является схема одноразовых паролей. Не стоит путать аутентификацию с авторизацией. При прохождении авторизации проверяются полномочия или права пользователя на

то, имеет ли он доступ к конкретному ресурсу и может ли выполнять там какие-либо операции. Методы безопасности в компьютерных сетях. Если условно разделить все существующие средства защиты, то любая система должна обеспечить безопасность своих внутренних информационных ресурсов и защитить данные в процессе их передачи в интернете. К функциям первой области относятся межсетевые экраны (или брандмауэры – firewalls), которые устанавливают в разрыв всех соединений внутренней сети с глобальной. С их помощью можно разделить локальную сеть на две части или даже использовать МЭ для внутреннего деления, чтобы защитить одну подсеть от другой (особенно актуально такое решение для крупных организаций, где необходимы независимые подразделения). Система может пострадать из-за любого вторжения в ее ресурс, ведь злоумышленники используют всевозможные средства для этого. Ваши данные могут быть стерты с помощью вируса, под вашим именем кто-то получит доступ к операционной системе, прочтет конфиденциальную информацию, заменит ее ложной, выведет все устройства и оборудование из рабочего состояния. Поэтому межсетевой экран должен уметь распознать, какие пользователи являются легальными, а какие – нет, правильно провести классификацию сетевой активности, чтобы не допустить вредоносной, но и не помешать нужной. Набор правил, который будет сформирован, поможет определить условия, по каким пакеты должны проходить из одной части сети в другую.

Если же компании нужно обеспечить безопасность информации в сетях, которая уже находится «в пути», тогда обычно обращаются к помощи средств виртуальных частных сетей (VPN). Очень важно, чтобы передаваемые данные, до того как дойдут к месту назначения, не были искажены, уничтожены или просмотрены посторонними. Способы, используемые в этой области средств, тоже могут быть различными. Существуют разграничения трафика, его шифрование, так что если у кого-то и получится добраться до самого пользовательского IP-пакета, то он сможет лишь удалить его, но не прочитает, не исказит и не подменит данные. Компания, которая хочет защитить свои ресурсы самым надежным образом, должна применять комплексный подход. Кроме вышеназванных, понадобится система, которая будет

осуществлять обнаружение вторжений, предотвращать их, не допускать утечек конфиденциальной информации. Еще желательно использование средств мониторинга сетей, анализа и моделирования информационных потоков, качественных антивирусных программ, не нужно забывать об архивировании и дублировании данных, резервном копировании, анализаторах протоколов, организационных и административных мерах, которые бы помогли предотвратить физический доступ посторонних к ее информации.

Проблемы защиты информации

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 доступа в Internet.

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.

Этот переход можно осуществлять одновременно с процессом построения всемирной информационной сети общего пользования, на базе использования сетевых компьютеров, которые с помощью сетевой карты 10Base-T и кабельного модема обеспечивают высокоскоростной доступ (10 Мбит/с) к локальному Web-серверу через сеть кабельного телевидения.

Для решения этих и других вопросов при переходе к новой архитектуре Internet нужно предусмотреть следующее:

1. ликвидировать физическую связь между будущей Internet (которая превратится во Всемирную информационную сеть общего пользования) и корпоративными и ведомственными сетями, сохранив между ними лишь информационную связь через систему World Wide Web;

2. заменить маршрутизаторы на коммутаторы, исключив обработку в узлах IP-протокола и заменив его на режим трансляции кадров Internet, при котором процесс коммутации сводится к простой операции сравнения MAC-адресов;

3. 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.

Дилемма безопасности такова: приходится делать выбор между защищенностью вашего имущества и его доступностью для вас, а значит, и возможностью полезного использования.

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.

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.

Средства защиты информации

Сейчас вряд ли кому-то надо доказывать, что при подключении к Internet Вы подвергаете риску безопасность Вашей локальной сети и конфиденциальность содержащейся в ней информации. По данным CERT Coordination Center в 1999 году было зарегистрировано 2421 инцидентов – взломов локальных сетей и серверов. По результатам опроса, проведенного Computer Security Institute (CSI) среди 500 наиболее крупных организаций, компаний и университетов с 1995 число незаконных вторжений возросло на 48,9 %, а потери, вызванные этими атаками, оцениваются в 66 млн. долларов США.

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 тематиче-

ской подборкой материалов российской прессы и материалами Hack Zone (Zhurnal.Ru).

Не смотря на кажущийся правовой хаос в рассматриваемой области, любая деятельность по разработке, продаже и использованию средств защиты информации регулируется множеством законодательных и нормативных документов, а все используемые системы подлежат обязательной сертификации Государственной Технической Комиссией при президенте России.

Информационная безопасность в Internet

Архитектура Internet подразумевает подключение к внешним открытым сетям, использование внешних сервисов и предоставление собственных сервисов вовне, что предъявляет повышенные требования к защите информации.

В Internet-системах используется подход клиент-сервер, а главная роль на сегодняшний день отводится Web-сервису. Web-серверы должны поддерживать традиционные защитные средства, такие как аутентификация и разграничение доступа; кроме того, необходимо обеспечение новых свойств, в особенности безопасности программной среды и на серверной, и на клиентской сторонах.

Таковы, если говорить совсем кратко, задачи в области информационной безопасности, возникающие в связи с переходом на технологию Inernet. Далее мы рассмотрим возможные подходы к их решению.

Формирование режима информационной безопасности – проблема комплексная.

Меры по ее решению можно разделить на четыре уровня:

- законодательный (законы, нормативные акты, стандарты и т.п.);
- административный (действия общего характера, предпринимаемые руководством организации);
- процедурный (конкретные меры безопасности, имеющие дело с людьми);
- программно-технический (конкретные технические меры).

Заключение

Проблема защиты информации в Internet ставится и, с той или иной степенью эффективности, решается с момента появления сетей на основе протоколов семейства TCP/IP.

В эволюциях технологий защиты можно выделить три основных направления. Первое – разработка стандартов, имплиментирующих в сеть определенные средства защиты, прежде всего административной. Примером являются IP security option и варианты протоколов семейства TCP/IP, используемые в Министерстве обороны США. Второе направление – это культура межсетевых экранов (firewalls), давно применяемых для регулирования доступа к подсетям. Третье, наиболее молодое и активно развивающееся, направление – это так называемые технологии виртуальных защищенных сетей (VPN, virtual private network, или intranet).

Наблюдаемый в последние годы взрывной рост популярности Internet и связанных с ней коммерческих проектов послужил толчком для развития нового поколения технологий защиты информации в TCP/IP-сетях. Причем если ранее, вплоть до начала 90-х, основной задачей защиты в Internet было сохранение ресурсов преимущественно от хакерских атак, то в настоящее время актуальной становится задача защиты коммерческой информации.

Выбор технологии защиты информации для большой открытой системы – сети масштаба Internet, крупной корпоративной сети, сети коммуникационного провайдера, должен удовлетворять ряду специфических требований:

- наличие *открытой* спецификации, отсутствие монополизма в части технологических решений
- *широкая масштабируемость* решений по техническим и ценовым параметрам
- *универсальность технологии, переносимость, многоплатформенность*
- *совместимость* аппаратных, программных, коммуникационных решений
- обеспечение, при необходимости, *комплексной* защиты информации

- простота управления ключами и организации защищенных коммуникаций для вновь подключенных пользователей

Принципы защиты информации

Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на четыре основных типа:

- перехват информации – целостность информации сохраняется, но ее конфиденциальность нарушена;
- модификация информации – исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;
- подмена авторства информации;
- перехват сообщения с его изъятием.

Данная проблема может иметь серьезные последствия.

Например, кто-то может послать письмо от вашего имени (этот вид обмана принято называть спуфингом) или Web-сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров.

В соответствии с перечисленными проблемами при обсуждении вопросов безопасности под самим термином "безопасность" подразумевается совокупность трех различных характеристик обеспечивающей безопасность системы:

1. Аутентификация – это процесс распознавания пользователя системы и предоставления ему определенных прав и полномочий. Каждый раз, когда заходит речь о степени или качестве аутентификации, под этим следует понимать степень защищенности системы от посягательств сторонних лиц на эти полномочия.

2. Целостность – состояние данных, при котором они сохраняют свое информационное содержание и однозначность интерпретации в условиях различных воздействий. В частности, в случае передачи данных под целостностью понимается идентичность отправленного и принятого.

3. Секретность – предотвращение несанкционированного доступа к информации. В случае передачи данных под этим термином обычно понимают предотвращение перехвата информации.

Криптография

Для обеспечения секретности применяется шифрование, или криптография, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию можно только при наличии ключа.

В основе шифрования лежат два основных понятия: алгоритм и ключ. Алгоритм – это способ закодировать исходный текст, в результате чего получается зашифрованное послание. Зашифрованное послание может быть интерпретировано только с помощью ключа.

Очевидно, чтобы зашифровать послание, достаточно алгоритма. Однако использование ключа при шифровании предоставляет два существенных преимущества. Во-первых, можно использовать один алгоритм с разными ключами для отправки посланий разным адресатам. Во-вторых, если секретность ключа будет нарушена, его можно легко заменить, не меняя при этом алгоритм шифрования. Таким образом, безопасность систем шифрования зависит от секретности используемого ключа, а не от секретности алгоритма шифрования.

Многие алгоритмы шифрования являются общедоступными.

Количество возможных ключей для данного алгоритма зависит от числа бит в ключе. Например, 8-битный ключ допускает 256 (28) комбинаций ключей. Чем больше возможных комбинаций ключей, тем труднее подобрать ключ, тем надежнее зашифровано послание. Так, например, если использовать 128-битный ключ, то необходимо будет перебрать $2^{128} \sim= 10^{40}$ ключей, что в настоящее время не под силу даже самым мощным компьютерам. Важно отметить, что возрастающая производительность техники приводит к уменьшению времени, требующегося для вскрытия ключей, и системам обеспечения безопасности приходится использовать все более длинные ключи, что, в свою очередь, ведет к увеличению затрат на шифрование.

Поскольку столь важное место в системах шифрования уделяется секретности ключа, то основной проблемой подобных систем является генерация и передача ключа. Существуют две основные схемы шифрования: симметричное шифрование (его также иногда называют традиционным или шифрованием с секрет-

ным ключом) и шифрование с открытым ключом (иногда этот тип шифрования называют асимметричным).

При симметричном шифровании отправитель и получатель владеют одним и тем же ключом (секретным), с помощью которого они могут зашифровывать и расшифровывать данные. При симметричном шифровании используются ключи небольшой длины, поэтому можно быстро шифровать большие объемы данных. Симметричное шифрование используется, например, некоторыми банками в сетях банкоматов. Однако симметричное шифрование обладает несколькими недостатками. Во-первых, очень сложно найти безопасный механизм, при помощи которого отправитель и получатель смогут тайно от других выбрать ключ. Возникает проблема безопасного распространения секретных ключей. Во-вторых, для каждого адресата необходимо хранить отдельный секретный ключ. В третьих, в схеме симметричного шифрования невозможно гарантировать личность отправителя, поскольку два пользователя владеют одним ключом.

В схеме шифрования с открытым ключом для шифрования послания используются два различных ключа. При помощи одного из них послание зашифровывается, а при помощи второго – расшифровывается. Таким образом, требуемой безопасности можно добиться, сделав первый ключ общедоступным (открытым), а второй ключ хранить только у получателя (закрытый, личный ключ). В таком случае любой пользователь может зашифровать послание при помощи открытого ключа, но расшифровать послание способен только обладатель личного ключа. При этом нет необходимости заботиться о безопасности передачи открытого ключа, а для того чтобы пользователи могли обмениваться секретными сообщениями, достаточно наличия у них открытых ключей друг друга.

Недостатком асимметричного шифрования является необходимость использования более длинных, чем при симметричном шифровании, ключей для обеспечения эквивалентного уровня безопасности, что сказывается на вычислительных ресурсах, требуемых для организации процесса шифрования.

Электронная цифровая подпись

Даже если послание, безопасность которого мы хотим обеспечить, должным образом зашифровано, все равно остается возможность модификации исходного сообщения или подмены этого сообщения другим. Одним из путей решения этой проблемы является передача пользователем получателю краткого представления передаваемого сообщения. Подобное краткое представление называют ***контрольной суммой***, или ***дайджестом*** сообщения.

Контрольные суммы используются при создании резюме фиксированной длины для представления длинных сообщений. Алгоритмы расчета контрольных сумм разработаны так, чтобы они были по возможности уникальны для каждого сообщения. Таким образом, устраняется возможность подмены одного сообщения другим с сохранением того же самого значения контрольной суммы.

Однако при использовании контрольных сумм возникает проблема передачи их получателю. Одним из возможных путей ее решения является включение контрольной суммы в так называемую электронную подпись.

При помощи электронной подписи получатель может убедиться в том, что полученное им сообщение послано не сторонним лицом, а имеющим определенные права отправителем. Электронные цифровые подписи создаются шифрованием контрольной суммы и дополнительной информации при помощи личного ключа отправителя. Таким образом, кто угодно может расшифровать подпись, используя открытый ключ, но корректно создать подпись может только владелец личного ключа. Для защиты от перехвата и повторного использования подпись включает в себя уникальное число – порядковый номер. Более подробно об электронной цифровой подписи (ЭЦП) читайте в разделе курса ОСВМ Аутентификация информации

С 2012 года в Казахстане функционирует свой Национальный удостоверяющий центр, в котором граждане и организации Казахстана могут получить свои закрытые ключи и программные пакеты для формирования своей цифровой подписи для ведения электронных юридических операций с ее использованием. Необ-

ходимо, однако, заметить, что данная система еще очень сырая и позволяет злоумышленникам легко воспользоваться чужой электронной подписью для совершения подложных сделок. Это происходит по следующим причинам: выдача файлов электронных подписей совершается "вручную", то есть оператор, выдающий подпись всегда может иметь ее копию на своем USB-носителе, пароль выдается на всех один (!!!) – 123456. При попытке смены пароля файл электронной подписи записанный на стираемом носителе, фатально повреждается, и, если владелец подписи не сделал предварительно копию, то он лишается возможности подписывать документы до получения новой подписи из НУЦ, ЦОН или у программистов районного налогового комитета.

На сегодня уже известно множество фиктивных сделок с недвижимостью и иным имуществом, а также незаконным получением документов с помощью чужой электронной подписи. Поэтому, единственно разумным действием, предохраняющим человека от лишения его собственности, является безусловный отказ от получения ЭЦП, а если таковая уже получена, то подача заявления о ее утере (отказе от оной).

Аутентификация

Аутентификация является одним из самых важных компонентов организации защиты информации в сети. Прежде чем пользователю будет предоставлено право получить тот или иной ресурс, необходимо убедиться, что он действительно тот, за кого себя выдает.

При получении запроса на использование ресурса от имени какого-либо пользователя сервер, предоставляющий данный ресурс, передает управление серверу аутентификации. После получения положительного ответа сервера аутентификации пользователю предоставляется запрашиваемый ресурс.

При аутентификации используется, как правило, принцип, получивший название "что он знает", – пользователь знает некоторое секретное слово, которое он посылает серверу аутентификации в ответ на его запрос. Одной из схем аутентификации является использование стандартных паролей. Эта схема является наиболее уязвимой с точки зрения безопасности – пароль может быть перехвачен и использован другим лицом. Чаще всего ис-

пользуются схемы с применением одноразовых паролей. Даже будучи перехваченным, этот пароль будет бесполезен при следующей регистрации, а получить следующий пароль из предыдущего является крайне трудной задачей. Для генерации одноразовых паролей используются как программные, так и аппаратные генераторы, представляющие собой устройства, вставляемые в слот компьютера. Знание секретного слова необходимо пользователю для приведения этого устройства в действие. Одной из наиболее простых систем, не требующих дополнительных затрат на оборудование, но в то же время обеспечивающих хороший уровень защиты, является S/Key, на примере которой можно продемонстрировать порядок представления одноразовых паролей.

В процессе аутентификации с использованием S/Key участвуют две стороны – клиент и сервер. При регистрации в системе, использующей схему аутентификации S/Key, сервер присылает на клиентскую машину приглашение, содержащее зерно, передаваемое по сети в открытом виде, текущее значение счетчика итераций и запрос на ввод одноразового пароля, который должен соответствовать текущему значению счетчика итерации. Получив ответ, сервер проверяет его и передает управление серверу требуемого пользователем сервиса. Подробнее о технологии аутентификации

Защита сетей

В последнее время корпоративные сети все чаще включаются в Интернет или даже используют его в качестве своей основы. Учитывая то, какой урон может принести незаконное вторжение в корпоративную сеть, необходимо выработать методы защиты. Для защиты корпоративных информационных сетей используются брандмауэры. Брандмауэр – это система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Как правило, эта граница проводится между локальной сетью предприятия и Интернетом, хотя ее можно провести и внутри. Однако защищать отдельные компьютеры невыгодно, поэтому обычно защищают всю сеть.

Брандмауэр пропускает через себя весь трафик и для каждого проходящего пакета принимает решение – пропускать его или

отбросить. Для того чтобы брандмауэр мог принимать эти решения, для него определяется набор правил.

Брандмауэр может быть реализован как аппаратными средствами (то есть как отдельное физическое устройство), так и в виде специальной программы, запущенной на компьютере.

Как правило, в операционную систему, под управлением которой работает брандмауэр, вносятся изменения, цель которых – повышение защиты самого брандмауэра. Эти изменения затрагивают как ядро ОС, так и соответствующие файлы конфигурации. На самом брандмауэре не разрешается иметь разделов пользователей, а следовательно, и потенциальных дыр – только раздел администратора. Некоторые брандмауэры работают только в однопользовательском режиме, а многие имеют систему проверки целостности программных кодов.

Брандмауэр обычно состоит из нескольких различных компонентов, включая фильтры или экраны, которые блокируют передачу части трафика. Все брандмауэры можно разделить на два типа:

пакетные фильтры, которые осуществляют фильтрацию IP-пакетов средствами фильтрующих маршрутизаторов;

серверы прикладного уровня, которые блокируют доступ к определенным сервисам в сети.

Таким образом, брандмауэр можно определить как набор компонентов или систему, которая располагается между двумя сетями и обладает следующими свойствами:

- весь трафик из внутренней сети во внешнюю и из внешней сети во внутреннюю должен пройти через эту систему;

- только трафик, определенный локальной стратегией защиты, может пройти через эту систему;

В таком случае система надежно защищена от проникновения.

Кардинальным решением защиты локальной сети является ее полная (физическая) изоляция от иных сетей.

---

[i] 1. Составлено на основе материалов: Безбогов, А. А. Безопасность операционных систем : учебное пособие / А. А. Безбогов, А. В. Яковлев, Ю. Ф. Мартемьянов. – Москва: Машиностроение-1
2. Информация взята из: https://camafon.ru/informatsionnaya-bezopasnost/zashhita-v-internete