А.М. Голиков

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Томск

Федеральное агентство по образованию

Томский государственный университет
систем управления и радиоэлектроники

А.М. Голиков

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

2007

УДК 004.056(075.8)
ББК 65.247я73
Г60

Голиков А.М.
Г60 **О**сновы информационной безопасности: учебное пособие / А.М. Голиков. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. – 288 с.
ISBN 978-5-868889-467-1

Изложены основные понятия теории информационной безопасности, методология построения систем защиты автоматизированных информационных систем (АС), раскрывается понятие формальных политик безопасности. Дана классификация математических моделей информационной безопасности, рассмотрены основные дискреционные и мандатные модели, основные критерии защищенности АС, классы защищенности, включая международные стандарты, а также основные средства защиты информации, включая неформальные (законодательные, административные, процедурные) и формальные (программно-технические), Представлена типовая модель безопасности информационной сети предприятия, методы и средства аудита безопасности информационных систем, рассмотрены методы и средства аудита безопасности информационных систем.

Для студентов, обучающихся по специальностям: 210403 «Защищенные системы связи» и 090106 «Информационная безопасность телекоммуникационных систем».

УДК 004.056(075.8)
ББК 65.247я73

ISBN 978-5-868889-467-1

СОДЕРЖАНИЕ

Предисловие

Проблема защиты информации не нова. Она появилась вместе с компьютерами. Естественно, что стремительное совершенствование компьютерных технологий отразилось и на принципах построения защиты информации. Задачи изменились, а мнения остались прежние - так рождаются мифы. Вот несколько мифов компьютерной безопасности.

Миф первый. «Защита информации и криптография - близнецы-братья». Этот миф, видимо, связан с тем, что с самого начала своего развития системы информационной безопасности разрабатывались для военных ведомств. Разглашение такой информации могла привести к огромным жертвам, в том числе и человеческим. Поэтому конфиденциальности (т.е. неразглашению информации) в первых системах безопасности уделялось особое внимание. Очевидно, что надежно защитить сообщения и данные от подглядывания и перехвата может только полное их шифрование. Видимо, из-за этого начальный этап развития компьютерной безопасности прочно связан с криптошифрами.

Однако сегодня информация имеет уже не столь «убойную» силу, и задача сохранения ее в секрете потеряла былую актуальность. Сейчас главные условия безопасности информации - ее доступность и целостность. Любой файл или ресурс системы должен быть доступен в любое время (при соблюдении прав доступа). Если какой-то ресурс недоступен, то он бесполезен. Другая задача защиты - обеспечить неизменность информации во время ее хранения или передачи. Это так называемое условие целостности.

Таким образом, конфиденциальность информации, обеспечиваемая криптографией, не является главным требованием при проектировании защитных систем. Выполнение процедур криптокодирования и декодирования может замедлить передачу данных и уменьшить их доступность, так как пользователь будет слишком долго ждать свои "надежно защищенные" данные, а это недопустимо в некоторых современных компьютерных системах. Поэтому система безопасности должна в первую очередь гарантировать доступность и целостность информации, а затем уже (если необходимо) ее конфиденциальность. Принцип современной защиты информации можно выразить так - поиск оптимального соотношения между доступностью и безопасностью.

Миф второй. «Во всем виноваты хакеры». Этот миф поддерживают средства массовой информации, которые со всеми ужасающими подробностями описывают «взломы банковских сеток». Однако редко упоминается о том, что хакеры чаще всего используют некомпетентность и халатность обслуживающего персонала. Хакер - диагност. Именно некомпетентность пользователей можно считать главной угрозой безопасности. Также серьезную угрозу представляют служащие, которые чем-либо недовольны, например, заработной платой.

Одна из проблем подобного рода - так называемые слабые пароли. Пользователи для лучшего запоминания выбирают легко угадываемые пароли. Причем проконтролировать сложность пароля невозможно. Другая проблема - пренебрежение требованиями безопасности. Например, опасно использовать непроверенное программное обеспечение. Обычно пользователь сам «приглашает» в систему вирусы и «троянских коней». Кроме того, много неприятностей может принести неправильно набранная команда. Так, при программировании аппарата ФОБОС-1 ему с Земли была передана неправильная команда. В результате связь с ним была потеряна.

Таким образом, лучшая защита от нападения - не допускать его. Обучение пользователей правилам безопасности может предотвратить нападения. Другими словами, защита информации включает в себя кроме технических мер еще и обучение или правильный подбор обслуживающего персонала.

Миф третий. «Абсолютная защита». Абсолютной защиты быть не может. Распространено такое мнение – «установил защиту и можно ни о чем не беспокоиться». Полностью защищенный компьютер - это тот, который стоит под замком в бронированной

комнате в сейфе, не подключен ни к какой сети (даже электрической) и выключен. Такой компьютер имеет абсолютную защиту, однако, использовать его нельзя. В этом примере не выполняется требование доступности информации. «Абсолютности» защиты мешает не только необходимость пользоваться защищаемыми данными, но и усложнение защищаемых систем. Использование постоянных, не развивающихся механизмов защиты опасно, и для этого есть несколько причин.

Кроме того, нельзя забывать о развитии и совершенствовании средств нападения. Техника так быстро меняется, что трудно определить, какое новое устройство или программное обеспечение, используемое для нападения, может обмануть вашу защиту. Например, криптосистема DES, являющаяся стандартом шифрования в США с 1977 г., сегодня может быть раскрыта методом «грубой силы» - прямым перебором.

Компьютерная защита - это постоянная борьба с глупостью пользователей и интеллектом хакеров.

В заключение хочется сказать о том, что защита информации не ограничивается техническими методами. Проблема значительно шире. Основной недостаток защиты - люди, и поэтому надежность системы безопасности зависит в основном от отношения к ней служащих компании. Помимо этого, защита должна постоянно совершенствоваться вместе с развитием компьютерной сети. Не стоит забывать, что мешает работе не система безопасности, а ее отсутствие.

1. Структура теории информационной безопасности

1.1. Основные понятия теории информационной безопасности

Для того, чтобы определить эти понятия воспользуемся математической логикой. Пусть **А** конечный алфавит, *А* - множество слов конечной длины в алфавите **А.**

Из **А** при помощи некоторых правил выделено подмножество *Я* правильных слов, которое называется языком. Если $Я_1$ - язык описания одной информации, $Я_2$ - другой, то можно говорить о языке Я, объединяющем $Я_1$ и $Я_2$ описывающем ту и другую информацию. Тогда $Я_1$ и $Я_2$ подъязыки *Я.*

Будем считать, что любая информация представлена в виде слова в некотором языке *Я.* Кроме того, можно полагать, что состояние любого устройства в вычислительной системе достаточно полно описано словом в некотором языке. Тогда можно отождествлять слова и состояния устройств и механизмов вычислительной системы или произвольной электронной системы обработки данных (ЭСОД). Эти предположения позволяют весь анализ вести в терминах некоторого языка.

Определение: Объектом относительно языка Я называется произвольное конечное множество языка *Я.*

Пример 1: Пусть текст в файле разбит на параграфы так, что любой параграф также является словом языка *Я* и, следовательно, тоже является объектом. Таким образом, один объект может являться частью другого.

Пример 2: Принтер компьютера - объект. Существует некоторый (достаточно сложный) язык, описывающий принтер и его состояния в произвольный момент времени. Множество допустимых описаний состояний принтера является конечным подмножеством слов в этом языке. Именно это конечное множество и определяет принтер как объект.

Другими словами объект – это пассивная сущность (любая именованная составляющая компьютерной системы), используемая для хранения или получения информации. В качестве объекта могут выступать записи, блоки, байты, слова, страницы, сегменты, файлы, биты, директории, терминалы, узлы, сети и т.д.

В информации выделим описания преобразований данных. Преобразование информации отображает слово, описывающее исходные данные, в другое слово. Описание

преобразования данных также является словом. Примерами объектов, описывающих преобразования данных, являются программы для ЭВМ.

Каждое преобразование информации может:

а) храниться;

б) действовать.

В случае а) речь идет о хранении описания преобразования в некотором объекте (файле). В этом случае преобразование ничем не отличается от других данных. В случае б) описание программы взаимодействует с другими ресурсами вычислительной системы - памятью, процессором, коммуникациями и др.

Определение: Ресурсы системы, выделяемые для действия преобразования, называются доменом.

Однако для осуществления преобразования одних данных в другие кроме домена необходимо передать этому преобразованию особый статус в системе, при котором ресурсы системы осуществляют преобразование. Этот статус будем называть «управление».

Определение: Преобразование, которому передано управление, называется процессом.

При этом подразумевается, что преобразование осуществляется в некоторой системе, в которой ясно, что значит передать управление.

Определение: Объект, описывающий преобразование, которому выделен домен и передано управление, называется субъектом.

То есть субъект можно определить как активную сущность (любая именованная составляющая компьютерной системы), которая может инициировать запросы ресурсов и использовать их для выполнения каких – либо вычислительных заданий. Под субъектами обычно понимаю пользователя, процесс или устройство.

С одной стороны основную концепцию идентификации субъектов и объектов в системе описать просто, а вот с другой стороны, при практической реализации оказывается не тривиальной задачей определить: что есть субъект, а что – объект. Например, в ОС процессы, безусловно, являются субъектами, в то время как файлы и связанные с ними директории – объектами. Но, когда субъекты получают сигналы на выполнение каких – либо заданий от других субъектов, то возникает вопрос рассматривать их как субъекты или же, как объекты.

В процессе исполнения субъекты выполняют некоторые операции. В результате происходит взаимодействие субъектов и объектов.

Определение: Доступ – это взаимодействие между субъектами и объектами, результатом которого является перенос информации между ними.

Существует две базовые операции, переносящие информации между ними субъектами и объектами: чтение, запись. Под операцией чтения понимается операция, результатом которой является перенос информации от объекта к субъекту. Под операцией записи понимается операция, результатом которой является перенос информации от объекта к субъекту [1 – 7].

В заключение можно добавить аксиому: все вопросы безопасности информации описываются доступами субъектов к объектам.

1.2. Ценность информации

Чтобы защитить информацию, надо затратить силы и средства, а для этого надо знать какие потери мы могли бы понести. Ясно, что в денежном выражении затраты на защиту не должны превышать возможные потери. Для решения этих задач в информацию вводятся вспомогательные структуры - ценность информации. Рассмотрим примеры.

1. Аддитивная модель. Пусть информация представлена в виде конечного множества элементов и необходимо оценить суммарную стоимость в денежных единицах из оценок компонент. Оценка строится на основе экспертных оценок компонент, и, если денежные оценки объективны, то сумма дает искомую величину. Однако, количественная оценка

компонент не всегда объективна даже при квалифицированной экспертизе. Это связано с неоднородностью компонентов в целом. Поэтому делают единую иерархическую относительную шкалу (линейный порядок, который позволяет сравнивать отдельные компоненты по ценности относительно друг друга). Единая шкала означает равенство цены всех компонент, имеющих одну и туже порядковую оценку.

Пример: $0_1,...,0_n$ - объекты, шкала 1<...<5. Эксперты оценили (2, 1, 3,...., 4) - вектор относительных ценностей объектов. Если есть цена хотя бы одного объекта, например, C_1=100 руб., то вычисляется оценка одного балла C_1/λ. = 50 руб.,

где λ - число баллов оценки первого объекта, и вычисляется цена каждого следующего объекта: C_2=50руб., C_3=150 руб. и т.д. Сумма дает стоимость всей информации. Если априорно известна цена информации, то относительные оценки в порядковой шкале позволяют вычислить цены компонент.

2. Порядковая шкала ценностей. Далеко не всегда возможно и нужно давать денежную оценку информации. Например, оценка личной информации, политической информации или военной информации не всегда разумна в денежном исчислении. Однако подход, связанный со сравнением ценности отдельных информационных элементов между собой, по-прежнему имеет смысл.

Пример: При оценке информации в государственных структурах используется порядковая шкала ценностей. Все объекты (документы) государственного учреждения разбиваются по грифам секретности. Сами грифы секретности образуют порядковую шкалу: несекретно < для служебного пользования <секретно < совершенно секретно (НС<ДСП<С<СС) или у американцев : unclassified<confidential<secret<top secret (U<Conf<S<TS). Более высокий класс имеет более высокую ценность и поэтому требования по его защите от несанкционированного доступа более высокие.

1.3. Анализ угроз информационной безопасности

Информация с точки зрения информационной безопасности обладает следующими категориями:

- *конфиденциальность* – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации
- *целостность* – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения
- *аутентичность* – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения
- *апеллируемость* – довольно сложная категория, но часто применяемая в электронной коммерции – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора, кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается «откреститься» от своих слов, подписанных им однажды.

В отношении информационных систем применяются иные категории:

- *надежность* – гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано
- *точность* – гарантия точного и полного выполнения всех команд
- *контрол*ь доступа – гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются

- *контролируемость* – гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса
- *контроль идентификации* – гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает
- *устойчивость к умышленным сбоям* – гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

Под угрозой обычно понимают потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Исследователи предложили выделить три различных типа угроз. А именно, было отмечено, что наиболее общие угрозы вычислительным системам могут быть рассмотрены как относящиеся к раскрытию, целостности или отказу служб вычислительной системы.

Угроза конфиденциальности. Заключается в том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности данная угроза имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой раскрытия используется термин «утечка».

В руководстве по использованию стандарта защиты информации американцы говорят, что существует только два пути нарушения конфиденциальности:

утрата контроля над системой защиты;

каналы утечки информации.

Если система обеспечения защиты перестает адекватно функционировать, то, естественно, траектории вычислительного процесса могут пройти через состояние, когда осуществляется запрещенный доступ. Каналы утечки характеризуют ту ситуацию, когда-либо проектировщики не смогли предупредить, либо система не в состоянии рассматривать такой доступ как запрещенный. Утрата управления системой защиты может быть реализована оперативными мерами и здесь играют существенную роль административные и кадровые методы защиты. Утрата контроля над защитой может возникнуть в критической ситуации, которая может быть создана стихийно или искусственно. Поэтому одной из главных опасностей для системы защиты является отсутствие устойчивости к ошибкам.

Утрата контроля может возникнуть за счет взламывания защиты самой системы защиты. Противопоставить этому можно только созданием защищенного домена для системы защиты.

Большой спектр возможностей дают каналы утечки. Основной класс каналов утечки в - каналы по памяти (т.е. каналы, которые образуются за счет использования доступа к общим объектам системы).

Угроза целостности. Нарушения целостности информации - это незаконные уничтожение или модификация информации.

Традиционно защита целостности относится к категории организационных мер. Основным источником угроз целостности являются пожары и стихийные бедствия. К уничтожению и модификации могут привести также случайные и преднамеренные критические ситуации в системе, вирусы, «троянские кони» , случайная ошибка и т.д.

Но не исключены санкционированные изменения, т.е. такие, которые сделаны определенными лицами с обоснованной целью (таким изменением является периодическая запланированная коррекция некоторой базы данных).

Некоторое время условно считалось, что правительства сосредотачивались на раскрытии, а деловые круги касались целостности. Но, обе эти стороны могли бы быть более или менее связаны каждой из двух угроз в зависимости от приложения.

Угроза отказа служб. Возникает всякий раз, когда в результате преднамеренных действий, предпринятых другим пользователем, умышленно блокируется доступ к некоторому ресурсу вычислительной системы. То есть, если один пользователь запрашивает

доступ к службе, а другой предпринимает что-либо для недопущения этого доступа, мы говорим, что имеет место отказ службы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, что бы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Кроме перечисленных основных видов угроз существуют и другие, которые принято классифицировать по ряду признаков.

1. *По природе возникновения.*

1.1. Естественные угрозы (независящих от человека: стихийные бедствия, магнитные бури. радиоактивное излучение и т.п.).

1.2. Искусственные угрозы (вызванные деятельностью человека: внедрение агентов в число персонала системы; подкуп, шантаж и т.п. персонала или отдельных пользователей; несанкционированного копирования секретных данных; разглашение, передача или утрата паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

2. *По степени преднамеренности проявления*. .

2.1. Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала (проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2.2. Угрозы преднамеренного действия (угрозы действий злоумышленника для хищения информации).

3. *По положению источника угроз*.

3.1. Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС. (перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, дистанционная фото- и видеосъемка).

3.2. 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).

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

3.4. 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).

4. *По степени зависимости от активности АС*.

4.1. Угрозы, которые могут проявляться независимо от активности АС.(вскрытие шифров криптозащиты информации; хищение магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем).

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

5. *По степени воздействия на АС.*

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

5.2. Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС. (Например, внедрение "закладок" и "вирусов"; изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.)

6. *По этапам доступа пользователей или программ к ресурсам АС.*

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

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

7. *По способу доступа к ресурсам АС.*

7.1. Угрозы, направленные на использование прямого стандартного пути

доступа к ресурсам АС. (незаконное получение паролей и других реквизитов разграничения доступа; несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики)

7.2. 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.); доступ к ресурсам АС путем использования недокументированных возможностей ОС).

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

8.1. Угрозы доступа к информации на внешних запоминающих устройствах (например, угроза несанкционированного копирования секретной информации с жесткого диска). 8.2. Угрозы доступа к информации в оперативной памяти. (чтение остаточной информации из оперативной памяти; угроза доступа к системной области оперативной памяти со стороны прикладных программ.)

8.3. Угрозы доступа к информации, циркулирующей в линиях связи. (незаконное подключение к линиям связи с целью 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).

8.4. 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 ликвидированы три основные угрозы (конфиденциальности, целостности и доступности).

1.4. Структура теории информационной безопасности

Основные уровни защиты информации

При рассмотрении вопросов защиты АС обычно используют четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой АС информации. Это позволяет систематизировать и обобщить весь спектр методов обеспечения защиты, относящихся к информационной безопасности. Перечислим основные уровни защиты информации:

- уровень носителей информации;
- уровень средств взаимодействия с носителем;
- уровень представления информации;
- уровень содержания информации.

Данные уровни были введены по следующим соображениям: во-первых, информация для удобства манипулирования чаще всего фиксируется на некотором материальном носителе, которым может быть бумага, дискета или что-нибудь в этом роде. Во-вторых, если способ представления информации таков, что она не может быть непосредственно воспринята человеком, возникает необходимость в преобразователях информации в доступный для человека способ представления.

Защита магнитных носителей информации (МНИ)

Проблема защиты машинных носителей информации (МНИ) в АС, решается в основном за счет организационно-режимных мер, делающих невозможным или существенно ограничивающим доступ злоумышленников к МНИ и документальным материалам АС. Одним из наиболее надежных подходов к защите НИИ является их физическая защита. В то же время защита МНИ имеет специфику, определяемую их реализацией и организацией.

Независимо от типа носителя, данные на носителях хранятся блоками (секторами, кластерами и т.п.). Как известно, для доступа к данным МНИ существуют два основных способа:

- последовательный доступ, когда блоки записываются друг за другом и для чтения следующего нужно пройти все предыдущие;
- прямой (произвольный) доступ, отличающийся тем, что блоки записываются и читаются в произвольном порядке.

Например, дисковые накопители являются устройствами произвольного доступа, накопители на магнитной ленте - последовательного доступа. Кроме этого, МНИ характеризуются:

- различными физическими принципами реализации;
- широким спектром объемов хранимой информации - от единиц до десятков тысяч мегабайт;
- многообразием конкретных реализаций носителей различными производителями.

Злоумышленник не может получить доступ к информации на машинном носителе в двух случаях:

1. когда злоумышленнику недоступен сам носитель;
2. когда злоумышленнику доступен носитель, но отсутствуют соответствующие средства взаимодействия с носителем.

Основными задачами обеспечения информационной безопасности АС от угрозы раскрытия конфиденциальности на уровне МНИ являются:

1. исключение прохождения носителей по технологическим участкам, не обусловленным производственной необходимостью;
2. предупреждение непосредственного доступа к носителям персонала, не отвечающего за операции с носителями (минимизация доступа), предупреждение утраты или хищения носителей информации.

Первая задача решается за счет рациональной организации производственного процесса движения носителей информации, обеспечивающего целенаправленное распределение носителей по технологическим участкам, вторая - за счет четкой и обоснованной регламентации порядка обращения с носителями.

При обеспечении сохранности информационных ресурсов персональных компьютеров многое зависит от выбора методов защиты информации на гибких, магнитных дисках (дискетах) от несанкционированного копирования.

Помимо классического изменения структуры дискеты (привязки к временным параметрам чтения и записи, нестандартной разметки дорожек и изменения межсекторной дистанции) можно предложить использовать методы кодирования информации, хранящейся на гибком диске, в соответствии с алгоритмом криптографического преобразования по ГОСТу 28147-89.

Алгоритм криптографического преобразования предназначен для аппаратной или программной реализации, удовлетворяет криптографическим требованиям, а его возможности не накладывают ограничений на применение. Устанавливая единый алгоритм криптографического преобразования для систем обработки информации, он определяет правила шифрования данных и выработки имитоприставки и рекомендован для организаций, предприятий и учреждений, применяющих криптографическую защиту информации,

хранимой и передаваемой в сетях ЭВМ, в отдельных вычислительных комплексах или отдельных компьютерах.

Режим гаммирования[1] с обратной связью был выбран как обеспечивающий наибольшую криптостойкость системы: в результате сцепления блоков информации

изменение одного бита во входном информационном потоке приводит к изменению всего выходного потока, так как кодирование каждого блока информации зависит от кодирования предыдущего блока.

Для более ясного понимания сути метода защиты информации на гибких магнитных дисках от копирования рассмотрим отличия стандартной структуры дискеты и структуры, реализованной в данном методе.

На стандартной дискете после форматирования можно выделить четыре основные области, а именно: загрузочный сектор (boot area), область таблицы размещения файлов (FAT area), корневой каталог (directory area) и область данных (data area). Загрузочный сектор всегда является первым сектором на дискете, именно сюда записывается информация о том, как организована дискета. За счет этого операционная система позволяет работать с большим набором по-разному организованных гибких дисков.

Назначение некоторых байтов загрузочного сектора, которые описывают организацию дискеты, приведены ниже:

11-12 байты — число байтов в секторе;
13 байт — число секторов в кластере;
14-15 байты — число резервных секторов;
16 байт — число копий FAT;
17-18 байты — число позиций в корневом каталоге;
19-20 байты — число секторов на диске;
21 байт — код типа диска.

Следующая важная область — FAT, в которой операционная система назначает секторы для размещения различных файлов. Здесь для каждого сектора имеется своя запись,

---

[1] Во второй половине XIX в. появился весьма устойчивый способ усложнения числовых кодов - *гаммирование.* Он заключался в перешифровании закодированного сообщения с помощью некоторого ключевого числа, которое и называлось *гаммой.* Шифрование с помощью гаммы состояло в сложении всех кодированных групп сообщения с одним и тем же ключевым числом. Эту операцию стали называть *"наложениемгаммы"*. Например, результатом наложения гаммы 6413 на кодированный текст 3425 71028139 являлась числовая последовательность 9838 3515 4552:

3425 7102 8139
\+ 6413 6413 6413
9838 3515 4552

Единицы переноса, появляющиеся при сложении между кодовыми группами, опускались. *"Снятие гаммы"* являлось обратной операцией:

9838 3515 4552
\- 6413 6413 6413
3425 7102 8139

в 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, обозначил греческой буквой X любую букву шифрованного текста, греческой буквой Г любую букву гаммы и строчной буквой *с* любую букву открытого текста. Он, по сути, *доказал,* что алгебраическая формула

x = (c+r)mod26

воспроизводит зашифрование по Виженеру при замене букв алфавита числами согласно следующей таблице: (в таблице каждой букве латинского алфавита соответствовала цифра совподающая с порядковым номером буквы в алф.).

Тем самым была заложена алгебраическая основа для исследования шифров замены типа шифра Виженера. Используя уравнение шифрования, можно было отказаться от громоздкой таблицы Виженера.

Позже лозунговая гамма стала произвольной последовательностью, а шифр с уравнением шифрования (1) стал называться *шифром гаммирования.*

содержащая информацию о том, занят сектор файлом или нет, если да, то каким именно, а также указывается информация о поврежденных секторах.

Размер таблицы размещения файлов зависит от размера диска: чем выше его емкость, тем больший размер должен быть у таблицы для хранения информации обо всех секторах диска. Для большей надежности подобных таблиц может быть несколько (обычно для стандартной дискеты 3,5" емкостью 1,44 Мб их две).

В корневом каталоге хранится информация о файлах, каталогах, времени и дате их создания, размерах и другие необходимые сведения. Каждой позиции каталога отводится 32 байта, назначение которых приведено ниже:

1-8 — имя файла;
9—11 байты — расширение имени;
12 байт — атрибуты файла;
13-22 байты — в резерве операционной системы;
23-24 байты — время создания;
25-26 байты — дата создания;
27-28 байты — начальный кластер;
29-32 байты — размер файла.

Все остальное дисковое пространство является областью данных, в которой хранится информация.

Использование метода защиты информации на гибких магнитных дисках от копирования подразумевает создание структуры дискеты, отличной от стандартной.

При форматировании дискеты создаются следующие разделы: системная область и область данных. В системной области указывается размер файла в байтах, его имя и расширение, пароль, с которым данный файл был зашифрован, информация о порядке расположения секторов и поврежденных секторах. Системная область и область с данными хранятся в зашифрованном виде.

На стандартных дискетах DOS при записи файлов формирует таблицу их размещения, в которой указывается последовательность расположения секторов для каждого файла. Применение классического метода изменения параметров дисковода пресекает возможность просмотра дискеты обычными средствами, которые работают со стандартными форматами дискет, в результате чего такую дискету нельзя скопировать без специальных программ.

Применяя программу DISK EXPLORER, можно проанализировать логическую структуру дискеты и, прочитав каждый сектор, сделать отдельные копии секторов, находящихся на дискете после изменения параметров дисковода. Но получение полного объема информации в этом случае не представляется возможным, поскольку последовательность расположения секторов с данными пользователю не известна, а определение нужной последовательности потребует перебора множества комбинаций. К тому же каждый сектор кодирован в режиме гаммирования с обратной связью, и его декодирование будет зависеть от декодирования предыдущего сектора.

Для того чтобы изменить режим работы дисковода, необходимо модифицировать содержимое определенных ячеек оперативной памяти. По адресу 0000h:0078h находится указание на таблицу данных, которые используются контроллером дисковода при работе с дискетой, и изменение этих параметров позволит работать с нестандартными форматами дискет.

В данном методе используется форматирование с параметрами, отличающимися для каждого сектора. Два сектора используются для хранения системной информации (размер, полное имя файла, данные о порядке следования секторов и поврежденных секторах, пароль, с которым был зашифрован файл).

Во время форматирования проверяется качество записи и считывания сектора, так как из-за потенциального наличия на дискете поврежденных секторов на ней может измениться допустимый объем. После этого вычисляется свободный объем на диске и сверяется с размером записываемого файла.

При восстановлении файла у пользователя запрашивается пароль, посредством которого декодируется системная область и проверяется пароль, полученный в процессе декодирования. При несовпадении работа завершается. В случае положительного результата выставляются новые параметры для дисковода, и происходит декодирование файла, записанного на диск.

Основным преимуществом разработанного метода является высокая криптографическая стойкость информации, записываемой на гибкий магнитный диск, которая достигается благодаря применению алгоритма криптографического преобразования, основанного на ГОСТе 28147-89. Применение согласно этому ГОСТу дополнительного режима выработки имитоприставки обеспечивает защиту находящейся на диске информации от изменений и имитации.

По сравнению с существующими стандартными программами для персональных компьютеров время чтения и записи сокращено в них на 10 %.

Особое внимание следует уделять любым носителям информации, покидающим пределы фирмы. Наиболее частыми причинами этого бывают ремонт аппаратуры и списание технологически устаревшей техники. Необходимо помнить, что на рабочих поверхностях носителей даже в удаленных областях находится информация, которая может представлять либо непосредственный интерес, либо косвенно послужить причиной вторжения в систему. Так, например, при использовании виртуальной памяти часть содержимого ОЗУ записывается на жесткий диск, что теоретически может привезти даже к сохранению пароля на постоянном носителе (хотя это и маловероятно). Ремонт, производимый сторонними фирмами на месте, должен производится под контролем инженера из службы информационной безопасности. Необходимо помнить, что при нынешнем быстродействии ЭВМ копирование файлов производится со скоростью, превышающей мегабайт в секунду, а установить второй жесткий диск для копирования в момент ремонта без надзора специалиста можно практически незаметно. Все носители информации, покидающие фирму должны надежно чиститься либо уничтожаться механически (в зависимости от дальнейших целей их использования).

И еще немного слов о защищенности самих носителей информации. На сегодняшний день не существует разумных по критерию «цена/надежность» носителей информации, не доступных к взлому. Строение файлов, их заголовки и расположение в любой операционной системе может быть прочитано при использовании соответствующего программного обеспечения. Практически невскрываемым может быть только энергонезависимый носитель, автоматически разрушающий информацию при попытке несанкционированного подключения к любым точкам, кроме разрешенных разъемов, желательно саморазрушающийся при разгерметизации, имеющий внутри микропроцессор, анализирующий пароль по схеме без открытой передачи. Однако, все это из области «сумасшедших» цен и военных технологий.

Для бизнес класса и частной переписки данная проблема решается гораздо проще и дешевле – с помощью криптографии. Любой объем информации от байта до гигабайта, будучи зашифрован с помощью более или менее стойкой криптосистемы, недоступен для прочтения без знания ключа. И уже совершенно не важно, хранится он на жестком диске, на дискете или компакт-диске, не важно под управлением какой операционной системы. Против самых новейших технологий и миллионных расходов здесь стоит математика, и этот барьер до сих пор невозможно преодолеть. Вот почему силовые ведомства практически всех стран, будучи не в состоянии противостоять законам математики, применяют административные меры против так называемой стойкой криптографии. Вот почему ее использование частными и юридическими лицами без лицензии Федерального агентства по связи и информации

(ФАПСИ), входящего в структуру одного из силовых ведомств государства, запрещено и у нас в России.

1.5. Основные виды атак на АС

Атака на компьютерную систему – это действие, предпринятое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости.

Основные виды атак:

1. *Вмешательство человека в работу АС*. К этому виду относятся организационные средства нарушения безопасности АС (кража носителей информации, несанкционированный доступ (НСД) к устройствам хранения и обработки информации, порча оборудования и т.д.) и осуществление нарушителем НСД к программным компонентам АС (все способы НСД в АС, а также способы получения нарушителем незаконных прав доступа к компонентам АС). Меры, противостоящие таким атакам, носят организационный характер (охрана, режим доступа к АС), а также включает в себя совершенствование систем обнаружения попыток атак (попыток подбора паролей).

2. *Аппаратно–техническое вмешательство в работу АС*. Т.е. нарушение безопасности и целостности информации в АС с помощью технических средств, например, получение информации по электромагнитному излучению устройств АС. Защита от таких угроз, кроме организационных мер, предусматривает соответствующие аппаратные (экранирование излучений аппаратуры) и программные меры (шифрация).

3. *Разрушающее воздействие на программные компоненты АС с помощью программных средств* (разрушающих программных средств (РПС)). К ним относятся компьютерные вирусы, троянские кони, закладки, «логическая бомба», «часовая мина». Средства борьбы с подобными атаками программно реализованных средств защиты.

Последний вид атак развивается более динамично, используя все последние достижения в области информационных достижений. Остановимся на нем более детально и дадим краткое описания некоторых РПС.

«Логические бомбы» и *«часовые мины»* - Это РПС, которые не выполняют никаких функций до наступления определенного события в системе, после чего «срабатывают», что, как правило, заключается в серьезных нарушениях работы системы, уничтожении информации.

«Троянский конь» - программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условного срабатывания. Обычно такие программы маскируются под какие – нибудь полезные утилиты, игровые программы, картинки или музыку.

Закладки также содержат некоторую функцию, наносящую ущерб АС, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

В качестве примера приведем некоторые функции, реализуемые троянскими конями и закладками:

1. Уничтожение информации. Конкретный выбор объектов и способов уничтожения зависит от фантазии автора такой программы и возможностей ОС
2. Перехват и передача информации.
3. Целенаправленная модификация кода программы, интересующая нарушителя. Обычно это программы, реализующие функции безопасности и защиты.

Компьютерный вирус – программа, которая может заражать другие программы, модифицируя их посредством добавления своей, возможно измененной, копии. Способен к саморазмножению, при этом «копии» вируса могут структурно и функционально различаться между собой.

В настоящее время в мире насчитывается более 40 тысяч только зарегистрированных компьютерных вирусов. Все компьютерные вирусы могут быть классифицированы по следующим признакам:

1. по среде обитания;
2. по способу заражения;
3. по степени опасности деструктивных (вредительских) воздействий;
4. по алгоритму функционирования.

По среде обитания вирусы делятся так же на:

1. сетевые;
2. файловые;
3. загрузочные;
4. комбинированные;

Средой обитания сетевых вирусов являются элементы компьютерных сетей. Файловые вирусы размещаются в исполняемых файлах. Загрузочные вирусы находятся в загрузочных секторах (областях) внешних запоминающих устройств (boot - секторах). Комбинированные вирусы размещаются в нескольких средах обитания. Примером таких вирусов служат загрузочные файловые вирусы. Эти вирусы могут размещаться как в загрузочных секторах накопителей на магнитных дисках, так и в теле загрузочных файлов.

По способу заражения среды обитания компьютерные вирусы делятся на:

1. резидентные;
2. нерезидентные.

Резидентные вирусы после их активации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ. Эти вирусы, используя привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию. *Нерезидентные вирусы* попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют вредительскую функцию и функцию заражения. Затем вирусы полностью покидают оперативную память, оставаясь в среде обитания. Если вирус помещает в оперативную память программу, которая не заражает среду обитания, то такой вирус считается нерезидентным.

Арсенал вредительских возможностей вирусов весьма обширен. Деструктивные возможности вирусов зависят от целей и квалификации их создателя, а так же от особенностей компьютерных систем.

По степени опасности для информационных ресурсов пользователя компьютерные вирусы делятся на:

1. безвредные вирусы;
2. опасные вирусы;
3. очень опасные вирусы.

Безвредные вирусы создаются авторами, которые не ставят себе цели нанести какой – либо ущерб ресурсам компьютерной системы (АС). Деструктивное воздействие таких вирусов сводиться к выводу на экран монитора невинных картинок, исполнению музыкальных фрагментов. Но при всей своей безобидности они расходуют ресурсы системы, в какой – то степени снижая эффективность функционирования, могут содержать ошибки, приводящие к нарушению алгоритма работы системы.

К *опасным* относятся вирусы, которые вызывают существенное снижение эффективности АС, но не приводящие к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах. В пример можно привести вирусы, вызывающие необходимость повторного выполнения программ, перезагрузки операционной системы.

Очень опасными следует считать вирусы, вызывающие нарушение конфиденциальности, уничтожение, необратимую модификацию информации, а так же вирусы, блокирующие доступ к информации, приводящие к отказу аппаратных средств.

Одним из основных условий безопасной работы АС является соблюдение ряда правил.

Правило 1: периодически обновляйте вашу антивирусную программу

Антивирусные сканеры способны защищать только от тех компьютерных вирусов, данные о которых содержатся в антивирусной базе. Конечно, существуют механизмы поиска и неизвестных вирусов (т.е. тех, описаний которых нет в антивирусной базе).. Однако это все равно слишком мало для того, чтобы считаться абсолютной защитой.

В связи с этим первоочередную важность приобретает необходимость регулярно обновлять антивирусные базы. Чем чаще будете это делаться, тем более защищенным будет рабочее место. Наиболее оптимальным решением является ежедневная загрузка обновлений, хотя бывают случаи, когда за день появляется сразу несколько обновлений. В связи с этим, рекомендуют настроить внутренний планировщик, присутствующий в большинстве современных антивирусных программ, на автоматическую загрузку обновлений 2 или 3 раза в день: утром, днем и вечером.

Правило 2: будьте осторожны с файлами в письмах электронной почты

Вряд ли стоит акцентировать внимание на том, что ни в коем случае нельзя запускать программы, присланные неизвестным лицом. Это правило является общеизвестным и не нуждается в пояснениях.

Другое дело файлы, полученные от знакомых, коллег, друзей. Во-первых, посланные ими программы могут быть инфицированы. Во-вторых, знакомые могут даже и не знать, что с их компьютера несанкционированно отправляются письма: вирус может это делать от чужого имени незаметно для владельца компьютера! Именно таким способом, к примеру, распространялись такие известные вирусы, как LoveLetter, Melissa и многие другие. Они незаметно получали доступ к адресной книге почтовой программы Outlook и рассылали свои копии по найденным адресам электронной почты, сопровождая послания завлекательными комментариями, призывающими запустить вложенный файл.

Не менее важным моментом является кажущаяся безопасность вложенных файлов определенного формата. Думаете, файлы с расширением PIF, GIF, TXT не могут содержать вредоносных программ? Даже в таких «безобидных» программах могут быть замаскированы вирусы.

Правило 3: ограничьте круг пользующихся компьютером

Идеальным вариантом является ситуация, когда никто, кроме самого владельца, не имеет доступа к компьютеру. Однако если это невозможно, то необходимо четко разграничить права доступа и определить круг разрешенных действий для других лиц. В первую очередь это касается работы с мобильными носителями, Интернет и электронной почтой. В данном случае важно контролировать все источники вирусной опасности и отрезать от них других пользователей.

Правило 4: своевременно устанавливайте «заплатки» установленному ПО

Многие вирусы используют “дыры” в системах защиты операционных систем и приложений. Антивирусные программы способны защищать от такого типа вредоносных программ, даже если на компьютере не установлена соответствующая “заплатка”, закрывающая “дыру”. Несмотря на это, рекомендуется регулярно проверять Web-сайты производителей установленного программного обеспечения и следить за выпуском новых “заплаток”. В первую очередь, это правило относится к операционной системе Windows и другим программам корпорации Microsoft. Нет, совсем не потому, что у этой компании самые худшие продукты, а потому, что они наиболее распространены и, соответственно, получают больше всего внимания со стороны создателей вирусов.

Правило 5: обязательно проверяйте мобильные носители информации

Несмотря на то, что около 85% всех зарегистрированных случаев заражения компьютерными вирусами приходятся на электронную почту и Интернет, не стоит забывать о таком традиционном способе транспортировки вредоносных кодов, как мобильные носители (дискеты, компакт-диски и т.п.). Перед тем, как начать их использовать на своем компьютере, необходимо тщательно проверить их антивирусной программой. Исключением могут быть разве что диски, предназначенные для форматирования.

Большую опасность представляют собой и столь широко распространенные в России пиратские компакт-диски. К примеру, проверка, проведенная «Лабораторией Касперского» в 1999 году, выявила факт присутствия вирусов на 23% закупленных носителей. Вывод прост: тщательно проверять даже приобретенные компакт-диски.

Правило 6: будьте осторожны с источниками, заслуживающими доверия

Как любви подвластны все возрасты, так же никто не застрахован от компьютерных вирусов. Это в равной мере относится к крупным компаниям-производителям программного и аппаратного обеспечения. Нередко случается, что посетителям их сайтов предлагаются зараженные программы. Показательный случай, когда в течение нескольких недель на сайте Microsoft находился документ Word, зараженный макро-вирусом Concept.

Не менее редки случаи присутствия вирусов на дискетах с драйверами к аппаратному обеспечению, с лицензионным программным обеспечением. Часто случается, что компьютер, переданный на техническое обслуживание в ремонтную мастерскую, возвращается не совсем чистым. Не то чтобы на мониторе был толстый слой пыли, а на клавиатуре паутина (хотя такое тоже случается), а просто на диске заводятся вирусы. Как правило, это происходит из-за того, что ремонтники пользуются одними и теми же дискетами для загрузки программ для тестирования различных узлов компьютера. Таким образом, они очень быстро переносят компьютерную «заразу» с одних компьютеров на другие. Вывод состоит в том, что, получив компьютер из ремонта, не забудьте тщательно проверить его на наличие вирусов.

Все это делает необходимым проверять даже те данные, которые получены из источников, заслуживающих доверия. Вряд ли в данном случае стоит обвинять самих производителей, что они якобы нарочно стараются заразить компьютер: в каждой работе бывают осечки. Просто иногда они касаются и антивирусной безопасности.

Правило 7: сочетайте разные антивирусные технологии

Не стоит ограничиваться классическим антивирусным сканером, запускаемым по требованию пользователя или при помощи встроенного планировщика событий. Существует ряд других, нередко более эффективных технологий, комбинированное использование которых способно практически гарантировать безопасную работу. К числу таких технологий относятся: во-первых, антивирусный монитор, постоянно присутствующий в памяти компьютера и проверяющий все используемые файлы в масштабе реального времени, в момент доступа к ним; во-вторых, ревизор изменений, который отслеживает все изменения на диске и немедленно сообщает, если в каком-либо из файлов поселился вирус; в-третьих, поведенческий блокиратор, обнаруживающий вирусы не по их уникальному коду, а по последовательности их действий. Сочетание описанных способов борьбы с вирусами является залогом успешной защиты от вредоносных программ.

Правило 8: всегда имейте при себе чистый загрузочный диск

Часто происходит так, что вирусы лишают компьютеры возможности производить первоначальную загрузку. Иными словами, информация на диске остается в целости и сохранности, но операционная система теряет способность загружаться. Для успешного разрешения подобных проблем необходимо иметь специальную чистую дискету с установленной антивирусной программой. С ее помощью Вы сможете произвести загрузку и восстановить систему.

Правило 9: регулярное резервное копирование

Это правило поможет сохранить данные не только в случае поражения компьютера каким-либо вирусом, но и в случае, если у компьютера произошла серьезная поломка в аппаратной части. Вряд ли кому-то хочется потерять результаты многолетних наработок вследствие произошедшего сбоя в системе вне зависимости от того, вызвано это вирусами или нет. Именно поэтому рекомендуют регулярно проводить копирование наиболее ценной информации на независимые носители: дискеты, магнитооптические диски, магнитные ленты, компакт-диски.

Правило 10: не паникуйте!

Вирусы являются такими же программами, как, допустим, калькулятор или записная книжка Windows. Их отличительная черта в том, что вирусы способны размножаться (т.е. создавать свои копии), интегрироваться в другие файлы или загрузочные секторы и производить другие несанкционированные действия. Вирусы создаются самыми обычными людьми, и ничего потустороннего в них нет. Гораздо больший вред сможете принести, если испугаетесь и совершите необдуманные действия, направленные на нейтрализацию вируса. Если работаете в корпоративной сети, немедленно позовите системного администратора. Если же просто домашний пользователь, то свяжитесь с компанией, у которой приобрели антивирусную программу. Дайте возможность профессионалам позаботиться о вашей безопасности. В конце концов, они за это получают деньги.

Существует еще один вид атаки, встречающийся в литературе под названием *«атака по социальной психологии»*. Сделаем краткий обзор нескольких довольно часто встречающихся методов.

Звонок администратору – злоумышленник выбирает из списка сотрудников того, кто не использовал пароль для входа в течение нескольких дней (отпуск, отгулы, командировка) и кого администратор не знает по голосу. Затем следует звонок с объяснением ситуации о забытом пароле, искренние извинения, просьба зачитать пароль, либо сменить его на новый. Больше чем в половине случаев просьба будет удовлетворена, а факт подмены будет замечен либо с первой неудачной попыткой зарегистрироваться истинного сотрудника, либо по произведенному злоумышленником ущербу.

Почти такая же схема, но в обратную сторону может быть разыграна злоумышленником в адрес сотрудника фирмы – звонок от администратора. В этом случае он представляется уже сотрудником службы информационной безопасности и просит назвать пароль либо из-за произошедшего сбоя в базе данных, либо якобы для подтверждения личности самого сотрудника по какой-либо причине (рассылка особо важных новостей), либо по поводу последнего подключения сотрудника к какому-либо информационному серверу внутри фирмы. Фантазия в этом случае может придумывать самые правдоподобные причины, по которым сотруднику «просто необходимо» вслух назвать пароль. Самое неприятное в этой схеме то, что если причина запроса пароля придумана, что называется "с умом", то сотрудник повторно позвонит в службу информационной безопасности только через неделю, месяц, если вообще это произойдет. Кроме того, данная схема может быть проведена и без телефонного звонка – по электронной почте, что неоднократно и исполнялось якобы от имени почтовых и Web-серверов в сети Интернет.

В качестве программных профилактических мер используются экранные заставки с паролем, появляющиеся через 5-10 минут отсутствия рабочей активности, автоматическое отключение клиента через такой же промежуток времени.

2. Методология построения систем защиты АС

2.1. Построение системы защиты от угрозы нарушения конфиденциальности информации

Функционирование комплексной системы защиты информации (АСЗИ) зависит не только от характеристик созданной системы, но и от эффективности ее использования на этапе эксплуатации АС. Основными этапами эксплуатации является максимальное использование возможностей АСЗИ, заложенных в систему при построении, и совершенствование ее защитных функций в соответствии с изменяющимися условиями.

Процесс эксплуатации АСЗИ можно разделить на применение системы по прямому назначению, непосредственно связанных с защитой информации в АС, и техническую эксплуатацию. Применение по назначению предусматривает организацию доступа к ресурсам АС и обеспечение их целостности.

Под организацией доступа к ресурсам понимается весь комплекс мер, который выполняется в процессе эксплуатации системы для предотвращения несанкционированного воздействия на технические и программные средства, а так же информацию.

Организация доступа к ресурсам предполагает:

1. разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам АС в соответствии с функциональными обязанностями должностных лиц;
2. организацию работы с конфиденциальными информационными ресурсами на объекте;
3. защиту от технических средств разведки;
4. охрану объекта;
5. эксплуатацию системы разграничения доступа.

Система разграничения доступа (СРД) является одной из основных составляющих АСЗИ. В этой системе можно выделить следующие компоненты:

1. средства аутентификации субъекта доступа;
2. средства разграничения доступа к техническим устройствам АС;
3. средства разграничения доступа к программам и данным;
4. средства блокировки неправомочных действий;
5. средства регистрации событий;
6. дежурный оператор системы разграничения доступа.

Согласно руководящим документам Гостехкомиссии под несанкционированным доступом к информации (НСД) будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств АС. НСД может носить случайный или преднамеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

- организационные;
- технологические;
- правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты - присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей

вопросы защиты информации.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация - это присвоение пользователям идентификаторов (понятие идентификатора будет определено ниже) и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация - это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

1. индивидуального объекта заданного типа;
2. знаний некоторой известной только ему и проверяющей стороне ин формации;
3. индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct password authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом третью сторону называют сервером аутентификации (authentication server) или арбитром (arbitrator).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

1. по хранимой копии пароля или его свёртке (plaintext-equivalent);
2. по некоторому проверочному значению (verifier-based);
3. без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge);
4. с использованием пароля для получения криптографического ключа (cryptographic).

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы

данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен «троянский конь»).

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя - некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя - некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя-совокупность его идентификатора и его пароля.

База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под парольной системой будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случай пароль-система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

1. интерфейс пользователя;
2. интерфейс администратора;
3. модуль сопряжения с другими подсистемами безопасности;
4. база данных учетных записей.

Ниже перечислены типы угроз безопасности парольных систем.

1. Разглашение параметров учетной записи через:

- подбор в интерактивном режиме;
- подсматривание;
- преднамеренную передачу пароля его владельцем другому лицу;
- захват базы данных парольной системы (если пароли не хранятся в базе в открытом

виде, для их восстановления может потрясаться подбор или дешифрование);

- перехват переданной по сети информации о пароле;
- хранение пароля в доступном месте.

2. Вмешательство в функционирование компонентов парольной системы через:
   - внедрение программных закладок;
   - обнаружение и использование ошибок, допущенных на стадии разработки;
   - выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

- выбрать пароль, который легко запомнить и также легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступном месте;
- ввести пароль так, что его смогут увидеть посторонние;
- передать пароль другому лицу намеренно или под влиянием заблуждения.

Далее рассмотрим криптографические методы защиты, которые в настоящее время являются базовыми для обеспечения надежной аутентификации сторон информационного обмена, защиты информации в транспортной подсистеме АС, подтверждения целостности объектов АС и т.д.

К средствам криптографической защиты информации (СКЗИ) относятся аппаратные, программно-аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации с целью:

- защиты информации при ее обработке, хранении и передаче по транспортной среде АС;
- обеспечения достоверности и целостности информации (в том числе с использованием алгоритмов цифровой подписи) при ее обработке, хранении и передаче по транспортной среде АС;
- выработки информации, используемой для идентификации и аутентификации субъектов, пользователей и устройств:
- выработки информации, используемой для защиты аутентифицирующих элементов защищенной АС при их выработке, хранении, обработке и передаче.

Отметим несколько существенных особенностей криптографического преобразования:

- в СКЗИ реализован некоторый алгоритм преобразования информации (шифрование, электронная цифровая подпись, контроль целостности и др.);
- входные и выходные аргументы криптографического преобразования присутствуют в АС в некоторой материальной форме (объекты АС);
- СКЗИ для работы использует некоторую конфиденциальную информацию (ключи);
- алгоритм криптографического преобразования реализован в виде некоторого материального объекта, взаимодействующего с окружающей средой (в том числе с субъектами и объектами защищенной АС).

В результате роль СКЗИ в защищенной АС - преобразование объектов.

Существенно важными являются следующие моменты:

1. СКЗИ обменивается информацией с внешней средой, а именно: в него вводятся ключи, открытый текст при шифровании;
2. СКЗИ в случае аппаратной реализации использует элементную базу ограниченной надежности (т.е. в деталях, составляющих СКЗИ, возможны неисправности или отказы);
3. СКЗИ в случае программной реализации выполняется на процессоре ограниченной надежности и в программной среде, содержащей посторонние программы, которые могут повлиять на различные этапы его работы;

4. СКЗИ хранится на материальном носителе (в случае программной реализации) и может быть при хранении преднамеренно или случайно искажено;

5. СКЗИ взаимодействует с внешней средой косвенным образом (питается от электросети, излучает электромагнитные поля и т.д.);

6. СКЗИ изготавливает или/и использует человек, могущий допустить ошибки (преднамеренные или случайные) при разработке и эксплуатации.

Разработчик преднамеренно или непреднамеренно может внести в программу некоторые свойства (например, возможность переключения в отладочный режим с выводом части информации на экран или внешне носители). Эксплуатирующий программу защиты человек может решить, что программа для него "неудобна" и использовать ее неправильно (вводить короткие ключи либо повторять один и тот же ключ для шифрования разных сообщений). То же замечание относится и к аппаратным средствам защиты.

В связи с этим помимо встроенного контроля над пользователем необходимо отслеживать правильность разработки и использования средств защиты с применением организационных мер.

Правильность функционирования технических средств АС, в рамках которых реализовано СКЗИ, определяется как соответствие выполнения элементарных инструкций (команд) описанному в документации. Ремонт и сервисное обслуживание СКЗИ также не должно приводить к ухудшению свойств СКЗИ в части параметров надежности.

Рассмотрим требования к средам разработки, изготовления и функционирования СКЗИ. Аппаратные средства, на которых реализуются программные или программно-аппаратные СКЗИ, и программно-аппаратная среда (программно-аппаратное окружение), в которой разрабатываются, изготавливаются и эксплуатируются СКЗИ, не должны иметь явных и скрытых функциональных возможностей, позволяющих:

- модифицировать или изменять алгоритм работы СКЗИ в процессе их разработки, изготовления и эксплуатации;
- модифицировать или изменять информационные или управляющие потоки и процессы, связанные с функционированием СКЗИ:
- осуществлять доступ (чтение и модификацию) посторонних лиц (либо управляемых ими процессов) к ключам и идентификационной, и аутентификационной информации;
- получать доступ к конфиденциальной информации СКЗИ.

Состав и назначение программно-аппаратных средств должны быть фиксированы и неизменны в течение всего времени, определенного в заключении о возможности использования.

Возможны два подхода к процессу криптографической защиты (в основном к шифрованию) объектов АС: предварительное и динамическое («прозрачное»).

Предварительное шифрование состоит в зашифровании файла некой программой (субъектом), а затем расшифровании тем же или иным субъектом (для расшифрования может быть применена та же или другая (специально для расшифрования) программа). Далее расшифрованный массив непосредственно используется прикладной программой пользователя. Данный подход имеет ряд недостатков, хотя и применяется достаточно широко.

Принципиальные недостатки метода предварительного шифрования:

- необходимость дополнительного ресурса для работы с зашифрованным объектом (дискового пространства - в случае расшифрования в файл с другим именем, или времени);
- потенциальная возможность доступа со стороны активных субъектов АС к расшифрованному файлу (во время его существования);
- необходимость задачи гарантированного уничтожения расшифрованного файла после его использования.

Сущность динамического шифрования объектов АС состоит в следующем. Происходит зашифрование всего файла (аналогично предварительному шифрованию).

Затем с использованием специальных механизмов обеспечивающих модификацию функций ПО АС, выполняющего обращения к объектам, ведется работа с зашифрованным объектом. При этом расшифрованию подвергается только та часть объекта, которая в текущий момент времени используется прикладной программой. При записи со стороны прикладной программы происходит зашифрование записываемой части объекта.

Данный подход позволяет максимально экономично использовать вычислительные ресурсы АС, поскольку расшифровывается только та часть объекта, которая непосредственно нужна прикладной программе. Кроме того, на внешних носителях информация всегда хранится в зашифрованном виде, что исключительно ценно с точки зрения невозможность доступа к ней. Динамическое шифрование целесообразно, таким образом, применять для защиты разделяемых удаленных или распределенных объектов АС.

2.2. Построение системы защиты от угрозы нарушения целостности

На этапе эксплуатации АС целостность информации в системе обеспечивается путем:

1. дублирования информации;
2. контроля целостности информации в АС;
3. особой регламентации процессов технического обслуживания;
4. выполнения комплекса антивирусных мероприятий.

Одним из важных условий обеспечения целостности информации в АС является ее дублирование. Стратегия дублирования выбирается с учетом важности информации, трудоемкости восстановления данных.

Простейшим методом контроля целостности является метод контрольных сумм. Для исключения возможности внесения изменений в контролируемый файл с последующей коррекцией контрольной суммы необходимо хранить контрольную сумму в зашифрованном виде или использовать секретный алгоритм вычисления контрольной суммы. Однако более приемлемым методом контроля целостности информации является использование хэш-функции, значение которой невозможно подделать без знания ключа, т.е. использование криптографических приемов.

Для защиты от компьютерных вирусов следует руководствоваться правилами, изложенными в первом разделе.

В силу того, что средства контроля целостности программ и файлов данных, хранимых в АС, должны обеспечивать защиту от несанкционированного изменения, то цифровая (электронная) подпись является одним из часто используемых для решения данной задачи механизмов.

В конце обычного письма или документа исполнитель или ответственное лицо обычно ставит свою подпись. Подобное действие преследует следующие цели. Во-первых, получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом. Во-вторых, личная подпись является юридическим гарантом авторства документа. Последний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т.д.

Если подделать подпись человека на бумаге весьма непросто, а установить авторство подписи современными криминалистическими методами - техническая деталь, то с цифровой подписью дело обстоит иначе. Подделать цепочку битов, просто ее скопировав, или незаметно внести нелегальные исправление в документ сможет любой пользователь.

В самой общей модели аутентификации сообщений представлено пять участников. Это отправитель А, получатель В, злоумышленник С, доверенная сторона Д и независимый арбитр Е. Задача отправителя А заключается в формировании и отправке сообщения Т получателю В. Задача получателя В заключается в получении сообщения Т и в установлении его подлинности. Задача доверенной стороны Д является документированная рассылка

необходимой служебной информации абонентам вычислительной сети, чтобы в случае возникновения спора между А и В относительно подлинности сообщения представить необходимые документы в арбитраж. Задача независимого арбитра Е заключается в разрешении спора между абонентами А и В относительно подлинности сообщения Т.

Перечислим возможные способы обмана (нарушения подлинности сообщения) при условии, что между участниками модели А, В, С отсутствует кооперация.

Способ А: отправитель А заявляет, что он не посылал сообщение Т получателю В, хотя в действительности его посылал (подмена отправленного сообщения или отказ от авторства).

Способ В1: получатель В изменяет полученное от отправителя А сообщение Т и заявляет, что данное измененное сообщение он получил от отправителя А (подмена принятого сообщения).

Способ В2: получатель в сам формирует сообщение и заявляет, что получил его от отправителя А (имитация принятого сообщения).

Способ С1: злоумышленник С искажает сообщение, которое отправитель А передает получателю В (подмена передаваемого сообщения).

Способ С2: злоумышленник С формирует и посылает получателю В сообщение Т от имени отправителя А (имитация передаваемого сообщения).

Способ С3: злоумышленник С повторяет ранее переданное сообщение, которое отправитель Д посылал получателю В (повтор ранее переданного сообщения).

Термин "цифровая подпись" используется для методов, позволяющих устанавливать подлинность автора сообщения при возникновении за относительно авторства этого сообщения. Как было уже сказано цифровая подпись применяется в информационных системах, в которых отсутствует взаимное доверие сторон (финансовые системы, системы контроля за соблюдением международных договоров и др.).

Защита от угрозы нарушения целостности информации на уровне содержания в обычной практике рассматривается как защита от дезинформации. Пусть у злоумышленника нет возможности воздействовать на отдельные компоненты АС, находящиеся в пределах контролируемой зоны, но если источники поступающей в нее информации находятся вовне системы, всегда остается возможность взять их под контроль противоборствующей стороной.

Для успешности борьбы с вероятной дезинформацией следует:

• различать факты и мнения;

• применять дублирующие каналы информации;

• исключать все лишние промежуточные звенья и т. п.

2.3. Построение системы защиты от угрозы отказа доступа к информации

Поскольку одной из основных задач АС является своевременное обеспечение пользователей системы необходимой информацией (сведениями, данными, управляющими воздействиями и т.п.), то угроза отказа доступа к информации применительно к АС может еще рассматриваться как угроза отказа в обслуживании или угроза отказа функционирования.

На этапе эксплуатации АС доступность информации в системе обеспечивается путем:

1. повышения отказоустойчивости АС;
2. противодействия перегрузкам и «зависания » системы;
3. использование строго определенного множества программ;
4. особой регламентации процессов технического обслуживания и проведения доработок.

Доступность информации поддерживается путем резервирования аппаратных средств, блокировок ошибочных действий людей, использование надежных элементов АС и отказоустойчивых систем. Устраняются так же преднамеренные угрозы перезагрузки элементов системы. Для этого используются механизмы измерения интенсивности

поступления заявок на выполнение и механизмы ограничения таких заявок. Должна быть предусмотрена возможность определения причин резкого потока заявок на выполнение программ или передачу информации.

В сложных системах практически не возможно избежать ситуаций, приводящих к «зависаниям» систем или их фрагментов. В результате сбоев аппаратных или программных средств, алгоритмических ошибок, допущенных на этапе разработки, ошибок операторов в системе происходят зацикливания программ, непредусмотренные остановки и другие ситуации, выход из которых возможен лишь путем прерывания вычислительного процесса и последующего его восстановления. На этапе эксплуатации ведется статистика и осуществляется анализ таких ситуаций. «Зависания» своевременно обнаруживаются, вычислительный процесс восстанавливается.

В защищенной АС должно использоваться только разрешенное программное обеспечение. Контроль состава программного обеспечения осуществляется при плановых проверках комиссиями и должностными лицами, дежурным оператором по определенному плану, неизвестному пользователям.

При прибытии специалистов из других организаций, например, для проведения доработок, кроме обычной проверки лиц, допускаемых на объект, должны проверяться на отсутствие закладок приборы, устройства, которые доставлены для выполнения работ.

Таким образом, надежность функционирования АС может быть сведена к надежности функционирования входящего в ее состав программного обеспечения. И существуют два основных подхода к обеспечению защиты ПО АС от угрозы отказа функционирования - предотвращение неисправностей (fault avoidance) и отказоустойчивость (fault tolerance). Отказоустойчивость предусматривает, что оставшиеся ошибки ПО обнаруживаются во время выполнения программы. Предотвращение неисправностей связано с анализом природы ошибок, возникающих на разных фазах создания ПО, и причин их возникновения.

Рассматривая защиту АС определим еще два уровня: уровень представления и уровень содержания информации.

На уровне представления информации защиту от угрозы отказа доступа к информации (защиту семантического анализа) можно рассматривать как противодействие сопоставлению используемым синтаксическим конструкциям (словам некоторого алфавита, символам и т. п.) определенного смыслового содержания. Применительно к АС задача защиты от угрозы доступности информации может рассматриваться как использование для обработки файла данных программ, обеспечивающих воспроизведение данных в том виде, как они были записаны.

На уровне содержания защита информации от угрозы доступности обеспечивается защитой актуальности информации или легализацией полученных сведений или данных. Применительно к АС защита содержания информации от угрозы блокировки доступа (отказа функционирования) означает юридическую обоснованность обработки и использования информации, хранящейся в АС.

2.4. Построение систем защиты от угрозы раскрытия параметров информационной системы

Методы защиты от угрозы раскрытия параметров информационной системы, в принципе, не отличаются от рассмотренных выше методов защиты конфиденциальности информации. Цель данного раздела - дать представление о тех параметрах АС, раскрытие которых позволит злоумышленнику в дальнейшем реализовать основные виды угроз: нарушения конфиденциальности информации, нарушения целостности информации и блокирования доступа к информации.

Для осуществления НСД злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав АС. Он осуществляет НСД, используя:

- знания о АС и умения работать с ней;
- сведения о системе защиты информации;
- сбои, отказы технических и программных средств;
- ошибки, небрежность обслуживающего персонала и пользователей.

Существует пять нестандартных методов исследований, которыми может воспользоваться злоумышленник для получения нужной ему информации:

1. диалоговые руководства и модели программ;
2. анализ найденных МНИ;
3. копание в мусоре;
4. изучение «фотографий»;
5. «вынюхивание».

Более детально рассмотрим первые два.

Диалоговые обучающие руководства и модели программ. Руководства и модели программ часто используются для обучения работе с компьютерной системой. Эти программы имитируют компьютерные экраны, какими видел бы их пользователь в процессе реальной работы в сети. Руководства и модели отличаются от реальной работы тем, что сообщают пользователю о стандартных методах общения с системой и иногда даже показывают ему необходимые в работе специальные детали. Если пользователь не прошел курс обучения, ему обычно выдается сборник упражнений для работы с облегченной версией настоящей системы, причем, как правило, выдается вместе с богатым набором всевозможных шпаргалок.

Руководства и модели дают новым пользователям практический опыт общения с программным обеспечением, с которым им придется иметь дело, знакомят с его функциями и задачами. Такие программы весьма часто используются в учебных целях вместо реальной системы, или же как дополнение к ней. На то имеется несколько причин. Что, если система еще внедряется, или проходит стадию обновления? А может быть, новичка слишком накладно обучать на «живой» системе - мало ли что. Модели решают подобные проблемы, так как их можно инсталлировать на любой компьютер.

Программы-модели можно получить в общественных, специализированных и даже научных библиотеках. Можно также заказать такую у производителя, написав ему, что собираетесь хорошо заплатить за его продукцию. Лесть, лож, давление на чувство сверхполноценства производителя, а потом, будто бы невзначай, вопрос: а нет ли, случаем, у господ хороших какой-нибудь «демонстрашки»? Не исключено, что удастся добыть такую программу у дружески настроенного сотрудника компьютерного отдела компании.

Анализ найденных МНИ. Пусть злоумышленник получил доступ к МНИ с конфиденциальной информацией. Для того чтобы получить доступ к содержанию информации, в общем случае он должен обеспечить

- считывание с МНИ хранящейся на нем информации
- получение доступа к содержимому логической единицы хранения информации (файла);
- воспроизведение содержимого файла в штатном режиме;
- экспертную оценку считанной и воспроизведенной информации.

При проведении злоумышленником мероприятий, направленных на учение информации с МНИ (как правило, это гибкий или жесткий магнитный диск), у него возникает необходимость решения следующих задач.

1. Диагностика состояния носителя, включающая получение
- необходимых для конкретной ОС элементов формата носителя;
- признаков инструментальных средств подготовки носителя к использованию;
- характеристики распределения информации по рабочей поверхности носителя;
- признаков удаленной, остаточной и скрытой информации;

- данных о сбойных секторах и недоступных для чтения областей;
- признаков нестандартного форматирования носителя.

2. Профилактика состояния носителя (выявление причин, приведших к тому или иному состоянию носителя).

3. Восстановление рабочего состояния носителя.

4. Восстановление, копирование и преобразование информации на носителе.

Как уже было отмечено, необходимым условием для считывания информации с МНИ является наличие аппаратной, программной и организационной составляющих физического доступа.

Чтобы осуществить подбор привода, настройку программного обеспечения и обращение к содержимому МНИ, необходимо провести идентификацию его типа. Для этого используются первичные признаки носителя:

- внешний вид данного носителя;
- информация о типе носителя;
- характеристика данного носителя.

Исходя из описанных возможных действий злоумышленника, необходимо создавать соответствующие защитные меры от разведки параметров системы, а именно не допускать при эксплуатации АС получения потенциальным противником указанных выше сведений.

Если имевшийся в наличии машинный носитель был правильно идентифицирован злоумышленником, для него подобран привод, то с большой вероятностью ему будет известен формат оригинального носителя, или же этот формат будет автоматически идентифицирован операционной системой, допускающей работу с приводом для данного носителя. Например, обычные 3,5" дискеты, как правило, отформатированы в стандарте IBM (MS DOS) на 1,44 Мбайта или 720 Кбайт либо в стандарте Apple Macintosh на 1,44 Мбайта или 720 Кбайт.

Однако возможно введение произвольных нестандартных способов разметки носителя, которые могут применяться не только для удобства их эксплуатации, но и с целью защиты хранящейся информации. Тогда потенциальный злоумышленник будет иметь дело с последовательностью из нулей и единиц. В этом случае потребуется классификация служебной, содержательной, остаточной и скрытой информации. По своему смыслу эта работа близка к довольно глубокому криптоанализу. Нельзя также исключать и применение более изощренных криптографических алгоритмов при зашифровании всего содержимого носителя, включая служебные области.

Процедура определения формата носителя на логическом уровне предполагает:

- определение числа и размера кластеров;
- выделение таблицы размещения файлов;
- выделение корневой директории.

Основным критерием того, осуществлен или нет логический доступ, служит способность злоумышленника выделить каждый файл на доступом ему машинном носителе. В настоящее время, из-за использования ограниченного числа типов операционных систем и еще меньшего числа способов размещения файлов на носителях, данная задача для злоумышленника может считаться решенной. В то же время для отдельных особо критичных АС (при наличии достаточного количества средств) можно рассмотреть вопрос о разработке уникальной подсистемы взаимодействия с носителем.

Если злоумышленник имеет файл, то ему известно его название с расширением, дата создания, объем, статус (только для чтения и др.). С учетом того, что существуют различные виды информации (текст, графимое изображение, звуковой и видеосигнал, программные модули и т.д.), а также различные способы ее представления, разработаны и активно используются стандарты оформления (форматы) файлов. Перечень таких форматов очень широк. Их многообразие объясняется в первую очередь большим количеством соответствующих программных продуктов. Заранее знать, в каком формате подготовлен файл, не всегда возможно. Однако для каждого вида информации, представленной в файле, для

каждого формата существуют характерные признаки. Таким образом, задача выявления смысла содержимого файла предполагает определение программного средства, с помощью которого этот файл был подготовлен, включая использованные для зашифрования средства криптографической защиты информации.

В случае применения криптографических средств защиты злоумышленник может применять криптографический анализ.

Отдельным направлением защиты АС является сокрытие логики ее работы и ее защитных функций, реализованных программно или программно - аппаратно. Это связано с тем, что большинство атак злоумышленников на системы защиты и защищаемую ими информацию включают в себя как обязательный этап изучение логики защитных и функциональных механизмов. В свою очередь, изучение логики программ АС разбивается на три стадии:

- выделение чистого кода программы;
- дизассемблирование;
- семантический анализ.

Выделение чистого кода программ может потребоваться злоумышленнику по следующим причинам.

- предприняты специальные меры для противодействия исследованию этого кода;
- предприняты меры, направленные на преобразование кода в другую форму, которые не преследуют реализацию противодействия; чаще всего это архивация или кодирование исходного

Дизассемблированием называется процесс перевода программы из исполняемых или объектных кодов на язык ассемблера. Задача дизассемблирования практически решена. В настоящее время практически для всех операционных систем существует много хороших дизассемблеров, почти стопроцентно справляющихся со стандартным кодом. Дизассемблированный текст может считаться полностью правильным, если при повторном ассемблировании получается исходный код. Аналогично, код считается не содержащим специальных приемов защиты от исследования, если дизассемблер получает полностью правильный текст. С помощью этапа дизассемблирования можно проверить качество выполнения этапа получения чистого кода: если дизассемблер не генерирует полностью правильный код, то тот этап не был закончен.

Семантический анализ программы - исследование программы изучением смысла составляющих ее функций (процедур) в аспекте операционной среды компьютера. Этот этап является заключительным и позволяет восстановить логику работы программы без исходных текстов. При этом используется вся полученная на предыдущих этапах информация, которая, как уже отмечалось, может считаться правильной только с некоторой вероятностью, причем не исключены вообще ложные факты или умозаключения.

Семантический анализ применяется к полученным ассемблерным текстам программы и состоит в нахождении и выделении управляющих конструкций, таких как циклы, подпрограммы и т.п., и основных структур данных. При этом определяются входные и выходные данные, а также реконструируется логика проводимых с ними преобразований.

Простейшим методом защиты исполняемого кода программы является его модификация. Самым примитивным способом модификации кода (по сложности реализации и надёжности) является его упаковка при помощи одной из стандартных программ-упаковщиков: PkUte, Diet и т.д. Подобная защита ненадёжна, но тем не менее позволяет скрыть истинный исполняемый код, содержащиеся в нём текстовые строки и другую информацию, особенно если после перекодировки предприняты дополнительные меры защиты, такие как затирание идентификатора упаковщика и прочей информации, характеризующей метод упаковки.

Более надёжным методом является использование нестандартных упаковщиков. Если в предыдущем случае при удачном определении метода упаковки исполняемый код можно

«развернуть», используя готовое средство, то при неизвестном упаковщике эта операция потребует предварительного анализа исполняемого кода подпрограммы, осуществляющей распаковку программы при её запуске.

Значительно более эффективным методом является шифрование тела программы и данных. Поскольку целью данного механизма защиты является обеспечение работы программы в нормальном режиме и предотвращение доступа к истинному исполняемому коду во всех остальных случаях, в качестве ключа к шифру целесообразно выбирать параметры системы и временные характеристики её работы, соответствующие именно этому режиму (картину расположения в памяти, значения системных переменных, режим работы видеоадаптера, взаимодействие с таймером).

Кроме того, модификация может не затрагивать всего кода, а касаться лишь отдельных команд (наиболее предпочтительны команды передачи управления, вызовы прерываний или их параметры), а также небольших фрагментов кода, играющих ключевую роль.

Более специализированными являются методы противодействия отладчикам. Это могут быть различные способы модификации кода при работе программы (совмещение сегмента стека с сегментом кода, шифрование кода и т.п.), активное противодействие путём периодической проверки и изменения векторов прерываний, в том числе и некорректными способами, блокировка клавиатуры и вывода на экран, контроль времени выполнения отдельных блоков программы, использование специфических особенностей микропроцессоров и т.п.

2.5. Методология построения защищенных АС

Рассмотрим методы построения защищенных АС. Эти методы условно можно разделить на две группы:

1) относящиеся к произвольному ПО АС:

- иерархический метод разработки;
- исследование корректности и верификация.

2) специфичные только для систем защиты (теория безопасных систем).

Иерархический метод разработки ПО АС. В соответствии с принципом абстракции при проектировании АС разработчики могут идти по меньшей мере двумя путями: от аппаратуры «вверх» - к виртуальной машине, представляющей АС, или от виртуальной машины «вниз»- к реальному оборудованию. Это и есть два основных метода проектирования - метод снизу вверх и метод сверху вниз. Остальные методы по своей сути сводятся к этим двум или являются их сочетанием.

Первый метод достаточно прост, требует намного меньших капитальных вложений, но и обладает меньшими возможностями. Он основан на известной схеме : «Вы – злоумышленник. Ваши действия?». То есть служба информационной безопасности, основываясь на данных о всех известных видах атак, пытается применить их на практике с целью проверки, а возможно ли такая атака со стороны реального злоумышленника.

Метод снизу вверх предполагает начало проектирования с основного аппаратного оборудования системы. При проектировании модули разбиваются на ряд слоев, причём нулевой слой виртуальной системы образует аппаратура. Слои, реализующие одно или несколько необходимых свойств, добавляются последовательно пока не будет получена желаемая виртуальная машина. К недостаткам метода проектирования снизу вверх относят:

- необходимость с самого начала принимать решение о выборе способа реализации компонентов АС-с помощью аппаратуры, микропрограмм или программ, что сделать очень трудно;
- возможность проектирования АС только после разработки аппаратуры;
- расхождение между реальной АС и определённой в ТЗ.

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

Далее следует выяснение насколько серьезный ущерб может принести фирме раскрытие или иная атака на каждый конкретный информационный объект. Этот этап носит название «вычисление рисков». В первом приближении риском называется произведение «возможного ущерба от атаки» на «вероятность такой атаки». Существует множество схем вычисления рисков, остановимся на одной из самых простых.

Ущерб от атаки может быть представлен неотрицательным числом в приблизительном соответствии со следующей таблицей 2.1.

Таблица 2.1.

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

Вероятность атаки представляется неотрицательным числом в приблизительном соответствии со следующей таблицей 2.2.

Таблица 2.2.

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

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

Следующим этапом составляется табл. 2.3. - таблица рисков предприятия. Она имеет следующий вид.

Таблица 2.3. Таблица рисков

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

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

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

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

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

Структурный принцип имеет фундаментальное значение и составляет основу большинства реализаций. Согласно этому принципу, для построения ПО требуются только три основные конструкции:

- функциональный блок;
- конструкция обобщенного цикла;
- конструкция принятия двоичного решения.

Функциональный блок можно представить как отдельный вычислительный оператор или как любую другую реальную последовательность вычислений с единственным входом и единственным выходом, как в подпрограмме. Организация цикла в литературе часто упоминается как элемент DO-WHILE. Конструкция принятия двоичного решения называется

IF-THEN-ELSE.

Эти конструкции могут сами рассматриваться как функциональные блоки, поскольку они обладают только одним входом и одним выходом. Таким образом, можно ввести преобразование операции цикла в функциональный блок и в последующем рассматривать всякий такой оператор цикла эквивалентом (несколько более сложного) функционального блока. Аналогично можно ввести преобразование конструкции принятия решения к функциональному блоку. Наконец, можно привести любую последовательность функциональных элементов к одному функциональному элементу. В то же время обратная последовательность преобразований может быть использована в процессе проектирования программы по нисходящей схеме, т.е. исходя из единственного функционального блока, который постепенно раскладывается в сложную структуру основных элементов.

Принцип модульного проектирования заключается в разделении программ на функционально самостоятельные части (модули), обеспечивающие заменяемость, кодификацию, удаление и дополнение составных частей.

Преимущества использования модульного принципа состоят в следующем:

- Упрощается отладка программ, так как ограниченный доступ к модулю и однозначность его внешнего проявления исключают влияние ошибок в других, связанных с ним, модулях на его функционирование.
- Обеспечивается возможность организации совместной работы больших коллективов разработчиков, так как каждый программист имеет дело с независимой от других частью программы.
- Повышается качество программы, так как относительно малый размер модулей и, как следствие, небольшая сложность их позволяют провести более полную проверку программы.

Исследование корректности реализации и верификация АС. Понятие корректности или правильности подразумевает соответствие проверяемого объекта некоторому эталонному объекту или совокупности формализованных эталонных характеристик и правил. Корректность ПО при разработке наиболее полно определяется степенью соответствия предъявляемым к ней формализованным требованиям программной спецификации. В спецификациях отражается совокупность эталонных характеристик, свойств и условий, которым должна соответствовать программа. 1 Основную часть спецификации составляют функциональные критерии и Ц характеристики. Исходной программной спецификацией, которой должна соответствовать программа, является ТЗ

При отсутствии полностью формализованной спецификации требований в качестве ТЗ, которому должна соответствовать АС и результаты ее функционирования, иногда используются неформализованные предоставления разработчика, пользователя или заказчика программ. Однако понятие корректности программ по отношению к запросам пользователя или заказчика сопряжено с неопределённостью самого эталона, которому должна соответствовать АС. Для сложных программ всегда существует риск обнаружить их некорректность (по мнению пользователя или заказчика) при формальной корректности относительно спецификаций вследствие неточности самих спецификаций. Традиционный взгляд на спецификацию требований заключается в том, что она представляет собой документ на естественном языке, который является интерфейсом между заказчиком и изготовителем. Хотя подготовке документа может предшествовать некоторое взаимодействие, именно этот документ в значительной степени выступает как «отправная точка» для изготовителя программ.

Таким образом, можно сделать вывод о том, что создание совокупности взаимоувязанных непротиворечивых спецификаций является необходимой базой для обеспечения корректности проектируемой программы. При этом спецификации должны:

- быть формальными;
- позволять проверять непротиворечивость и полноту требований заказчика;

- служить основой для дальнейшего формализованного проектирования ОС.

Существует несколько подходов к определению спецификаций требований.

Спецификация как описание. Заказчик выдает спецификацию, чтобы изготовители могли снабдить его тем изделием, которое он желает, поэтому заказчик видит этот документ главным образом как описание системы, которую он желал бы иметь. В принципе, в описании должно быть указано, что должна и что не должна делать система. На практике обычно по умолчанию предполагается, что система должна делать то, что уточняется в спецификации, и не должна делать ничего более. В этом состоит главная проблема с описательной стороной спецификации. Предполагается, что заказчик всегда точно знает всё, что система должна и не должна делать. Более того. в дальнейшем предполагается, что заказчик полностью перенёс это знание в специфицированный документ.

Спецификация как предписание. Изготовитель смотрит на специфицированный документ как на набор составных частей, подлежащих сборке, чтобы разрешить проблему заказчика. Такой предписывающий взгляд обуславливается не только трудностями создания описательного документа (как указывалось выше), но и сведениями, которые умышленно или неумышленно расширяют или ограничивают свободу изготовителя.

Договорная методология. В рамках «описание заказчика-предписание изготовителю» спецификация рассматривается как формальное разделение между сторонами. Что касается заказчика, то он оговаривает минимально приемлемое, тогда как изготовитель - максимально требуемое. Договор предлагается и принимается при зарождении системы и заканчивается после завершения системы, когда заказчик принимает систему как отвечающую его минимальным требованиям. Во время изготовления системы в принципе не предполагается никаких взаимодействий, даже если изготовитель подозревает, что предписываемое не совсем соответствует тому, что заказчик желает видеть в действительности.

Спецификация как модель. Современные более строгие представления о спецификации трактуют ее как модель системы. При условии, что лежащая в основе модели семантика в достаточной мере обоснована, такая спецификация обеспечивает чёткую формулировку требований.

Соответствующие модели подходят также для автоматизированного контроля целостности и другого прогнозного анализа, который, в частности, обеспечит прекращение разработки системы, в принципе не способной удовлетворить требованиям.

Модели как описание системы имеют следующие отличительные черты по сравнению с другими способами формального описания:

- хорошее сочетание нисходящего и восходящего подходов к их разработке с возможностью выбора абстрактного описания;
- возможность описания параллельной, распределенной и циклической работы;
- возможность выбора различных формализованных аппаратов для описания систем.

Основное преимущество использования формальной модели заключается в возможности исследования с ее помощью особенностей моделируемой системы. Основывая формальный метод разработки на математической модели и затем, исследуя модель, можно выявить такие грани поведения системы, которые в противном случае не были бы очевидны до более поздних стадий.

Так как целевым объектом проектирования является АС, то модель может описывать либо саму АС, либо ее поведение, т.е. внешние проявления функционирования АС. Модель, описывающая поведение АС по сравнению с моделью АС, обладает одним важным преимуществом - она может быть проверена и оценена как исполнителями, так и заказчиками, поскольку заказчики не знают, как должна работать АС, но зато они представляют, что она должна делать. В результате такого моделирования может быть проверена корректность спецификаций относительно исходной постановки задачи, т.е. ТЗ. Кроме того, критерии правильности считаются достаточными при условии, что спецификация представляет собой.

исчерпывающее описание «внешнего» поведения объекта при всех возможных (или запланированных) ситуациях его использования.

Как было отмечено выше, при разработке АС, особенно ее компонентов, представляющих систему защиты информации, для обеспечения высоких гарантий отсутствия неисправностей и последующего доказательства того, что система функционирует согласно требованиям ТЗ, используются формальные подходы к ее проектированию.

Формальное проектирование алгоритмов базируется, в основном, на языках алгоритмических логик, которые включают высказывание вида Q{S}R, читающееся следующим образом: если до исполнения оператора S было выполнено условие Q, то после него будет R'. Здесь Q называется предусловием, а R-постусловием. Эти языки были изобретены практически одновременно Р.У. Флойдом (1967 г.), С.А.Р. Хоаром (1969 г.) и учеными польской логической школы (А. Сальвицкий и др., 1970 г.). Как предусловие, так и постусловие являются предикатами.

Преимущество представления алгоритма в виде преобразователя предикатов состоит в том, что оно дает возможность:

- анализировать алгоритмы как математические объекты;
- дать формальное описание алгоритма, позволяющее интеллектуально охватить алгоритм;
- синтезировать алгоритмы по представленным спецификациям;
- провести формальное верифицирование алгоритма, т.е. доказать корректность его реализации.

Методология формальной разработки и доказательства корректности алгоритмов в настоящее время хорошо разработана и изложена в целом ряде работ. Вкратце суть этих методов сводится к следующему:

- разработка алгоритма проводится методом последовательной декомпозиции, с разбивкой общей задачи, решаемой алгоритмом, на ряд более мелких подзадач;
- критерием детализации подзадач является возможность их реализации с помощью одной конструкции ветвления или цикла;
- разбиение общей задачи на подзадачи предусматривает формулирование пред- и постусловий для каждой подзадачи с целью их корректного проектирования и дальнейшей верификации.

Для доказательства корректности алгоритма (верификация) формулируется математическая теорема Q{S}R, которая затем доказывается. Доказательство теоремы о корректности принято разбивать на две части. Одна часть служит для доказательства того, что рассматриваемый алгоритм вообще может завершить работу (проводится анализ всех циклов). В другой части доказывается корректность постусловия в предположении, что алгоритм завершает работу.

Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trusted computing base-TCB) появилось в зарубежной практике обеспечения информационной безопасности достаточно давно. Смысл характеристики «доверенная» можно пояснить следующим образом.

Дискретная природа характеристики «безопасный» (в том смысле, что либо нечто является безопасным, полностью удовлетворяя ряду предъявляемых требований, либо не является, если одно или несколько требований не выполнены) в сочетании с утверждением «ничто не бывает безопасным на сто процентов» подталкивают к тому, чтобы вести более гибкий термин, позволяющий оценивать то, в какой степени разработанная защищенная АС соответствует ожиданиям заказчиков. В этом отношении характеристика «доверенный» более адекватно отражает ситуацию, где оценка, выраженная этой характеристикой (безопасный или доверенный), основана не на мнении разработчиков, а на совокупности факторов, включая мнение независимой экспертизы, опыт предыдущего сотрудничества с разработчиками, и в конечном итоге, является прерогативой заказчика, а

не разработчика.

Доверенная вычислительная среда (ТСВ) включает все компоненты и механизмы защищенной автоматизированной системы, отвечающие за реализацию политики безопасности - комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии. Политика безопасности включает в себя требования в адрес персонала, менеджеров и технических служб. Основные направления разработки политики безопасности:

- определение какие данные и насколько серьезно необходимо защищать,
- определение кто и какой ущерб может нанести фирме в информационном аспекте,
- вычисление рисков и определение схемы уменьшения их до приемлемой величины.

Все остальные части АС, а также ее заказчик полагаются на то, что ТСВ корректно реализует заданную политику безопасности даже в том случае, если отдельные модули или подсистемы АС разработаны высококвалифицированными злоумышленниками с тем, чтобы вмешаться в функционирование ТСВ и нарушить поддерживаемую ею политику безопасности.

Минимальный набор компонентов, составляющий доверенную вычислительную среду, обеспечивает следующие функциональные возможности:

- взаимодействие с аппаратным обеспечением АС;
- защиту памяти;
- функции файлового ввода-вывода;
- управление процессами.

Дополнение и модернизация существующих компонентов АС с учетом требований безопасности могут привести к усложнению процессов сопровождения и документирования. С другой стороны, реализация всех перечисленных функциональных возможностей в рамках централизованной доверенной вычислительной среды в полном объеме может вызвать разрастание размеров ТСВ и, как следствие, усложнение доказательства корректности реализации политики безопасности. Так, операции с файлами могут быть реализованы в ТСВ в некотором ограниченном объеме, достаточном для поддержания политики безопасности, а расширенный ввод-вывод в таком случае реализуется в той части АС, которая находится за пределами ТСВ. Кроме того, необходимость внедрения связанных с безопасностью функций во многие компоненты АС, реализуемые в различных модулях АС, приводит к тому, что защитные функции распределяются по всей АС, вызывая аналогичную проблему.

Определены следующие этапы разработки защищенной АС:

- определение политики безопасности;
- проектирование модели АС;
- разработка кода АС;
- обеспечение гарантий соответствия реализации заданной политике.

3. Формальные политики безопасности

3.1 Понятие формальной политики безопасности

Рассматривая вопросы безопасности информации в компьютерных системах можно говорить о наличии некоторых «желательных» состояний данных систем. Эти желательные состояния (описанные в терминах модели собственно компьютерной системы, например, в терминах субъектно-объектной модели) описывают «защищенность» системы. Понятие «защищенности» принципиально не отличается от любых других свойств технической системы, например, «надежной работы», и является для системы внешним, априорно заданным. Особенностью понятия «защищенность» является его тесная связь с понятиями «злоумышленник» (как обозначение внешней причины для вывода системы из состояния

«защищенности») или «угроза» (понятие, обезличивающее причину вывода системы из защищенного состояния из-за действий злоумышленника).

При рассмотрении понятия «злоумышленник» практически всегда выделяется объект его воздействия - часть системы, связанная с теми или иными действиями злоумышленника («объект атаки»). Следовательно, можно выделить три компоненты, связанные с нарушением безопасности системы:

1. «злоумышленник» - внешний по отношению к системе источник нарушения свойства «безопасность»;
2. «объект атаки» - часть, принадлежащая системе, на которую злоумышленник производит воздействие;
3. «канал воздействия» - среда переноса злоумышленного воздействия.

Интегральной характеристикой, описывающей свойства защищаемой системы, является политика безопасности - качественное (или качественно-количественное) описание свойств защищенности, выраженное в терминах, описывающих систему. Описание политики безопасности может включать или учитывать свойства злоумышленника и объекта атаки.

Описание политики безопасности включает:

1. Множество возможных операций над объектами.

2.Для каждой пары «субъект-объект» (Si,0j) назначение множества разрешенных операций, являющегося подмножеством всего множества возможных операций. Операции связаны обычно с целевой функций защищаемой системы (т.е. с категорией, описывающей назначение системы и решаемые задачи), например, операциями «создание объекта», «удаление объекта», «перенос информации от произвольного объекта к предопределенному - чтение» и т. д.

Можно сформулировать две аксиомы защищенных компьютерных систем (АС):

Аксиома 1. В защищенной АС всегда присутствует активная компонента (субъект), выполняющая контроль операций субъектов над объектами. Данная компонента фактически отвечает за реализацию некоторой политики безопасности.

Аксиома 2. Для выполнения в защищенной АС операций над объектами необходима дополнительная информация (и наличие содержащего ее объекта) о разрешенных и запрещенных операциях субъектов с объектами.

В данном случае мы оперируем качественными понятиями «контроль», «разрешенная и запрещенная операция», данные понятия будут раскрыты и проиллюстрированы ниже.

Существует дополнительная аксиома.

Аксиома 3. Все вопросы безопасности информации описываются доступами субъектов к объектам.

Важно заметить, что политика безопасности описывает в общем случае нестационарное состояние защищенности. Защищаемая система может изменяться, дополняться новыми компонентами (субъектами, объектами, операциями субъектов над объектами). Очевидно, что политика безопасности должна быть поддержана во времени, следовательно. в процесс изучения свойств защищаемой системы должны быть добавлены процедуры управления безопасностью.

С другой стороны, нестационарность защищаемой АС, а также вопросы реализации политики безопасности в конкретных конструкциях защищаемой системы (например, программирование контролирующего субъекта в командах конкретного процессора компьютера) предопределяют необходимость рассмотрения задачи гарантирования заданной политики безопасности.

В результате, можно сказать, что компьютерная безопасность решает четыре класса взаимосвязанных задач:

1. Формулирование и изучение политик безопасности.
2. Реализация политик безопасности.
3.Гарантирование заданной политики безопасности.

Типовой жизненный цикл АС состоит из следующих стадий:

1. Проектирование АС и проектирование политики безопасности.

2. Моделирование ПБ и анализ корректности ПБ, включающий усыновление адекватности политики безопасности и целевой функции СС.

3. Реализация ПБ и механизмов ее гарантирования, а также процедур и механизмов управления безопасностью.

4. Эксплуатация защищенной системы.

Рассмотрим подробно подходы к решению поставленных задач.

3.2. Понятие доступа и монитора безопасности

В теории компьютерной безопасности практически всегда рассматривается модель произвольной АС в виде конечного множества элементов. Указанное множество можно разделить на два подмножества: множество объектов и множество субъектов. Данное разделение основано на свойстве элемента «быть активным» или «получать управление» (применяются также термины «использовать ресурсы» или «пользоваться вычислительной мощностью»). Оно исторически сложилось на основе модели вычислительной системы, принадлежащей фон Нейману, согласно которой последовательность исполняемых инструкций (программа, соответствующая понятию «субъект») находится в единой среде с данными (соответствующими понятию «объект»).

Модели, связанные с реализацией ПБ, не учитывают возможности субъектов по изменению АС, которые могут привести к изменению ее свойств и как предельный случай к полной неприменимости той или иной модели к описанию отношений «субъект-объект» в измененной АС.

Этот факт не является недостатком политики безопасности. Достоверность работы механизмов реализации политики безопасности считается априорно заданной, поскольку в противном случае невозможна формализация и анализ моделей. Однако вопрос гарантий политики безопасности является ключевым как в теории, так и в практике. Рассматривая активную роль субъектов в АС, необходимо упомянуть о ряде важнейших их свойств, на которых базируется излагаемая ниже модель.

Во-первых, необходимо заметить, что человек-пользователь воспринимает объекты и получает информацию о состоянии АС через субъекты, которыми он управляет и которые производят отображение информации в воспринимаемом человеком виде.

Во-вторых, угрозы компонентам АС (АС рассматривается в модели потоков или состояний исходят от субъектов как активной компоненты, порождающей потоки и изменяющей состояние объектов в АС.

В-третьих, субъекты могут влиять друг на друга через изменяемые ими объекты, связанные с другими субъектами, порождая в конечном итоге в системе субъекты (или состояния системы), которые представляют угрозу для безопасности информации или для работоспособности самой системы.

Будем считать разделение АС на субъекты и объекты априорным. Будем считать также, что существует априорный безошибочный критерий различения субъектов и объектов в АС (по свойству активности). Кроме того, считаем в условиях всех утверждений, что декомпозиция АС на субъекты и объекты фиксирована.

Подчеркнем отличие понятия субъекта компьютерной системы от человека-пользователя следующим определением.

Пользователь - лицо (физическое лицо), аутентифицируемое некоторой информацией и управляющее субъектом компьютерной системы через органы управления ЭВМ. Пользователь АС является, таким образом, внешним фактором, управляющим состоянием субъектов: В связи с этим далее будем считать пользовательское управляющее воздействие таким, что свойства субъектов, сформулированные в ниже приводимых определениях, не

зависят от него (т. е. свойства субъектов не изменяемы внешним управлением). Смысл данного условия состоит в предположении того факта, что пользователь, управляющий программой, не может через органы управления изменить ее свойства (условие неверно для систем типа компиляторов, средств разработки, отладчиков и др.).

Будем также полагать, что в любой дискретный момент времени множество субъектов АС не пусто (в противном случае соответствующие моменты времени исключаются из рассмотрения и рассматривается отрезки с ненулевой мощностью множества субъектов).

Аксиома 4. Субъекты в АС могут быть порождены только активной компонентой (субъектами) из объектов.

Специфицируем механизм порождения новых субъектов следующим определением.

Определение 1. Объект Oi называется источником для субъекта Sm, ели существует субъект Sj, в результате воздействия которого на объект Oi в компьютерной системе возникает субъект Sm.

Субъект Sj, порождающий новый субъект из объекта Oi, в свою очередь, называется активизирующим субъектом для субъекта Sm, Sm назовем порожденным объектом.

Введем обозначение: *Create (Sj, Oi)»>Sк* - из объекта Oi порожден объект Sk при активизирующем воздействии субъекта Sj. Create назовем операцией порождения субъектов (см. рис. 1).

Операция Create задает отображение декартова произведения множеств субъектов и объектов на объединение множества субъектов пустым множеством. Заметим также, что в АС действует дискретное время и фактически новый субъект Sk порождается в момент времени t+1 относительно момента t, в который произошло воздействие порождающего субъекта на объект-источник.

Очевидно, что операция порождения субъектов зависит как от свойств активизирующего субъекта, так и от содержания объекта-уточника.

Считаем, что если Create(Sj, Oi)-> NULL (конструкция NULL далее обозначает пустое множество), то порождение нового субъекта из объекта Oi при активизирующем воздействии Sj невозможно. Так, практически во всех операционных средах существует понятие исполняемого файла - объекта, могущего быть источником для порождения субъекта. Например, для MS DOS файл edit.com является объектом источником для порождения субъекта-программы текстового редактора, а порождающим субъектом является, как правило, командный интерпретатор shell (объект-источник ~ command.com). Из архитектуры фон Неймана следует также, что с любым субъектом связан (или ассоциирован) некоторый объект (объекты), отображающий его состояние, - например, для активной программы (субъекта) ассоциированным объектом будет содержание участка оперативной памяти с исполняемым кодом данной программы.

Определение 2. Объект Oi в момент времени t ассоциирован субъектом Sm, если состояние объекта Oi повлияло на состояние субъекта в следующий момент времени (т.е. субъект Sm использует ин формацию, содержащуюся в объекте Oi).

Введем обозначение "множество объектов {0m}t ассоциировано субъектом Si в момент времени t": Si({0m}t).

В данном случае определение не в полной мере является формально строгим, поскольку состояние субъекта описывается упорядоченной совокупностью ассоциированных с ним объектов, а ассоциированный объект выделяется по принципу влияния на состояние субъекта, т. е. в определении прослеживается некая рекурсия. С другой стороны, известны рекурсивные определения различных объектов (например, дерева). Зависимость от времени позволяет однозначно выделять ассоциированные объекты том случае, если в начальный момент ассоциированный объект можно определить однозначно (как правило, это вектор исполняемого кода и начальные состояния ряда переменных программы).

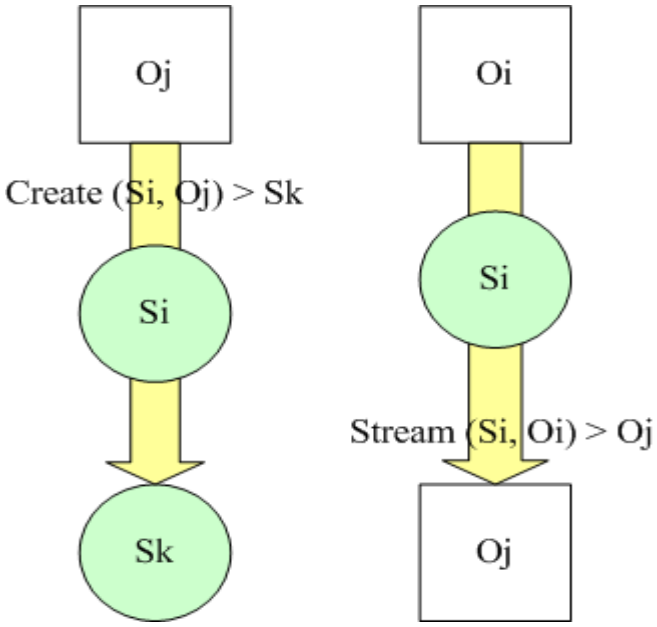


Рис. 3.1. Порождения субъекта и понятие потока

Субъект в общем случае реализует некоторое отображение множества ассоциированных объектов в t-ный момент времени на множество ассоциированных объектов в t+l-ный момент времени. В связи с этим можно выделить ассоциированные объекты, изменение которых изменяет вид отображения ассоциированных объектов (объекты, содержащие, как правило, код программы - функционально ассоциированные), и ассоциированные объекты-данные (являющиеся аргументом операции, но не изменяющие вида отображения). Далее под ассоциированными объектами понимаются функционально ассоциированные объекты, в иных случаях делаются уточнения.

Следствие (к определению 2). В момент порождения субъекта Sm из объекта Oi он является ассоциированным объектом для субъекта Sm.

Необходимо заметить, что объект-источник может быть ассоциированным для активизирующего субъекта, тогда порождение является автономным (т. е. не зависящим от свойств остальных субъектов и объектов). Если же объект-источник является неассоциированным (внешним) для активизирующего субъекта, то порождение не является автономным и зависит от свойств объекта-источника.

Свойство субъекта "быть активным" реализуется и в возможности выполнения действий над объектами. При этом необходимо отметить, что пассивный статус объекта необходимо требует существования потоков информации от объекта к объекту (в противном случае невозможно говорить об изменении объектов), причем данный поток инициируется субъектом.

Определение 3. Потоком информации между объектом Om и объектом Oj называется произвольная операция над объектом Oj, реализуемая в субъекте Si и зависящая от Om.

Заметим, что как Oj, так и Om могут быть ассоциированными или ассоциированными объектами, а также «пустыми» объектами (NULL).

Обозначения: *Stream (Si, 0m)-> Oj* - поток информации от объекта Om к объекту Oj. При этом будем выделять источник (Om) и получатель приемник) потока (Oj). В определении подчеркнуто, что поток информации рассматривается не между субъектом и объектом, а между объектами, например, объектом и ассоциированными объектами субъекта либо между двумя объектами), а активная роль субъекта выражается в реализации данного потока (это означает, что операция порождения (отека локализована в субъекте и отображается состоянием его функционально ассоциированных объектов). Отметим, что операция Stream может создавать новый объект или уничтожать его. На рис.2 схематически изображены

различные виды потоков.

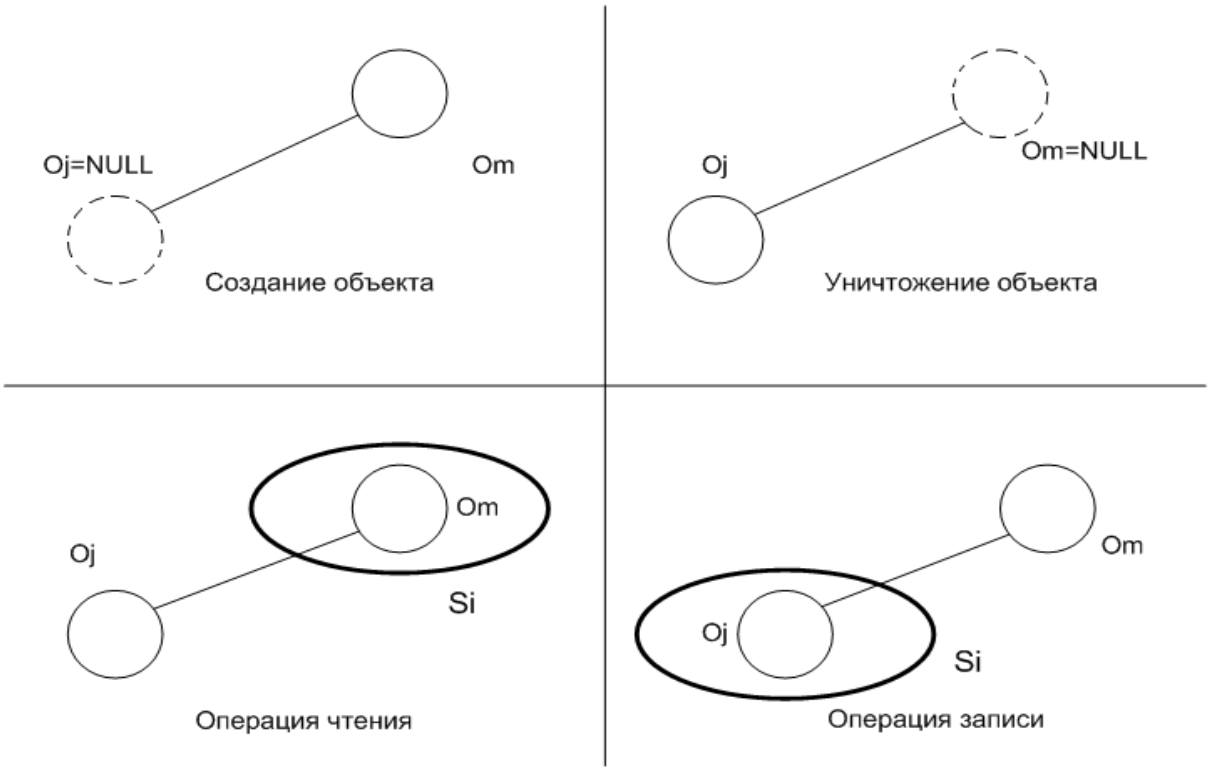


Рис. 3.2. Примеры потоков в АС

Далее будем для краткости говорить о потоке, подразумевая веденное понятие потока информации.

Понятие ассоциированных с субъектом объектов, как легко видеть из нижеизложенного, не является искусственной конструкцией. Корректно говорить о потоках информации можно лишь между одинаковыми сущностями, т.е. объектами. Кроме того, в ассоциированных объектах отображается текущее состояние субъекта. Отображения Stream и Create описываются с точки зрения разделения на субъекты и объекты все события (изменения субъектов и объектов), происходящие в АС.

Из данного определения также следует, что поток всегда инициируется(порождается) субъектом.

Определение 4. Доступом субъекта Si к объекту Oj будем называть порождение потока информации между некоторым объектом (например, ассоциированным с субъектом объектами Si(0m)) и объектом Oj .

Выделим все множество потоков P для фиксированной декомпозиции АС на субъекты и объекты во все моменты времени (все множество потоков является объединением потоков по всем моментам дискретного времени) и произвольным образом разобьем его на два непересекающихся подмножества: N и L, P = N U L.

Обозначим

N-подмножество потоков, характеризующее несанкционированный доступ;

L - подмножество потоков, характеризующих легальный доступ.

Дадим некоторые пояснения к разделению множеств L и N. Понятие «безопасности» подразумевает наличие и некоторого состояния «опасности» - нежелательных состояний какой-либо системы (в данном случае АС). Будем считать парные категории типа «опасный - безопасный» априорно заданными для АС и описываемыми политикой безопасности, а результатом применения политики безопасности к АС - разделение на множество «опасных»

потоков N и множество «безопасных» L. Деление на L и N может описывать как свойство целостности (потоки из N нарушают целостность АС) или свойство конфиденциальности (потоки из N нарушают конфиденциальность АС), так и любое другое произвольное свойство.

Определение 5. Правила разграничения доступа субъектов к объектам есть формально описанные потоки, принадлежащие подмножеству L.

В предлагаемой субъектно-ориентированной модели не производится уточнений известных моделей политик безопасности (политика безопасности описывает только критерии разбиения на множества L и N), но формулируются условия корректного существования элементов АС, обеспечивающих реализацию той или иной политики безопасности. Поскольку критерий разбиения на множества L и N не связан со следующими далее утверждениями (постулируется лишь наличие субъекта, реализующего фильтрацию потоков), то можно говорить об инвариантности субъектно-ориентированной модели относительно любой принятой в АС политики безопасности (не противоречащей условиям утверждений).

Определение 6. Объекты Oi и Oj тождественны в момент времени t, если они совпадают как слова, записанные в одном языке.

Например, при представлении в виде байтовых последовательностей объекты 01= (O11, 012, ..., O1m) и 02=(021 022, , 02k) одинаковы, если m=k и O1i = 02i для всех i от 1 до k (Oij- байты).

Для введения понятия тождественности субъектов условимся о наличии процедуры сортировки ассоциированных объектов, которая позволяет говорить о возможности попарного сравнения. На практике всегда существует алгоритм, обеспечивающий возможность попарного сравнения и зависящий от конкретной архитектуры АС. Например, достаточно легко выделить и попарно сравнивать, например, участки активной памяти, отвечающие коду программ (отличающиеся абсолютным адресом загрузки в оперативную память) или содержанию ценных и массивов.

Определение 7. Субъекты Si и Sj тождественны в момент времени попарно тождественны все ассоциированные с ними объекты.

Следствие (из определений 6 и 7). Порожденные субъекты тождественны, если тождественны порождающие субъекты и объекты-

Верность данного следствия вытекает из тождества функционально ассоциированных объектов в порождающих субъектах, которые отвечают за порождение нового субъекта, а также из тождества аргументов (ассоциированных объектов-данных), которые отвечают объектам- источникам.

Для разделения всего множества потоков в АС на подмножества L необходимо существование активной компоненты (субъекта), который:

- активизировался бы при возникновении любого потока;
- производил бы фильтрацию потоков в соответствии с принадлежностью множествам L или N.

Заметим, что если существует Stream (Si, 0j)->0m и существует Stream(Sk, 0m)->0i, то существует и Stream ((Si, Sk), 0j)->0i, т. е. Отношение «между объектами существует поток» является транзитивным (относительно пары субъектов). Именно в этом смысле будем говорить об участи субъекта (Sk) в потоке (если От является ассоциированным объектом субъекта, не тождественного Si). Введем несколько определений.

Определение 8. Монитор обращений (МО) - субъект, активизирующийся при возникновении потока от любого субъекта к любому объекту.

Можно выделить два вида МО:

Индикаторный МО - устанавливающий только факт обращения - к объекту.

МО - субъект, функционирующий таким образом, что при возникновении потока от ассоциированного объекта От Si (Si(0m)) к объекту Oj и обратно существует ассоциированный с МО объект 0m0 (в данном случае речь идет об ассоциированных объектах-данных), тождественный объекту От или Si(0m). Содержательный МО полностью

участвует в потоке от субъекта к объекту (в том смысле, что информация проходит через его ассоциированные объекты-данные и существует тождественное отображение объекта на какой-либо ассоциированный объект МО).

Теперь сформулируем понятие монитора безопасности (в литературе также применяется понятие монитора ссылок). Это понятие связано с упоминаемой выше задачей фильтрации потоков. Поскольку целью является обеспечение безопасности АС, то и целевая функция монитора — фильтрация с целью обеспечения безопасности (отметим еще раз, что разделение на N и L задано априорно).

Определение 9. Монитор безопасности объектов (МБО) -монитор обращений, который разрешает поток, принадлежащий только множеству легального доступа L. Разрешение потока в данном случае понимается как выполнение операции над объектом - получателем потока, а запрещение -как невыполнение (т.е. неизменность объекта -получателя потока).

Монитор безопасности объектов фактически является механизмом реализации политики безопасности в АС. Обратимся теперь к основным моделям работы МБО.

3.3. Основные типы формальных политик безопасности

Существуют два типа политики безопасности: дискреционная и мандатная.

Основой *дискреционной (дискретной) политики безопасности* является дискреционное управление доступом (Oiscretion.ary Access Control - OAC), которое определяется двумя свойствами:

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

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

В качестве при мера реализаций дискреционной политики безопасности в АС можно привести матрицу доступов, строки которой соответствуют субъектам системы, а столбцы - объектам; элементы матрицы характеризуют права доступа. К недостаткам относится статичность модели. Это означает, что данная политика безопасности не учитывает динамику изменений состояния АС, не накладывает ограничений на состояния системы.

Кроме этого, при использовании дискреционной политики безопасности возникает вопрос определения правил распространения прав доступа и анализа их влияния на безопасность АС. В общем случае при использовании данной политики безопасности перед МБО, который при санкционировании доступа субъекта к объекту руководствуется некоторым набором правил, стоит алгоритмически неразрешимая задача: проверить приведут ли его действия к нарушению безопасности или нет.

В то же время имеются модели АС, реализующих дискреционную политику безопасности, которые предоставляют алгоритмы проверки безопасности.

Так или иначе, матрица доступов не является тем механизмом, который бы позволил реализовать ясную и четкую систему защиты информации в АС. Этим обуславливается поиск других более совершенных политик безопасности.

Основу *мандатной (полномочной) политики безопасности* составляет мандатное управление доступом (Mandatory Access Control - MAC), которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- задан линейно упорядоченный набор меток секретности;
- каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации - его уровень секретности в АС;

- каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в АС - максимальное значение метки секретности объектов, к которым субъект имеет доступ; метка секретности субъекта называется его уровнем доступа.

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

Чаще всего мандатную политику безопасности описывают в терминах, понятиях и определениях свойств модели Белла-Лапалуда, которая будет рассмотрена ниже. в рамках данной модели доказывается важное утверждение, указывающее на принципиальное отличие систем, реализующих мандатную защиту, от систем с дискреционной защитой: *если начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушают ограничений, сформулированных политикой безопасности, то любое состояние системы безопасно.*

Кроме того, по сравнению с АС, построенными на основе дискреционной политики безопасности, для систем, реализующих мандатную политику, характерна более высокая степень надежности. Это связано с тем, что МБО такой системы должен отслеживать не только правила доступа субъектов системы к объектам, но и состояния самой АС. Таким образом, каналы утечки в системах данного типа не заложены в нее непосредственно (что мы наблюдаем в положениях предыдущей политики безопасности), а могут появиться только при практической реализации системы вследствие ошибок разработчика. В дополнении к этому правила мандатной. .политики безопасности более ясны и просты для пони мания разработчиками и пользователями АС, что также является фактором, положительно влияющим на уровень безопасности системы. С другой стороны, реализация систем с политикой безопасности данного типа довольно сложна и требует значительных ресурсов вычислительной системы.

3.4. Разработка и реализация формальных политик безопасности

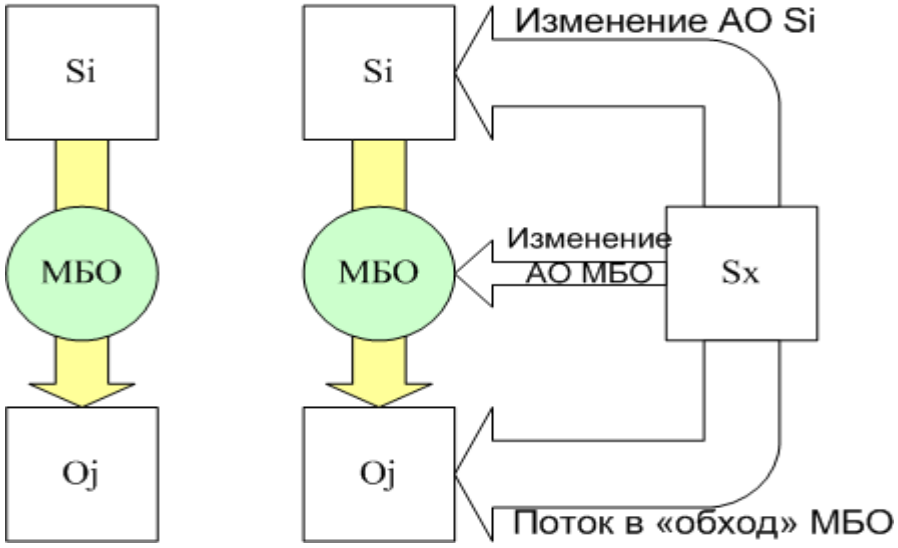


Рис. 3.3. Возможные пути нарушения политики безопасности

Представляется очевидным, что при изменении функционально ассоциированных с субъектом реализации политики безопасности (МБО) объектов могут измениться и свойства самого МБО, заключающиеся в фильтрации потоков, и как следствие могут возникнуть потоки, принадлежащие множеству N. Введем в связи с этим понятие корректности субъектов.

Определение 10. Пара субъектов Si и Sj называется не влияющими друг на друга (или корректными относительно друг друга), если в любой момент времени отсутствует поток (изменяющий состояние объекта) между ассоциированным объектом субъекта Si(Osi) и Sj(Osj), причем Osj не является ассоциированным объектом Si, а Osi не является ассоциированным объектом Sj.

Дадим некоторые пояснения к определению: «изменение состояния объекта» трактуется в данном определении как нетождественность объектов в соответствующие моменты времени, но при этом подчеркнуто, что операция изменения объекта локализована в субъекте, с которым этот объект не ассоциирован. Смысл понятия корректности можно пояснить на примере: существующие в едином пространстве ОП программы не должны иметь функциональных возможностей изменения «чужого» вектора кода и состояния переменных.

Вообще говоря, можно сформулировать более жесткое определение.

Определение 11. Пара субъектов Si и Sj называется абсолютно не влияющими друг на друга (или абсолютно корректными относительно друг друга), если в условиях определения 10 множества ассоциированных объектов указанных субъектов не имеют пересечения.

Абсолютная корректность легко достижима в случае виртуального адресного пространства.

Определение абсолютной корректности позволяет сформулировать достаточные условия гарантированного осуществления только легального доступа.

Утверждение 1 (достаточное условие гарантированного выполнения политики безопасности в АС 1).

Монитор безопасности объектов разрешает порождение потоков только из множества L, если все существующие в системе субъекты абсолютно корректны относительно него и друг друга.

Доказательство. Условие абсолютной корректности (по определению 11) предполагает неизменность функционально ассоциированных объектов МБО (поскольку потоков,

изменяющих ассоциированные объекты МБО, не существует). С другой стороны, такие потоки могут появиться при изменении ассоциированных объектов, принадлежащих другим субъектам АС (изменятся свойства субъекта, в том числе (возможно) и по порождению потоков к МБО). Условие корректности субъектов относительно друг друга делает это невозможным (по определению абсолютной корректности). Это, в свою очередь, означает, что МБО реализует только потоки из подмножества L. Утверждение доказано.

Однако сформулированное утверждение накладывает весьма жесткие и трудноисполнимые условия на свойства субъектов в АС. Кроме того, невозможно гарантировать корректность любого субъекта, активизируемого в АС, относительно МБО. В связи с этим логично ограничить множество порождаемых субъектов, которые априорно корректны относительно МБО. В связи с этим введем определение монитора порождения субъектов (по аналогии с монитором обращений) и монитора безопасности субъектов.

Определение 12. Монитор порождения субъектов (МПС) - субъект, активизирующийся при любом порождении субъектов.

По аналогии с переходом от МО к МБО введем понятие монитора безопасности субъектов.

Определение 13. Монитор безопасности субъектов (МБС) - субъект, который разрешает порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и порождающих объектов.

Воздействие МБС выделяет во всем множестве субъектов S подмножество разрешенных E. Заметим также, что если в подмножество субъектов в момент времени t включается субъект МБС, то первым аргументом операции Create может быть только субъект, входящий во множество субъектов, а аргумент-объект, вообще говоря, любым.

Сформулируем теперь ряд базовых определений, которые в дальнейшем будут повсеместно использоваться.

Определение 14. АС называется замкнутой по порождению субъектов, если в ней действует МБС, разрешающий порождение только фиксированного конечного подмножества субъектов для любых объектов-источников, рассматриваемых для фиксированной декомпозиции АС на субъекты и объекты.

При рассмотрении вопросов реализации защищенных сред будет использоваться термин «замкнутая программная среда», который по существу эквивалентен приведенному выше определению.

Однако замкнутости АС по порождению субъектов недостаточно для описания свойств системы в части защищенности, поскольку необходимо обеспечить корректность порождаемых МБС субъектов относительно его самого и МБО. Механизм замкнутой программной среды сокращает множество возможных субъектов до некоторого множества фиксированной мощности, но при этом допускает существование некорректных субъектов, включенных в замкнутую среду.

Сформулируем определение изолированности АС.

Определение 15. Множество субъектов АС называется изолированным (абсолютно изолированным), если в ней действует МБС и субъекты из порождаемого множества корректны (абсолютно корректны) относительно друг друга и МБС.

Следствие. Любое подмножество субъектов изолированной (абсолютно изолированной АС), включающее МБС, также составляет изолированную (абсолютно изолированную) среду.

Следствие. Дополнение изолированной (абсолютно изолированной) АС субъектом, корректным (абсолютно корректным) относительно любого из .числа входящие в изолированную (абсолютно изолированную) среду, оставляет ее изолированной (абсолютно изолированной).

Теперь возможно переформулировать достаточное условие гарантированного выполнения политики безопасности следующим образом.

Утверждение 2 (достаточное условие гарантированного выполнения политики безопасности в АС 2).

Если в абсолютно изолированной АС существует МБО и порождаемые субъекты абсолютно корректны относительно МБО, а также МБС абсолютно корректен относительно МБО, то в такой АС реализуется только доступ, описанный в ПРД. Доказательство. Из определения абсолютной изолированности следует возможность существования в АС только конечного множества субъектов, которые, в свою очередь, корректны относительно МБС (по определению 16 и следствию из него).

Далее, по условию утверждения (корректность МБО относительно любого из порождаемых субъектов и МБС) ассоциированные объекты могут изменяться только самим МБО, следовательно, в АС реализуются только потоки, принадлежащие множеству L. Утверждение доказано.

Легко видеть, что данное утверждение является более конструктивным относительно предыдущего достаточного условия гарантированной защищенности, поскольку ранее требовалась корректность МБО относительно произвольного субъекта, что практически невозможно. В данном же случае множество субъектов ограничено за счет применения механизма МБС и возможно убедиться в попарной корректности порождаемых субъектов.

При рассмотрении технической реализации изолированности субъектов в АС будет употребляться термин «изолированная программная среда» (ИПС), который описывает механизм реализации изолированности для конкретной программно-аппаратной реализации АС и при соответствующей декомпозиции на субъекты и объекты.

При рассмотрении операции порождения субъекта возникает весьма важная проблема, связанная с тем, что в реальных АС одинаково поименованные объекты могут иметь различное состояние в пространстве (например, быть размещенными в различных каталогах) или во времени.

Предположим, что зафиксировано состояние объекта Om в некоторый момент временит. Будем обозначать состояние объекта Om в момент времени t как 0m[t].

Определение 16. Операция порождения субъекта Create(Sk,Om)->Si называется порождением с контролем неизменности объекта, если для любого момента времени t>to, в который активизирована операция порождения объекта Create, порождение субъекта Si возможно только при тождественности объектов 0m[to] и 0m[t].

Следствие. В условиях определения 16 порожденные субъекты Si[tl]H Si[t2] тождественны, если tl>to и t2>to. При tl=t2 порождается один и тот же субъект.

При порождении субъектов с контролем неизменности объекта в АС допустимы потоки от субъектов к объектам-источникам, участвующим в порождении субъектов, с изменением их состояния.

Утверждение 3 (базовая теорема ИПС)

Если в момент времени to в изолированной АС действует только порождение субъектов с контролем неизменности объекта и существуют потоки от любого субъекта к любому объекту, не противоречащие условию корректности (абсолютной корректности) субъектов, то в любой момент времени t>to АС также остается изолированной (абсолютно изолированной).

Доказательство. По условию утверждения в АС возможно существование потоков, изменяющих состояние объектов, не ассоциированных в этот момент времени с каким-либо субъектом. Если объект с измененным состоянием не является источником для порождения субъекта, то множество субъектов изолированной среды нерасширяемо, в противном случае (измененный объект является источником для порождения субъекта) по условиям утверждения (порождение субъекта с контролем) порождение субъекта невозможно. Следовательно, мощность множества субъектов не может превышать той, которая была зафиксирована до изменения состояния любого объекта. Последствию из определения 16 (о замкнутости множества субъектов в ИПС с невозрастанием мощности множества субъектов)

получим, что множество субъектов АС изолировано. Утверждение доказано.

Можно сформулировать методологию проектирования гарантированно защищенных АС. Сущность данной методологии состоит в том, что при проектировании защитных механизмов АС необходимо опираться на совокупность приведенных выше (утверждения 1-3) достаточных условий, которые должны быть реализованы для субъектов, что гарантирует защитные свойства, определенные при реализации МБО в АС (т. е. гарантированное выполнение заданной МБО политики безопасности).

Рассмотренная концепция изолированной программной среды является расширением зарубежных подходов к реализации ядра безопасности.

Ядро безопасности - специальный компонент механизма защиты, занимающий внешнее по отношению к другим механизмам положение и предназначенный для решения задач общей организации защиты информации и контроля работы других компонентов механизмов защиты. Соответственно такому назначению к ядру предъявляются особые требования, а для создания сформулированны особые подходы. Вообще говоря, идея централизации некоторых, наиболее ответственных процедур защиты информации и особенно - процедур управления механизмами защиты не является новой: возраст этой идеи уже превышает два десятилетия. Правда, первоначально ядро безопасности представлялось как некоторый комплекс программ, выполняющий особые функции защиты и организованный особо тщательно. Поэтому концепция ядра безопасности развивалась как в плане расширения выполняемых функций, так и в плане комплектности подходов к его построению. Ядро безопасности рассматривается как центральный компонент системы защиты и непосредственно выполняющая ряд важных функций защиты, таких как контроль, регистрация, уничтожение, сигнализация и др. Существо названных функций в самом общем виде заключается в следующем. Под контролем понимается систематическая проверка состояния и работоспособности всех средств и механизмов защиты информации, имеющихся в АС. Под регистрацией в современных системах обеспечения безопасности информации понимают совокупность средств и методов, предназначенных для регулярного сбора, фиксации, обработки и выдачи сведений о функционировании механизмов защиты, включая и ведение регистрационных журналов об обращениях к защищаемым данным и программам. Под уничтожением в системах защиты понимается своевременное уничтожение всех тех данных и программ, которые больше не нужны для дальнейшего функционирования АС, но сохранение которых может послужить причиной несанкционированного получения информации или способствовать такому получению. Отсюда однозначно вытекает важность данной функции. Под сигнализацией понимается решения ряда задач: предупреждение пользователей о необходимости соблюдения мер защиты, информирование службы безопасности о выходе из строя или нарушении или попытке нарушения безопасности и т.п.

Обычно модель функционирования ядра безопасности изображается в виде следующей схемы, представленной на рис. 4.

На рис. 4 "база данных защиты" означает объект, содержащий в себе информацию о потоках множества L (защита по "белому списку" - разрешения на потоки) или N (защита по "черному списку" - запрещение на потоки).

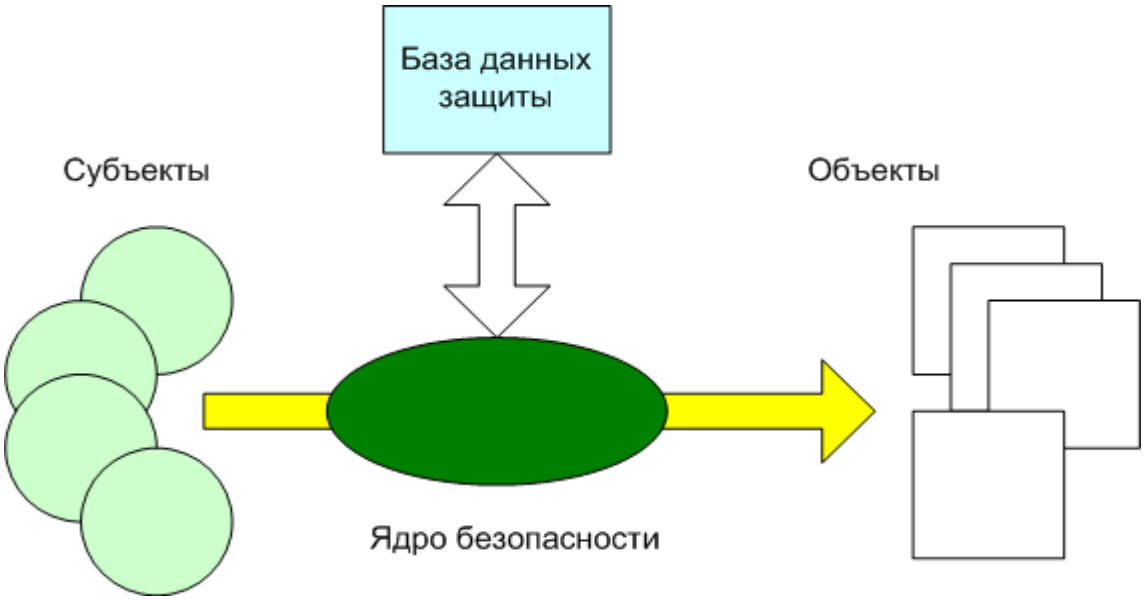


Рис. 3.4. Классическая модель ядра безопасности

Для учета влияния субъектов в АС необходимо рассматривать расширенную схему взаимодействия элементов системы реализаций и гарантирования ПБ.

В рис. 5 подчеркнута роль монитора безопасности субъектов при порождении субъектов из объектов. Взаимодействие субъектов и объектов при порождении потоков уточнено введением ассоциированных с субъектом объектов. Конструкция ОУ на схеме обозначает объект управления, т. е. объект, содержащий информацию о разрешенных значениях отображения Stream (об элементах множества L или N) и Create (элементы множества E). Объект управления может быть ассоциирован (ассоциированный объект - данные) как с МБО, такие МБС.

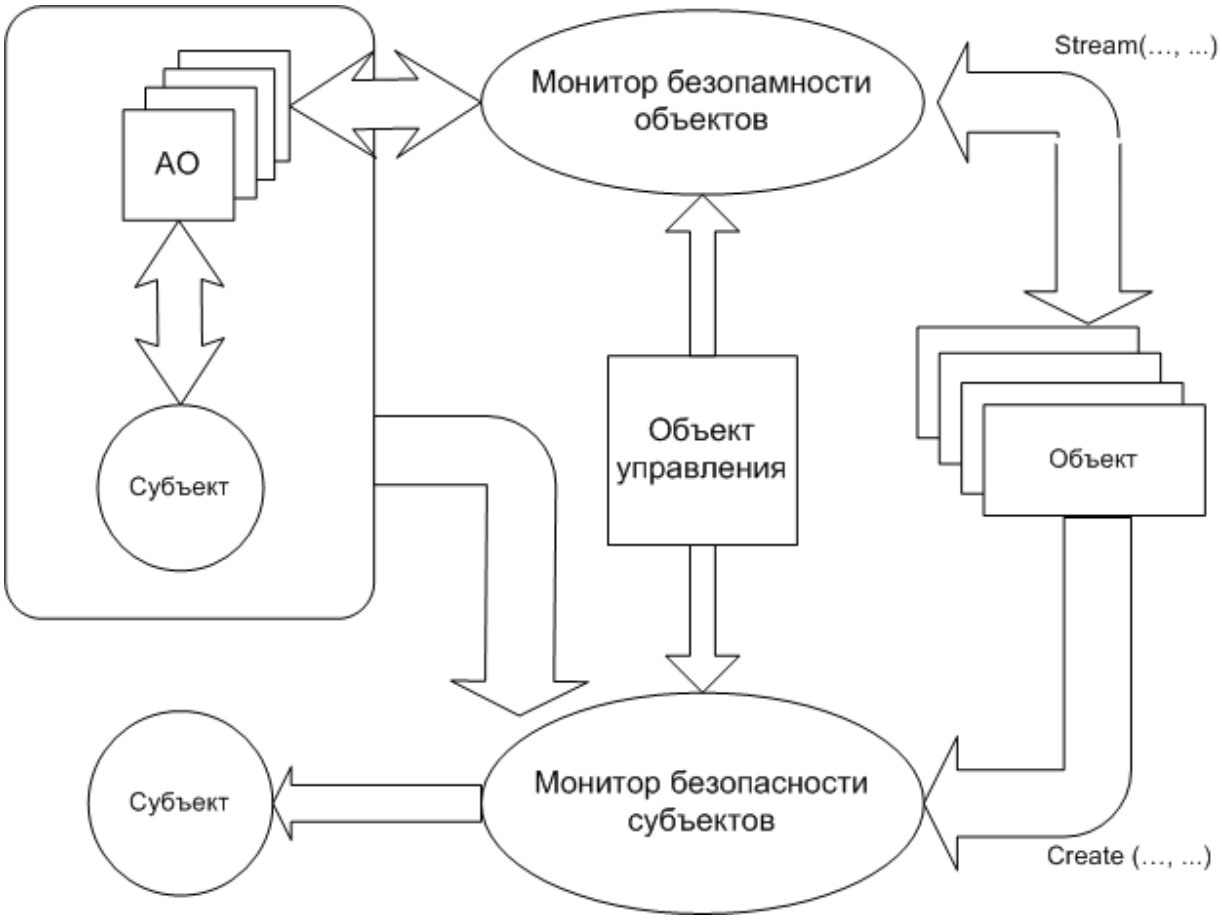


Рис. 3.5. Ядро безопасности с учетом контроля порождения субъектов

Перейдем к описанию практических методов построения ИПС. Целью рассмотрения практических подходов является иллюстрация тезиса о том, что достаточные условия гарантированной защищенности могут быть практически выполнены в реальных АС.

Опираясь на утверждение 3 (базовую теорему ИПС), сформулированное и доказанное в предыдущей части, опишем метод субъектно-объектного взаимодействия в рюмках ИПС для более конкретной архитектуры АС.

Из утверждения 3 следует, что для создания гарантированно защищенной АС (в смысле выполнения заданной политики безопасности) необходимо:

1. Убедиться в попарной корректности субъектов, замыкаемых в ИПС (либо убедиться в корректности любого субъекта относительно МБО и МБС).

2. Спроектировать и реализовать программно (или программно - аппаратно) МБС так, чтобы:

- для любого субъекта и любого объекта производился контроль порождения субъектов (т. е. чтобы реализация МБС соответствовала его определению);
- порождение любого субъекта происходило с контролем неизменности объекта-источника,

3. Реализовать МБО в рамках априорно сформулированной политики безопасности.

Надо заметить, что приводимые выше утверждения верны только тогда, когда описанная и реализованная политика безопасности не нарушает их условий (проверка данного факта зависит от модели ПБ и является отдельной весьма важной задачей).

Кроме того, необходимо обратить внимание на следующее. Объект управления, который является ассоциированным объектом МБС (обычно ассоциированный объект - данные), играет решающую роль в проектировании ИПС. При возможности изменения

состояния объекта управления потенциально возможно «размыкание» программной среды, т. е. добавление к множеству разрешенных субъектов дополнительных, реализующих злоумышленные функции. С другой стороны, процесс управления безопасностью подразумевает возможность изменения объекта управления (подробнее в части 3). Возможность изменения объекта управления (реализация потока Stream (субъект управления, АО объекты субъекта управления)->ОУ) должна присутствовать для выделенных субъектов (возможно с дополнительным условием активизации этого субъекта выделенным пользователем (пользователями)).

Важную роль при проектировании ИПС играет свойство АС, заключающееся в поэтапной активизации субъектов из объектов различного уровня представления информации. Рассмотрим в таблице 3.1. иерархию уровней при загрузке операционной системы.

В таблице выделен термин «сектор» для обозначения представления объекта аппаратно-программного уровня. Он обозначает непрерывную последовательность элементов хранения (байт) на материальном носителе, характеризуемую местом расположения.

Термин «файл» обозначает абстрактный объект, построенный по списочной структуре из объектов «сектор». Объекты типа «файл» и «сектор» выделены исключительно исходя из типовой архитектуры объектов АС.

Таблица 3.1. Иерархия уровней при загрузке ОС

Уровен	Субъект	Локализация	Представление информации	Через какие функции реализуются потоки
0	Субъект аппаратно-программного уровня	ПЗУ	сектора	через микропрограммы ПЗУ
1	Субъект уровня первичной загрузки	Загрузчик ОС	сектора	через Bios или первичный загрузчик
2	Субъект уровня вторичного загрузчика (драйвер)	драйверы ОС	сектора	через Bios или первичный загрузчик
3	Субъект уровня ОС	ядро ОС	файлы	через драйверы
4	Субъект пользовательского уровня	Прикладные приложения	файлы	через ядро ОС

В общем случае можно говорить о рекурсивной структуре объектов некоторого уровня, вмещающей объекты предыдущего уровня. На нулевом уровне первичный объект (элементарная структура нижнего уровня) в таблице 3.1. соответствует термину «сектор».

С учетом иерархической структуры представления объектов можно говорить о том, что в начальные этапы активизации АС декомпозиция на субъекты и объекты динамически изменяется. Следовательно, основная теорема ИПС может быть применима только на отдельных интервалах времени, когда уровень представления объектов постоянен и декомпозиция фиксирована. Можно утверждать, что ИПС, действующую от момента активизации до момента окончания работы АС, невозможно сформировать в начальный момент активизации АС.

Пусть в АС выделяется конечное число уровней представления объектов U={0, ..., R}, R - максимальный уровень представления объекта.

С точки зрения выполнения условий утверждения 3 имело бы смысл говорить о некотором "стационарном" состоянии АС, когда в отображениях Stream и Create участвуют только объекты уровня R. Тогда реализация МБС может быть значительно упрощена (в том смысле, что все аргументы-объекты операции Create имеют тот же уровень). Необходимо обратить внимание на то, что такое требование, с одной стороны, может накладывать ограничительные условия на свойства прикладного ПО (невозможность инициирования потоков, включающих объекты уровня менее R, прикладными программами), а с другой стороны, быть следствием проектировочных решений реализации субъекта, локализованного в ядре операционной системы (примером является ОС Windows NT 4.0, запрещающая операции ниже уровня "файл" со стороны субъектов прикладного уровня).

Практическая реализация всех операционных систем позволяет выделить две фазы их работы: активизация субъектов с ростом уровня представления объектов (фаза загрузки или начальная фаза) и фаза стационарного состояния (когда уровень представления объектов не увеличивается). Конечно, необходимо сделать оговорку касающуюся возможности реализации потоков к объектам нижнего уровня (операционные системы типа DOS, в которых возможна операция с любым объектом нижнего уровня (сектор) из программ прикладного уровня).

Тогда практическая реализация ИПС может состоять из двух этапов: предопределенное выполнение начальной фазы, включающее в себя момент активизации МБС (и МБО), и работа в стационарной фазе в режиме ИПС (возможно, с контролем неизменности объектов-источников).

Введем понятие последовательности активизации компонент АС. Смысл вводимых понятий и формулируемых ниже утверждений состоит в необходимости приведения субъектов АС в одно и то же состояние после активизации первичного субъекта аппаратно - программного уровня, или, иначе говоря, в задании предопределенной последовательности активизации субъектов АС.

Обозначим: ZL-последовательность пар (i, j)t (t=0, 1, 2, ...,1-l –моменты времени) длины 1, такие, что Create (Si,0j)[1]->Sm[t+1].

Обозначим также:

Sz - множество всех субъектов, включенных в последовательность ZL,

Oz - множество всех объектов, включенных в последовательность ZL.

Для многопотоковых АС можно рассматривать несколько (возможно, зависимых друг от друга) последовательностей ZL и соответственно множеств Sz и Oz.

Определение 17. Состоянием АС в момент времени t называется упорядоченная совокупность состояний субъектов.

Утверждение 4 (условие одинакового состояния АС).

Состояние АС в моменты времени txl и tx2 (txl и tx2 исчисляются для двух отрезков активности АС от нулевого момента активизации АС tol и to2- например, включения питания аппаратной части) одинаково, если:

1.txl=tx2,

2. тождественны субъекты Si[tol] и Si[to2],

3. неизменны все объекты из множества Oz,

4. неизменна последовательность ZL.

Доказательство (по принципу математической индукции)

Верность утверждения при t=1 следует из определения тождественности субъектов.

Пусть утверждение верно для t==k<l.

Тогда в момент времени k+1 могут быть порождены только тождественные субъекты, поскольку тождественны активизирующие субъекты (по предположению индукции) и по условию утверждения неизменны элементы множества Oz. Длина 1 последовательности ZL

определяется:

1. По признаку невозможности управления субъектами, принадлежащими множеству Sz, со стороны пользователя (в противном случае последовательность активизации субъектов может быть изменена).

2. По признаку доступности для контроля неизменности всех объектов из множества Oz.

3. По признаку невозрастания уровня представления информации (в данном случае имеется в виду, что существует момент времени tx такой, что для любого t>tx объект-аргумент Oj операции Stream(Si, Oj) принадлежит одному уровню представления).

Необходимо заметить, что последовательность ZL локализуется в некотором объекте либо совокупности объектов (например, для DOS последовательность активизации субъектов предопределена содержанием файлов AUTOEXEC.BAT и CONFIG.SYS) и неизменность последовательности ZL тождественна неизменности указанных объектов, для ОС Windows NT последовательность активизации компонент определена содержанием соответствующих ключей реестра (registry).

Пусть в последовательности ZL можно выделить zi такое, что для любого Zk, k>i отображений Create и Stream используют только объекты уровня R. Другими словами, с момента времени i наступает стационарная фаза функционирования АС.

В этих условиях, а также при попарной корректности субъектов и действии МБС с контролем неизменности объектов-источников на уровне R с момента времени m>k верно:

Утверждение 5 (достаточное условие ИПС при ступенчатой загрузке)

При условии неизменности ZL и неизменности объектов из Oz в АС с момента времени установления неизменности ZL и Oz действует изолированная программная среда.

Доказательство. Необходимо заметить, что все условия утверждения 5 соответствуют утверждению 4. Уточнения касаются структуры последовательности ZL.

Согласно утверждению 4 с момента временило до момента t==l действует изолированная (в рамках) Sz программная среда.

Для доказательства утверждения необходимо убедиться в том, что:

- МБС в момент времени t=m гарантировано активизируется,
- в любой момент t>m программная среда изолирована.

Первое следует из утверждения 4 (при 1=т состояние программной среды всегда будет одинаково, следовательно, всегда будет активизирован субъект МБС). Второе следует из определения МБС и условия теоремы.

С момента времени t==0 до момента времени 1 программная среда изолирована, с момента времени t>m программная среда также изолирована, следовательно, АС изолирована при любом t>0. Утверждение доказано.

Используя утверждения 3,4 и 5, рассмотрим процесс практического проектирования защищенного фрагмента АС.

Первоначально необходимо убедиться в выполнении условий корректности или абсолютной корректности для субъектов, участвующих в порождении ИПС. Указанные субъекты в основном могут быть локализованы на уровне программно-аппаратной компоненты ЭВМ (программы ПЗУ, загрузчики операционных сред), т. е. работать на уровне, близком к взаимодействию с оборудованием АС, либо на уровне операционной среды. Доказательство корректности субъектов программно-аппаратного уровня значительно отличается от соответствующих доказательств для субъектов прикладного уровня. В связи с этим выделим проверку условий корректности субъектов в два шага. Шагом 1 назовем доказательство корректности субъектов программно-аппаратного уровня. Понятие модуль обозначает реализацию объекта- источника, а совокупность субъекта, порожденного из объекта-источника и всего множества ассоциированных с этим субъектом объектов в течение всего времени существования субъекта, называется, как правило, процессом (или задачей, заданием).

Далее необходимо определить состав программных средств базовой вычислительной среды, т. е. определить конкретную операционную среду, дополнительные программные средства сервиса (например, программные оболочки или средства телекоммуникации) и программные средства поддержки дополнительного оборудования (программы управления принтером и др.). После этого наступает самый трудоемкий этап (Шаг 2), на котором необходимо убедиться в корректности субъектов описанного базового набора программных средств. При этом важно заметить следующее.

В составе ПО АС не должно быть целого класса возможностей -назовем их инструментальными. Прежде всего это возможность изменения состояния ассоциированных объектов со стороны субъекта (например, изменение содержимого оперативной памяти) других субъектов (изменение содержания подразумевает существование операций Stream типа запись), возможность инициирования и прекращения выполнения процессов нестандартным образом (помимо механизмов операционной среды). Кроме того, при реализации МБС и МБО на стационарной фазе функционирования АС необходимо отсутствие в любых субъектах, замкнутых в ИПС, операций порождения потоков Stream к объектам уровня k<R.

Обобщенно достаточные условия к базовому набору ПО можно сформулировать следующим утверждением.

Утверждение б (требования к субъектному наполнению изолированной программной среды)

Для того чтобы ИПС поддерживалась в течение всего времени активности АС, достаточно, чтобы в составе программного обеспечения, могущего быть инициированным в ИПС, не было функций порождения субъектов и прекращения их работы, кроме заранее предопределенных при реализации МБС, и не существовало возможностей влияния на среду выполнения (под средой выполнения понимается множество ассоциированных объектов) любого процесса, а также инициирования потоков к объектам логического уровня менее R.

Поясним требование невозможности прекращения выполнения субъекта каким-либо иным образом, кроме предопределенного. В данном случае необходимо учитывать, что во множестве субъектов, замкнутых в ИПС, выделены два особых субъекта - МБС и МБО. Прекращение существования МБС означает нарушение условия замкнутости среды, а прекращение существования МБО означает допустимость потоков множества N, т. е. несанкционированный доступ.

Шаг 3 заключается в проектировании и разработке программных или программно-аппаратных средств защиты в АС, а затем и их тестировании. Он подразумевает проектирование и реализацию в заданном множестве субъектов МБС и МБО.

Шаг 4 заключается в "замыкании" всего комплекса программного обеспечения, включая и средства защиты, в изолированную программную среду.

Итак, показано, что основными элементами поддержания изолированности программной среды являются контроль целостности и контроль порождения процессов.

Выше мы уже сформулировали понятия МБС и порождения субъектов с контролем их неизменности. Необходимо заметить, что для достоверного контроля неизменности объекта (т. е. с вероятностью ошибки, равной 0) необходимо убедиться в полном тождестве проверяемого объекта и образца. Из этого следует, что эталон должен содержать не меньше информации, чем проверяемый объект. Из этого в свою очередь следует, что эталонный объект должен быть как минимум одинаковой длины с проверяемым. На практике такой подход может быть применен с серьезными ограничениями (например, для объектов небольшого объема типа программ ПЗУ или загрузчиков ОС).

В связи с этим для контроля целостности применяют объекты, содержащие информацию, зависящую от всего содержания объекта, но тем не менее значительно меньшего объема, вычисленную при помощи класса функций типа «хэш-функций». Очевидно, что в этом случае процесс установления неизменности объекта становится

вероятностным.

Исходя из данного факта невозможно говорить о гарантированных (детерминировано) свойствах системы (поскольку неизменность объекта гарантируется лишь с некоторой вероятностью, не равной 1). Следовательно, все условия утверждений выполняются с некоторой вероятностью, зависящей от свойств применяемых для контроля целостности хэш-функций. Для подчеркивания изменившихся условий будем говорить далее не о контроле неизменности объекта, а о контроле целостности (КЦ) объекта.

Необходимо отметить также, что в процедуре контроля неизменности (которая теперь принимает вероятностный характер) участвуют как минимум два объекта: объект контроля и эталонный объект (хэш-значение), а также субъект, реализующий хэш-функцию и производящий сравнение.

Поэтому для субъекта контроля целостности важным является выполнение следующих условий:

- качественный алгоритм контроля целостности (термин «качественный» будет пояснен ниже);
- контроль реальных данных (т. е. отображение состояния контролируемого и эталонного объемов в ассоциированные объекты-данные субъекта контроля целостности, совпадающее с тождественным).

Поясним подробнее второй пункт. Контроль целостности всегда сопряжен с чтением данных (т. е. с инициированием потоков от объектов к ассоциированным объектам-данным субъекта контроля целостности, причем потоки могут соответствовать различному уровню представления информации - чтение по секторам, по файлам и т. д.). Например, встроенный в BIOS ПЭВМ субъект (практически это программная закладка - см. ниже) может навязывать при чтении вместо одного сектора другой или редактировать непосредственно буфер, в который были прочитаны данные. Аналогичный эффект может быть вызван субъектами операционной среды, например, субъектами, локализованными в первичных загрузчиках ОС. С другой стороны, даже контроль самого BIOS может происходить "под наблюдением" какой-либо дополнительной аппаратуры и не показать его изменения. Аналогичные эффекты могут возникать и при обработке файла. Цель организации режима чтения реальных данных состоит в тождественном отображении параметров чтения на АО субъекта чтения (поток от АО субъекта КЦ к АО субъекта чтения) и тождественном отображении считываемого объекта (в соответствии с параметрами, переданными субъекту чтения) к ассоциированным объектам-данным субъекта КЦ.

Поясним теперь понятие качественного КЦ с точки зрения математических свойств функции КЦ. Предположим, что имеется некоторый объект F и некоторый алгоритм H, преобразующий объект F в некоторый объект M, который представляется словом того же языка, но меньшей длины. Этот алгоритм таков, что при случайном равновероятном выборе двух объектов F1 и F2 из множества возможных соответствующие им объекты MI=H(F1) и M2==H(F2) с высокой вероятностью различны. Тогда проверка целостности данных строится так: рассматриваем объект F, по известному алгоритму H строим K=H(F) и сравниваем M, заранее вычисленное как M = H(F), с K. При совпадении считаем объект неизменным. Алгоритм H называют, как правило, хэш-функцией, или реже контрольной суммой, а число M - хэш-значением.

Качество КЦ определяется в данном случае выполнением следующих условий:

1. По известному объекту M=H(F) нахождение другого объекта G, не тождественного F, такого, что M==H(G), является задачей с трудоемкостью не менее заданной Th.
2. Объект M должен быть недоступен для изменения.
3. Длина объекта M должна обеспечивать условную вероятность P(H(Fi)=H(F2)/Fi не тождествен F2) не более заданной Pь.

Поясним смысл этих условий. Пусть программа злоумышленника изменила объект F (статическое искажение). Тогда, вообще говоря, хэш-значение M для данного объекта

изменится. Если субъекту злоумышленника доступен для изменения объект М (существует соответствующий поток), то он может по известному алгоритму Н вычислить новое хэш-значение для измененного объекта и заместить им исходное.

Пусть хэш-значение недоступно, тогда можно попытаться так построить измененный объект, чтобы хэш-значение его не изменилось; принципиальная возможность этого имеется, поскольку отображение, задаваемое алгоритмом хэширования Н, не биективно (неоднозначно).

Таким образом, при условии недоступности хэш-значения для изменения и доступности для изменения объекта-источника трудоемкость нарушения ИПС с КЦ объектов-источников (т. е. возможность породить субъект из объекта-источника, не тождественного исходному объекту) совпадает с Тн. При однократной попытке инициировать субъект из случайно равновероятно выбранного объекта-источника вероятность нарушения ИПС (успешное порождение субъекта) не превосходит Ph. Итак, «качество» ИПС определяется свойствами хэш-функции Н, а именно: величинами Тн и Рн.

Обобщим приводимые выше рассуждения в методе "безопасной загрузки", или ступенчатого контроля. Он заключается в постепенном установлении неизменности компонент программно-аппаратной среды:

1. Сначала проверяется неизменность программ ПЗУ, при положительном исходе через проверенные на целостность программы ПЗУ считывается загрузочный сектор и драйверы операционной системы (по секторам) и их неизменность также проверяется, кроме того, проверяется целостность объекта, определяющего последовательность активизации компонент;
2. Через функции чтения, проверенной ОС, инициируется процесс контроля порождения процессов (реализация МБС);
3. Инициирование процесса контроля доступа к объектам завершает проектирование гарантировано защищенной АС.

Рассматривая вопросы программно-технической реализации ИПС, необходимо заметить, что мощность множества субъектов в некотором сегменте АС (выделенном по признаку принадлежности одной ЭВМ) с момента включения питания до момента запуска процессов пользователя увеличивается. Первоначально активизируются субъекты аппаратно-программного уровня (программы ПЗУ), затем указанные субъекты порождают из объектов-источников данного уровня (это, как правило, сектора внешних носителей информации) субъектов уровня операционной среды.

Субъекты уровня операционной среды, как уже отмечалось, также делятся на два подуровня: нижний уровень — субъекты — первичные загрузчики ОС (работающие с информацией уровня секторов) и верхний уровень - субъекты-драйверы (порождаемые субъектами - первичными загрузчиками из объектов-секторов), работающие с объектами уровня «файл» (последовательности секторов). На этапе перехода от субъектов-загрузчиков к субъектам-драйверам происходит переход и к другой декомпозиции АС на объекты (от секторов к файлам). Указанная иерархия действует в любой известной на сегодняшний день АС и естественным образом предопределяет архитектуру, в рамках которой формируется и функционирует ИПС.

Например, аппаратная архитектура ПЭВМ типа IBM PC задает следующие этапы активизации различных субъектов АС. При включении питания ПЭВМ происходит тестирование ОП, инициализация таблицы векторов прерываний и поиск расширений BIOS. При их наличии управление передается на них. После отработки расширений BIOS в память считывается первый сектор дискеты или винчестера и управление передается на него (образуется код загрузчика), затем код загрузчика считывает драйверы операционной системы, далее интерпретируются файлы конфигурации, подгружается командный интерпретатор и выполняется файл автозапуска.

При реализации ИПС на нее должна быть возложена функция контроля запусков

программ и контроля целостности.

При описании методологии проектирования ИПС упоминалась проблема контроля реальных данных. Эта проблема состоит в том, что контролируемая на целостность информация может представляться по-разному на разных уровнях.

Внедренный в систему субъект может влиять на процесс чтения-записи данных на уровне файлов (или на уровне секторов) и предъявлять системе контроля некоторые другие вместо реально существующих данных. Этот механизм неоднократно реализовался в STELS-вирусах. Однако верно утверждение.

Утверждение 7 (достаточное условие чтения реальных данных)

Если субъект, обслуживающий процесс чтения данных (т. е. указанный субъект инициируется запрашивающим данные субъектом и участвует в потоке), содержал только функции тождественного отображения данных на ассоциированные объекты-данные любого субъекта, инициирующего поток чтения, и целостность объекта-источника для этого субъекта зафиксирована, то при его последующей неизменности чтение с использованием порожденного субъекта будет чтением реальных данных.

Доказательство. Верность утверждения следует из определения тождественности субъекта и из условия утверждения, гарантирующего неизменность объекта-источника.

Необходимо и здесь сделать оговорку о вероятностном характере установления неизменности и говорить, что чтение реальных данных возможно с вероятностью, определяемой алгоритмом КЦ.

Метод ступенчатого контроля не противоречит утверждениям 4 и 5 и предусматривает разделение последовательности активизации компонент ZL на подпоследовательности с одинаковым уровнем представления информации.

Реализация метода ступенчатого контроля целостности должна удовлетворять условиям утверждения 4.

Опишем практическую реализацию сформулированных методов.

Выше было сказано о том, что субъект контроля неизменности объектов, входящих в процедуры активизации АС и объектов, описывающих последовательность активизации компонент, должен быть активен уже на этапе работы субъектов аппаратно-программного уровня, но его объект-источник технически не может быть проверенна неизменность. В связи с этим подчеркнем весьма важный факт для любых реализаций ИПС.

Аксиома 5. Генерация ИПС рассматривается в условиях неизменности конфигурации тех субъектов АС, которые активизируются до старта процедур контроля целостности объектов Oz и последовательности ZL. Неизменность данных субъектов обеспечивается внешними по отношению к самой АС методами и средствами. При анализе или синтезе защитных механизмов свойства указанных субъектов являются априорно заданными.

При решении практических вопросов генерации ИПС можно выделить три самостоятельных направления.

Первое из них связано с использованием внешних по отношению к АС субъектов (как правило, размещенных на внешнем носителе), целостность которых гарантируется методами хранения или периодического контроля. Предопределенность активизации субъектов, локализованных на внешних носителях, обеспечивается свойствами субъектов аппаратно-программного уровня (например, возможно установить такую аппаратную конфигурацию ПЭВМ, при которой будет происходить загрузка операционной системы с ГМД).

Второе направление связано с локализацией ИПС в рамках территориально ограниченного рабочего места (как правило, ПЭВМ) и использует аппаратную поддержку для задания предопределенной последовательности активизации субъектов. Данное направление, как правило, включает и аппаратную поддержку аутентификации пользователей.

Третье направление связано с реализацией метода доверенной загрузки операционной среды с использованием уже имеющихся в ней механизмов реализации и гарантирования ПБ.

Необходимо заметить, что в различные интервалы активности АС субъектами могут

управлять различные пользователи, для которых множество разрешенных субъектов E различно, в связи с этим будем говорить о множестве Ei для i-го пользователя АС.

Будем также подразумевать, что перед установлением однозначного соответствия множества Ei пользователю i происходит процедура его аутентификации.

Ниже будут кратко рассмотрены все способы реализации ИПС. Говоря о первом из них необходимо отметить, что в его рамках можно рассматривать конфигурацию ИПС в двух вариантах:

- при локализации всех объектов-источников для порождения ИПС в рамках одного или нескольких внешних носителей;
- при локализации части объектов-источников на внешнем носителе, а части - во внешней памяти рабочего места.

Вторая конфигурация характеризуется потенциальной возможностью нарушения изолированности, состоящей в том, что активизация субъектов из объектов-источников, не принадлежащих внешнему носителю, может производиться вне рамок ИПС. В качестве примера можно рассмотреть ситуацию, когда программы запускаются в рамках операционной среды, загруженной с дискеты. С другой стороны, запуск указанных программ возможен и при загрузке ОС с другого носителя (в частности, с носителей рабочего места), и при этом возможна активизация и тех модулей, которые находятся на дискете.

Следовательно, основной задачей при использовании внешнего носителя для генерации ИПС является обеспечение невозможности активизации любого субъекта из объекта-источника внешнего носителя вне рамок зафиксированной для этого носителя последовательности активизации компонент ИПС.

Наиболее ранний описанный способ проектирования ИПС в рамках подхода с использованием внешнего носителя получил название «невидимой дискеты». Этот способ заключается в том, что все объекты, принадлежащие множеству Oz, и объекты, описывающие последовательность ZL, помещаются на внешний носитель, с которого может быть произведена загрузка операционной системы (обычно дискета). Неизменность объектов обеспечивается физической защитой носителя от записи.

Кроме того, использование специальной технологии не позволяет использовать объекты (в том числе и обеспечить выполнение программ) без загрузки ОС именно с этой дискеты. Практически такая дискета выглядит достаточно нетривиально: будучи помещенной в дисковод ПЭВМ она выглядит как неформатированная (или, вином варианте, пустая). После загрузки с такой "пустой" дискеты пользователь сразу «погружается» в заданную программу и работает с ней, обращаясь в том числе и к данным на винчестере и запуская программы с локальных несменяемых носителей рабочего места с предварительным контролем неизменности соответствующих им объектов-источников (исполняемых файлов).

Предлагаемый способ позволяет исключить использование изготовленной дискеты без загрузки с нее. Дополнив загружаемую с такой дискеты операционную среду программами проверки целостности, можно добиться соблюдения всех требований изолированности программно-аппаратной среды.

Как следует из утверждения 5, одним из важнейших условий поддержания ИПС является невозможность изменения последовательности активизации компонент.

В данном случае целостность объектов, содержащих последовательность активизации компонент, гарантируется физическим запретом записи на дискету,

Важной проблемой является невозможность прерывания процесса активизации компонент, В ряде операционных сред для этого имеются штатные возможности, предусмотренные для обеспечения защиты от ошибок пользователя, сформировавшего некорректную последовательность активизации компонент ОС. В связи с этим должны быть приняты меры, гарантирующие пассивность органов управления в период отработки последовательности ZL (например, аппаратная блокировка клавиатуры с момента активизации модифицированного BOOT до момента окончания активизации субъектов

множества Sz).

Описанный метод позже был реализован во внешних носителях типа CD-ROM, которые позволили значительно (на два порядка) увеличить информационную емкость носителя и загружать с него развитые операционные среды типа OS/2. Однако однократность записи существенно снижает гибкость построения ИПС таким методом.

Неудобство использования загрузочной дискеты и ее быстрый износ обусловили возникновение следующего способа проектирования ИПС.

Откажемся от рассмотрения загрузочной дискеты и рассмотрим ПЭВМ с загрузкой ОС с устройства локального хранения (винчестера) и дополнительным аппаратным устройством изолирования среды.

Рассмотрим два этапа - этап установки ИПС и этап эксплуатации ИПС. Предположим существование N пользователей, каждый i-ный из которых характеризуется некоторой персональной информацией Ki, не известной другим пользователям и хранящейся на некотором материальном носителе (например, устройстве сенсорной памяти типа Touch Memory). Существует также администратор системы с ИПС, который знает все Ki и единолично проводит этап установки. Пользователи (владельцы Ki) же участвуют только в этапе эксплуатации.

Процесс установки ИПС состоит из следующих действий:

1. В ПЭВМ устанавливается аппаратный модуль, включающий в себя устройство и программы ПЗУ данного устройства (субъекты аппаратно-программного уровня), реализующие:

- операции сервиса аутентифицирующего носителя пользователя Ci (как минимум его чтение);
- аутентификацию пользователя с номером inc введенному им Ki; 1- чтение массива данных, содержащего множество доступных для пользователя i объектов-источников (исполняемых модулей) Fil, Fi2, …,Fim, составляющих Oz, а также объект, содержащий ZL;
- вычисление информации Mil, Mi2, ... Mim, фиксирующей целостность объектов-источников Fil, ..., Fim каждого объекта-источника (информация Mij должна удовлетворять требованиям хэш-значений и, возможно, зависеть от Ki), Mij=H(Ki, Fj)
- блокирование устройств управления и предотвращение загрузки операционной среды с внешнего носителя.

2. Администратор определяет для пользователя i набор потенциально возможных для активизации субъектов Ei, Ei={Pil, ..., Pimi}, i==l, ...,N. Create (Pik, Fj)->Pij, mi - число разрешенных к запуску задач для i-го пользователя.

3. Администратор формирует (и заносит на носитель) или считывает с носителя для i-го пользователя его Ki и вычисляет значения для последующего контроля целостности Mijr== H(Ki, Fjr) где H- функция КЦ (хэш-функция).

4. Администратор проделывает действия 2 и 3 для всех N пользователей.

5. Администратор устанавливает в АС МБС с объектом-источником Fипс и фиксирует его целостность. Установка модуля происходит с учетом условий утверждения 5.

6. Администратор фиксирует целостность объекта, содержащего ZL.

Процесс эксплуатации состоит из следующих действий.

1. Включение питания и активизация аппаратного модуля:

а) Идентификация пользователя i по Ki.

При успехе выполняется п. б), при неудаче ПЭВМ блокируется.

б) Проверка целостности всех установленных в ПЭВМ ПЗУ. При положительном исходе выполняется п. в), при неудаче ПЭВМ блокируется.

в) Чтение по секторам файлов операционной среды и проверка их целостности.

г) Чтение как файла Fипс (с помощью функций операционной среды) и проверка его целостности. Вариантом может быть чтение Fипс по секторам.

д) Активизация процесса контроля Рипс. Create(Sx,Fипс)->Fипс. Активизация МБО.

е) Запуск избранной задачи i-го пользователя (может не выполняться).

2.РаботавИПС.

Запуск каждого процесса Ps сопровождается проверками:

а) Принадлежит ли Ps к множеству разрешенных для i (Ei) если да, то выполняется п. б), иначе запуск игнорируется.

б) Совпадает ли G==H(Ki, Fs,) с M=H(Ki, Fs), вычисленной администратором.

в) При положительном исходе б) задача запускается, иначе запуск игнорируется.

Легко видеть, что условия изолированности среды выполнены. Кроме того, в данном случае реализован механизм ступенчатого контроля, обеспечивающий чтение реальных данных.

При дополнении в ИПС реализации МБО и выполнении условий, предъявленных выше, к субъектам, входящим в ИПС, сформированная программная среда будет гарантированно защищенной в рамках политики безопасности, реализованной в МБО.

Используя утверждение 4, об одинаковости состояний АС после активизации проверенных на неизменность субъектов в неизменной последовательности, можно описать метод доверенной загрузки компонент операционной среды (кратко «метод доверенной загрузки»).

Пусть предопределен порядок загрузки компонентов ОС (под загрузкой компонентов ОС понимается активизация различных субъектов ОС из соответствующих объектов-источников различного уровня иерархии). Процедуру загрузки ОС назовем доверенной, если:

- установлена неизменность компонент ОС (объектов), участвующих в загрузке (иными словами - объектов, принадлежащих множеству Oz), причем неизменность установлена до порождения первого субъекта из ZL;
- установлена неизменность объектов, определяющих последовательность активизации компонент ОС (с учетом нескольких уровней иерархии), неизменность обеспечена в течение заданного интервала времени; состояние указанных объектов не может быть изменено никем, кроме предопределенного пользователя (пользователей) АС (это условие соответствует неизменности последовательности ZL).

Легко видеть, что процедура доверенной загрузки обеспечивает одинаковое состояние АС после выполнения загрузки (согласно утверждению 4).

Основная техническая проблема при реализации доверенной загрузки состоит в доступе к объектам высшего уровня иерархии ОС (файлам) до загрузки ядра данной ОС (загружаемую ОС далее будем называть пользовательской). Однако при возможности генерации ИПС для какой-либо иной ОС (далее будем называть ее базовой) можно предложить итеративную реализацию доверенной загрузки с использованием ресурсов указанной ОС.

Рассмотрим реализацию доверенной загрузки ОС на основе генерации ИПС для одной из операционных сред вычислительной системы. Предположим, что имеется базовая операционная система, для которой возможна полноценная генерация ИПС. Пусть в вычислительной Системе существуют еще операционные системы Os1, 0s2, ..., OSn. Ставится задача доверенного запуска операционной среды OSj. Пусть в базовой операционной системе имеется некоторое условно называемое "шлюзовое ПО" между базовой операционной системой и OSj. Функции шлюзового ПО заключаются в обеспечении доступа к файловой системе операционной системы OSj (т. е. объектам уровня R).

Пусть также пользователь i имеет физический доступ к комплекту технических средств (рабочему месту) сети (ЭВМ) Tm, на котором установлена операционная система OSj. При использовании комплекта Tm пользователем i.

1. Происходит аутентификация пользователя i (по его индивидуальной информации).

2. Проверяются права пользователя по использованию аппаратной компоненты комплекта Tm.

3. Контролируется целостность (на основе информации пользователя Ki либо без нее)

всех объектов базовой ОС, размещенных на некотором носителе, локально или удаленно (через технические средства ЛВС) связанном с Тт.

4. Загружается базовая операционная система и контролируется целостность шлюзового ПО.

5. Загружается шлюзовое ПО (при этом становится доступной как минимум в режиме чтения файловая структура OSj, размещенная локально на Tm).

6. Контролируется целостность объектов уровней, меньших Rj (Rj - максимальный уровень представления объектов в OSj) для OSj (см. выше).

7. Контролируется целостность объектов уровня Rj (файлов) OSj.

8. Контролируется целостность объекта, задающего последовательность загрузки компонент.

9. Осуществляется принудительная загрузка (инициируется предопределенный в силу целостности объектов Oz и последовательности ZL порядок загрузки компонент ОС) проверенной на целостность OSj.

Утверждение 8 (условия генерации ИПС при реализации метода)

Пусть ядро ОС содержит МБО и МБС, инициируемые в ОС субъекты попарно корректны, их объекты-источники принадлежит множеству проверяемых на неизменность в ходе доверенной загрузки, МБО запрещает изменение любого объекта-источника и выполнена процедура доверенной загрузки ОС. Тогда после инициирования ядра ОС генерируется ИПС.

Доказательство. Процедура доверенной загрузки по построению обеспечивает неизменность Oz и ZL, по условию утверждения для порождения субъектов разрешены только объекты-источники, принадлежащие 0z, неизменность объектов-источников по условию гарантируется свойствами МБО. Следовательно, выполнены условия утверждения 5 и генерируется ИПС. Утверждение доказано.

4. Математические модели информационной безопасности

Модель информационной безопасности - формальное выражение политики безопасности.

Формальные модели необходимы и используются достаточно широко, потому что только с их помощью можно доказать безопасность системы опираясь при этом на объективные и неопровержимые постулаты математической теории. модели безопасности позволяют обосновать жизнеспособность системы и определяют базовые принципы ее архитектуры и используемые при ее построении технологические решения Основная цель создания политики безопасности информационной системы и описания ее в виде формальной модели — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Кроме того, формальные модели безопасности позволяют решить еще целый ряд задач возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации защищенных информационных систем (производители, потребители, эксперты-квалификаторы).

Производители защищенных информационных систем используют модели безопасности в следующих случаях:

- при составлении формальной спецификации политики безопасности разрабатываемой системы;
- при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты;
- в процессе анализа безопасности системы в качестве эталонной модели;

- при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности.

Потребители путем составления формальных моделей безопасности получают возможности довести до сведения производителей свои требования в четко определённой и непротиворечивой форме, а также оценить соответствие защищенных систем своим потребностям. Эксперты по квалификации в ходе анализа адекватности реализации политики безопасности в защищенных системах используют модели безопасности в качестве эталонов.

Все рассматриваемые модели безопасности основаны на следующих базовых представлениях:

1. Система является совокупностью взаимодействующих сущностей — субъектов и объектов. *Б*езопасность обработки информации и обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности. Считается, что система безопасна, если субъекты не имеют возможности нарушить правила политики безопасности.

2. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов отношений определяется в виде набора операций, которые субъекты могут производить над объектами.

3. Все операции контролируются монитором взаимодействий и либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

4. Политика безопасности задается в виде правил, в соответствии с которыми должны осуществляться все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

5. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет состояние системы. Каждое состояние системы является либо безопасным, либо небезопасным в соответствии с предложенным в модели критерием безопасности.

6. Основной элемент модели безопасности — это доказательство утверждения (теоремы) о том, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

4.1. Классификация математических моделей информационной безопасности по основным видам угроз

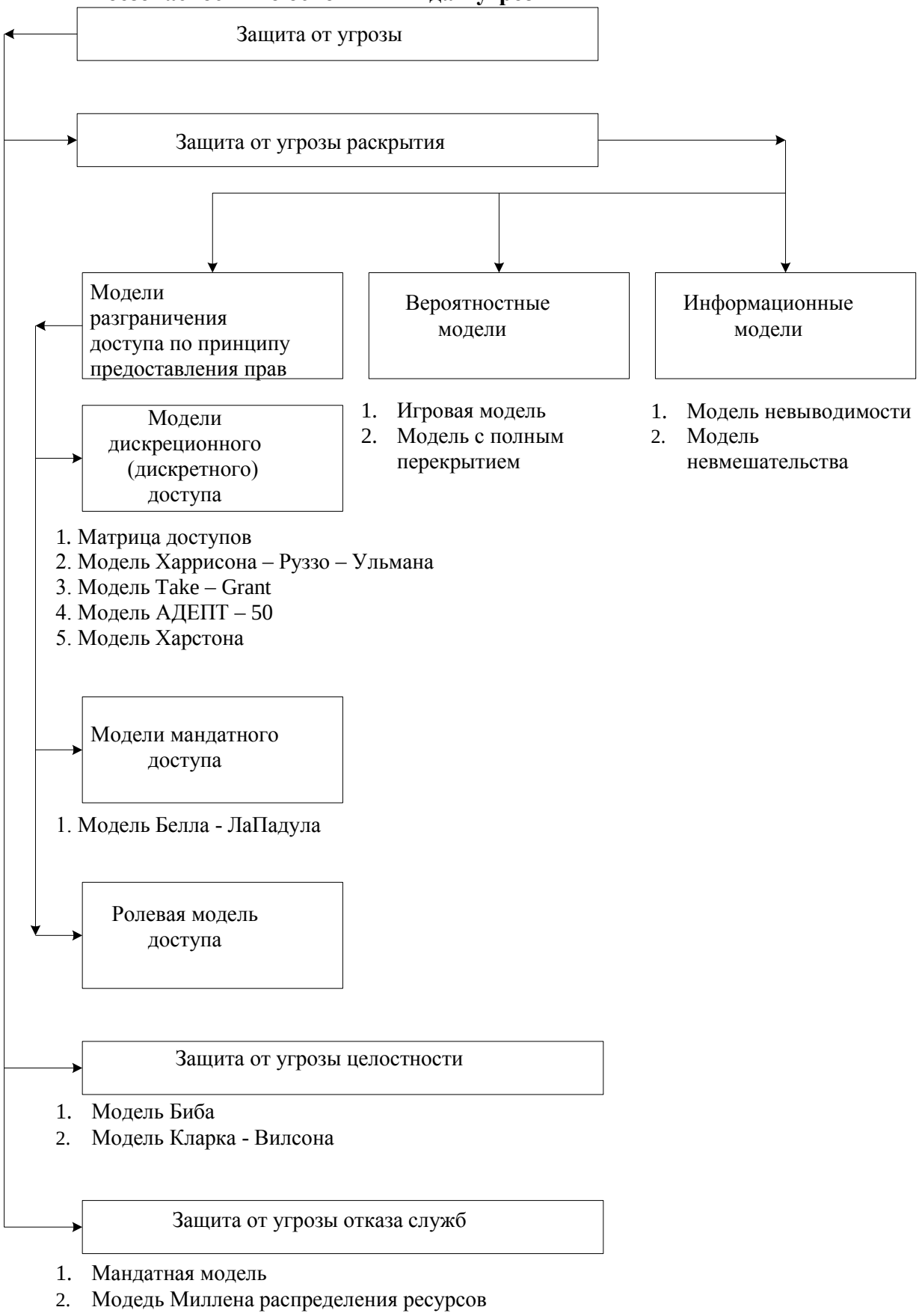


Рис. 4.1. – Классификация моделей информационной безопасности

4.2. Модели разграничения доступа (защита от угрозы раскрытия информации)

4.2.1. Описание системы защиты с помощью матрицы доступа

Пусть O - множество объектов, S - множество субъектов, $S \subseteq O$. Пусть $U=\{U_1,...,U_m\}$ - множество пользователей. Определим отображение: own: $0 \rightarrow U$.

В соответствии с этим отображением каждый объект объявляется собственностью соответствующего пользователя. Пользователь, являющийся собственником объекта, имеет все права доступа к нему, а иногда и право передавать часть или все права другим пользователям. Кроме того, собственник объекта определяет права доступа других субъектов к этому объекту, то есть политику безопасности в отношении этого объекта. Указанные права доступа записываются в виде матрицы доступа, элементы которой - суть подмножества множества **R**, определяющие доступы субъекта S, к объекту 0_i(i = 1, 2,...,; j = 1, 2,...).

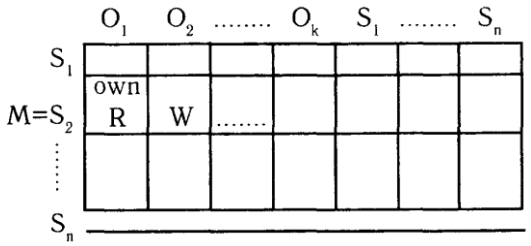


Рис. 4.2. Матрица доступов

Существует несколько вариантов задания матрицы доступа.

1. Листы возможностей: Для каждого субъекта S_i создается лист (файл) всех объектов, к которому имеет доступ данный объект.

2. Листы контроля доступа: для каждого объекта создается список всех субъектов, имеющих право доступа к этому объекту.

Дискреционная политика связана с исходной моделью таким образом, что траектории процессов в вычислительной системе ограничиваются в каждом доступе. Причем вершины каждого графа разбиваются на классы и доступ в каждом классе определяется своими правилами каждым собственником. Множество неблагоприятных траекторий ***N*** для рассматриваемого класса политик определяется наличием неблагоприятных состояний, которые в свою очередь определяются запретами на некоторые дуги. Дискреционная политика наиболее исследована. Существует множество разновидностей этой политики. Однако многих проблем защиты эта политика решить не может. Одна из самых существенных слабостей этого класса политик - то, что они не выдерживают атак при помощи «троянского коня». Это означает, в частности, что система защиты, реализующая дискреционную политику, плохо защищает от проникновения вирусов в систему и других средств скрытого разрушающего воздействия. Покажем на примере принцип атаки "Троянским конем" в случае дискреционной политики.

Пример 1: Пусть U_1 - некоторый пользователь, а U_2 - пользователь-злоумышленник, O_1 - объект, содержащий ценную информацию, O_2 - программа с «троянским конем» T, и M - матрица доступа, которая имеет вид:

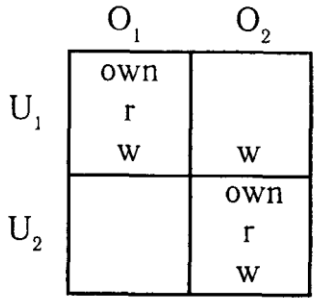


Рис. 4.3.

Проникновение программы происходит следующим образом. Злоумышленник U_2 создает программу O_2 и, являясь ее собственником, дает U_1 запускать ее и писать в объект O_2 информацию. После этого он инициирует каким-то образом, чтобы U_1 запустил эту программу (например, O_2 - представляет интересную компьютерную игру, которую он предлагает U_1 для развлечения). U_1 запускает O_2 и тем самым запускает скрытую программу T, которая обладая правами U_1 (т.к.была запущена пользователем U_1), списывает в себя информацию, содержащуюся в O_1. После этого хозяин U_2 объекта O_2, пользуясь всеми правами, имеет возможность считать из O_2 ценную информацию объекта O_1.

Следующая проблема дискреционной политики -это автоматическое определение прав. Так как объектов много, то задать заранее вручную перечень прав каждого субъекта на доступ к объекту невозможно. Поэтому матрица доступа различными способами агрегируется, например, оставляются в качестве субъектов только пользователи, а в соответствующую ячейку матрицы вставляются формулы функций, вычисление которых определяет права доступа субъекта, порожденного пользователем, к объекту O. Разумеется, эти функции могут изменяться во времени. В частности, возможно изъятие прав после выполнения некоторого события. Возможны модификации, зависящие от других параметров.

Одна из важнейших проблем при использовании дискреционной политики - это проблема контроля распространения прав доступа. Чаще всего бывает, что владелец файла передает содержание файла другому пользователю и тот, тем самым, приобретает права собственника на информацию. Таким образом, права могут распространяться, и даже, если исходный владелец не хотел передавать доступ некоторому субъекту S к своей информации в O, то после нескольких шагов передача прав может состояться независимо от его воли. Возникает задача об условиях, при которых в такой системе некоторый субъект рано или поздно получит требуемый ему доступ. Эта задача исследовалась в модели "take-grant", когда форма передачи или взятия прав определяются в виде специального права доступа (вместо own).

4.2.2. Дискреционная модель «Хиррисона–Руззо-Ульмана»

Модель безопасности Харрисона-Руззо-Ульмана, являющаяся классической дискреционной моделью, реализует произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа.

В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей — субъектов (множество S), которые осуществляют доступ к информации, пассивных сущностей — объектов (множество O), содержащих защищаемую информацию, и конечного множества прав доступа $R = \{r_{1p} .... r_{п}\}$, означающих полномочия на выполнение соответствующих действий (например, чтение, запись, выполнение).

Поведение системы моделируется с помощью понятия состояния. Пространство состояний системы образуется декартовым произведением множеств составляющих ее объектов, субъектов и прав — OxSxR. Текущее состояние системы Q в этом пространстве

определяется тройкой, состоящей из множества субъектов, множества объектов и матрицы прав доступа M, описывающей текущие права доступа субъектов к объектам, — Q=(S,O,M). Строки матрицы соответствуют субъектам, а столбцы — объектам, поскольку множество объектов включает в себя множество субъектов, матрица имеет вид прямоугольника. Любая ячейка матрицы M[s,o] содержит набор прав субъекта s к объекту o, принадлежащих множеству прав доступа R. Поведение системы во времени моделируется переходами между различными состояниями. Переход осуществляется путем внесения изменений в матрицу M с помощью команд.

В классической модели допустимы только следующие элементарные операции:

enter r into M[s,o] (добавление субъекту s права r для объекта o)
delete r from M[s,o] (удаление у субъекта s права r для объекта o)
create subject s (создание нового субъекта s)
create object o (создание нового объекта o)
destroy subject s (удаление существующего субъекта S)
destroy object o (удаление существующего объекта o)

Применение любой элементарной операции op в системе, находящейся в состоянии Q=(S,O,M) влечет за собой переход в другое состояние $Q'=(S',O',M^I)$, которое отличается от предыдущего состояния Q по крайней мере одним компонентом.

Операция **enter** вводит право r в существующую ячейку матрицы доступа. Содержимое каждой ячейки рассматривается как множество, т.е. если это право уже имеется, то ячейка не изменяется. Операция называется **enter** монотонной, поскольку она только добавляет права в матрицу доступа и ничего не удаляет. Действие операции **delete** противоположно действию операции **enter.** Она удаляет право из ячейки матрицы доступа, если оно там присутствует. Поскольку содержимое каждой ячейки рассматривается как множество, **delete** не делает ничего, если удаляемое право отсутствует в указанной ячейке. Поскольку **delete** удаляет информацию из матрицы доступа, она назьшается немонотонной операцией. Операции **create subject** и **destroy subject** представляют собой аналогичную пару монотонной и немонотонной операции.

Заметим, что для каждой операции существует еще и предусловие ее выполнения: для того чтобы изменить ячейку матрицы доступа с помощью операций **enter** пли **delete** необходимо, чтобы эта ячейка существовала, т. е. чтобы существовали соответствующие субъект и объект. Предусловиями операций создания **create subject/object,** является отсутствие создаваемого субъекта/объекта, операций удаления **destroy subject/object** — наличие субъекта/объекта. Если предусловие любой операции не выполнено, то ее выполнение безрезультатно.

Формальное описание системы ∑(Q,R,C) состоит из следующих элементов:

- конечный набор прав доступа $R = \{r_1, ..., r_n\}$;
- конечные наборы исходных субъектов $So = \{s_1, ... s_i\}$ и объектов $O_0 = \{o_1, ..., o_m\}$, где $So \subseteq O_0$;
- исходная матрица доступа, содержащая права доступа субъектов к объектам — M_o;
- конечный набор команд $O\{aj(x_1, x_k)\}$, каждая из которых состоит из условий выполнения и интерпретации в терминах перечисленных элементарных операций.

Поведение системы во времени моделируется с помощью последовательности состояний {Qj}, в которой каждое последующее состояние является результатом применения некоторой команды из множества C к предыдущему $Q_{n+1} = C_n(Q_n)$.Каждое состояние определяет отношения доступа, которые существуют между сущностями системы в виде множества субъектов, объектов и матрицы прав. Поскольку для обеспечения безопасности необходимо наложить запрет на некоторые отношения доступа, для заданного начального

состояния системы должна существовать возможность определить множество состояний, в которые она сможет из него попасть. Это позволит задавать такие начальные условия (интерпретацию команд C, множества объектов Oo, субъектов So и матрицу доступа M_o), при которых система никогда не сможет попасть в состояния, не желательные с точки зрения безопасности. Следовательно, для построения системы с предсказуемым поведением необходимо для заданных начальных условий получить ответ на вопрос: сможет ли некоторый субъект s когда-либо приобрести право доступа r для некоторого объекта o?

Критерий безопасности модели Харрисона–Руззо-Ульмана формулируется следующим образом:

Для заданной системы начальное состояние Qo = (So,Oo,Mo) является безопасным относительно права r, если не существует применимой к Qo последовательности команд, в результате которой право r будет занесено в ячейку матрицы M, в которой оно отсутствовало в состоянии Q_0.

Смысл данного критерия состоит в том, что для безопасной конфигурации системы субъект никогда не получит право r доступа к объекту, если он не имел его изначально.

Из критерия безопасности следует, что для данной модели ключевую роль играет выбор значений прав доступа и их использование в условиях команд. Хотя модель не налагает никаких ограничений на смысл прав и считает их равнозначными, те из них, которые участвуют в условиях выполнения команд, фактически представляют собой не права доступа к объектам (как, например, чтение и запись), а права управления доступом, или права на осуществление модификации ячеек матрицы доступа. Таким образом, по сути дела данная модель описывает не только доступ субъектов к объектам, а распространение прав доступа от субъекта к субъекту, поскольку именно изменение содержания ячеек матрицы доступа определяет возможность выполнения команд, в том числе команд, модифицирующих саму матрицу доступа, которые потенциально могут привести к нарушению критерия безопасности.

Необходимо отметить, что с точки зрения практики построения защищенных систем модель Харрисона – Руззо - Ульмана является наиболее простой в реализаций и эффективной в управлении, поскольку не требует никаких сложных алгоритмов, и позволяет управлять полномочиями пользователей с точностью до операции над объектом, чем и объясняется ее распространенность среди современных систем. Кроме того, предложенный в данной модели критерий безопасности является весьма сильным в практическом плане, поскольку позволяет гарантировать недоступность определенной информации для пользователей, которым изначально не выданы соответствующие полномочия.

Однако, Харрисон, Руззо и Ульман доказали, что в общем случае не существует алгоритма, который может для произвольной системы, ее начального состояния Qo = ($So,0_0,M_0$) и общего права r решить, является ли данная конфигурация безопасной. Доказательство опирается на свойства машины Тьюринга, с помощью которой моделируется последовательность переходов системы из состояния в состояние.

Как уже было сказано, все дискреционные модели уязвимы по отношению к атаке с помощью «троянского коня», поскольку в них контролируются только операции доступа субъектов к объектам, а не потоки информации между ними. Поэтому, когда "троянская" программа, которую нарушитель подсунул некоторому пользователю, переносит информацию из доступного этому пользователю объекта в объект, доступный нарушителю, то формально никакое правило дискреционной политики безопасности не нарушается, но утечка информации происходит.

Таким образом, дискреционная модель Харрисона – Руззо - Ульмана в своей общей постановке не дает гарантий безопасности системы, однако именно она послужила основой для целого класса моделей политик безопасности, которые используются для управления доступом и контроля за распространением прав во всех современных системах.

4.2.3. Модель «Take-Grant»

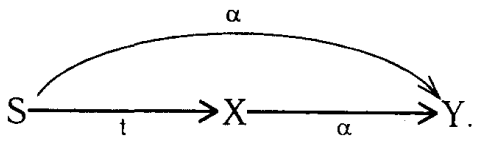
Модель распространения прав доступа Take–Grant, предложенная впервые в 1976г., используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа в таких системах. В качестве основных элементов модели используются граф доступа и правила его преобразования. Цель модели – дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступа. В настоящее время данная модель получила продолжение как расширенная модель Take–Grant, в которой рассматриваются пути возникновения информационных потоков в системах с дискреционным разграничением доступа.

Перейдем к формальному описанию модели. Обозначим: **O** - множество объектов (файлы), **S** – множество активных субъектов (пользователи); R={r, w, c} - множество доступов, где r - читать, w - писать, c - вызывать. Допускается, что субъект X может иметь права $\alpha \subseteq R$ на доступ к объекту Y, эти права записываются в матрице контроля доступов. Кроме этих прав мы введем еще два: право take (t) – право брать права доступа и право grant (g) – право давать права доступа, которые также записываются в матрицу контроля доступов субъекта к объектам. Можно считать, что эти права определяют возможности преобразования одних графов состояний в другие. Преобразование состояний, то есть преобразование графов доступов, проводятся при помощи команд. Существует 4 вида команд, по которым один граф доступа преобразуется в другой.

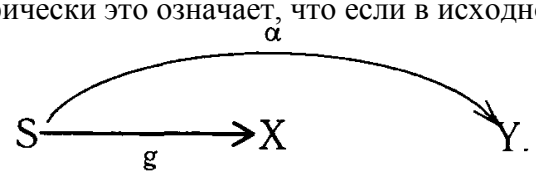
1. **Take (брать)**. Пусть S - субъект, обладающий правом t к объекту X и $\alpha \subseteq R$ - некоторое право доступа объекта X к объекту Y. Тогда возможна команда "S take α forY from X". В результате выполнения этой команды в множество прав доступа субъекта S к объекту Y добавляется право α. Графически это означает, что, если в исходном графе доступов G был подграф

$$S \xrightarrow{t} X \xrightarrow{\alpha} Y$$

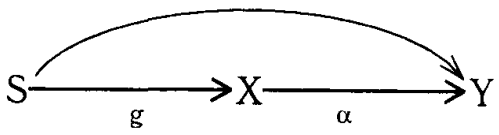
то в новом состоянии G', построенном по этой команде t, будет подграф



2. **Grant (давать)**. Пусть субъект S обладает правом *g* к объекту X и правом $\alpha \subseteq R$ к объекту Y. Тогда возможна команда "S grant α for Y to X". В результате выполнения этой команды граф доступов G преобразуется в новый граф G', который отличается от G добавленной дугой (X Y). Графически это означает, что если в исходном графе G был подграф



то в новом состоянии G будет подграф:



3. **Create (создавать)**. Пусть S - субъект, $\beta \subseteq R$. Команда "S create P for new object X" создает в графе новую вершину X и определяет P как права доступов S к X. То есть по сравнению с графом G в новом состоянии G' добавляется подграф вида

$$S \xrightarrow{\beta} X$$

4. **Remove (удалить)**. Пусть S - субъект и X - объект, β⊆R. Команда "S remove P for X" исключает права доступа P из прав субъекта S к объекту X. Графически преобразования графа доступа G в новое состояние G' в результате этой команды можно изобразить следующим образом:

$$S \xrightarrow{p} X, S \xrightarrow{p/\beta} X$$

Под безопасностью будем понимать возможность или невозможность произвольной фиксированной вершине P получить доступ α∈R к произвольной фиксированной вершине X путем преобразования текущего графа G некоторой последовательностью команд в граф G', где указанный доступ разрешен.

Определение. В графе доступов G вершины P и S называются tg-связными, если существует путь в G, соединяющий P и S, безотносительно ориентации дуг, но такой, что каждое ребро этого пути имеет метку, включающую t или *g*.

Примем без доказательств следующие теоремы.

Теорема 1. *Субъект P может получить доступа к, объекту X, если существует субъект S, имеющий доступ a, к вершине X такой, что субъекты P и S связаны произвольно ориентированной дугой, содержащей хотя бы одно из прав t или g*

Теорема. 2. *Пусть в системе все объекты являются субъектами. Тогда субъект P может получить доступ a к субъекту X тогда и только тогда, когда выполняются условия:*

1. Существует субъект S такой, что в текущем графеG есть дуга $S \xrightarrow{\alpha} X$.
2. S tg-связна с P.

Перечисленный правила «Брать», «Давать», «Создавать», «Уничтожать» для отличия от правил расширенной модели Take – Grant будем называть де – юре правилами.

4.2.4. Расширенная модель Take–Grant

В расширенной модели Take–Grant рассматриваются пути и стоимости возникновения информационных потоков в системах с дискреционным разграничением доступа.

В классической модели Take–Grant по существу рассматриваются два права доступа: t и g, а так же четыре правила (правила де-юре) преобразования графа доступов. В расширенной модели дополнительно рассматриваются два права: на чтение r (read) и на запись w (write), а так же шесть правил (правила де-факто) преобразования графа доступов: pose, spy, find, pass и два правила без названия.

В результате применения к графу доступов правил де–факто в него добавляются мнимые дуги, помеченные r или w и изображаемые пунктиром (рисунок). Вместе с дугами графа, соответствующими правам r и w (реальными дугами), мнимые дуги указывают на направления информационных каналов в системе.

Состояние системы описывается его графом. Переход из состояния в состояние определяется операциями или правилами преобразования графа доступов. Преобразование графа G а граф G’ в результате выполнения правила op обозначим $G \mid_{op} G'$.

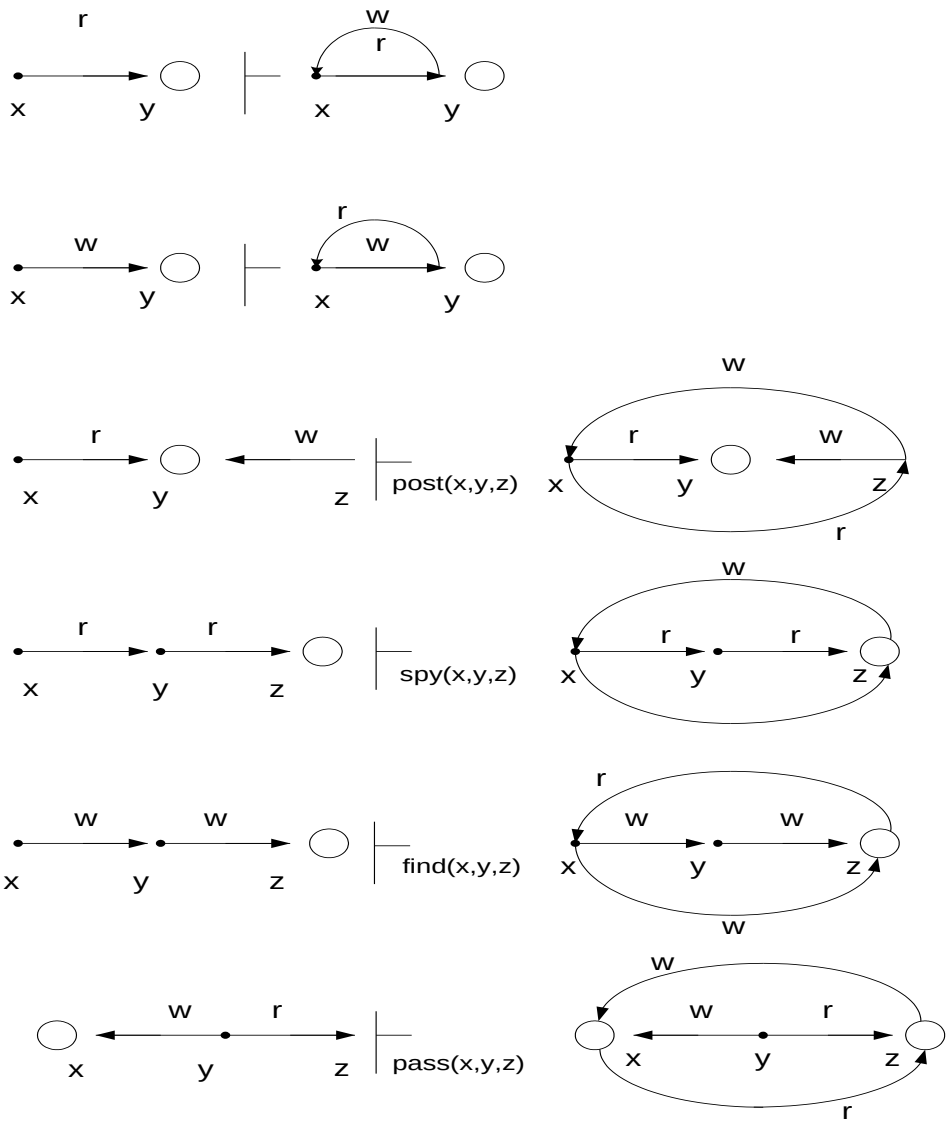


Рис. 4.4. Правила де–факто

К мнимым дугам нельзя применять правила де – юре преобразования графа доступов. Информационные каналы нельзя брать или передавать другим объектам системы.

Проблемы взаимодействия – центральный вопрос при похищении прав доступа.

Каждое правило де–юре требует для достижения своей цели участия одного субъекта, а для реализации правила де–факто необходим один или два субъекта. Желательно во множестве всех субъектов выделить подмножество так называемых субъектов - заговорщиков – участников процессов передачи прав или информации. В небольших системах эта задача легко решаема. Многократное просматривая граф доступов и применяя к нему все возможные правила де–юре и де–факто, можно найти замыкание графа доступов, которое будет содержать дуги, соответствующие всем информационным каналам системы. Однако, если граф доступов большой, то найти его замыкание весьма сложно.

Допустим, факт нежелательной передачи прав или информации состоялся. Каков наиболее вероятный путь его осуществления? В классической модели Take–Grant не дается прямого ответа.

Предположим, что чем больше узлов на пути между вершинами, по которым произошла передача прав доступа или возник информационный поток, тем меньше вероятность использования этого пути. Например, на рисунке 4 видно, что интуитивно наиболее вероятный путь передачи информации от субъекта z к субъекту x лежит через объект y. В тоже время злоумышленник может специально использовать более длинный путь.

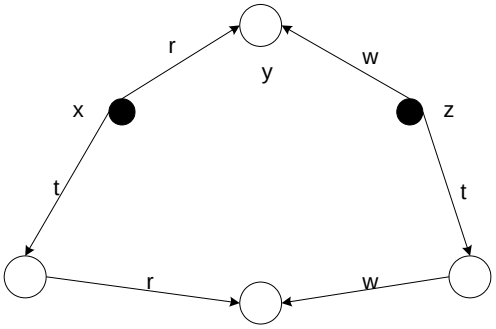


Рис. 4.5. Пути возникновения информационного канала от z к x

Таким образом, в расширенную модель Take–Grant можно включить понятие вероятности и стоимости пути передачи прав или информации. Путям наименьшей стоимости соответствует наивысшая вероятность и их исследуют в первую очередь.

К моделям дискреционного пита так же относятся модель АДЕПТ-50 и модель Харстона. Дадим им краткую характеристику.

4.2.5. Модель АДЕПТ–50

В данной модели представлены четыре типа сущностей (любая именованная составляющая компьютерной системы): пользователи(u), задания(j), терминалы(t) и файлы(f), причем каждая сущность описывается тройкой: (L,F,M), где режим M - набор видов доступа, полномочия F – группа пользователей, имеющих право на доступ к определенному объекту.

Сформулируем правила этой модели:

1. Пользователь u получает доступ к системе$\Leftrightarrow$ u$\in$ U.

2. Пользователь u получает доступ к терминалу t$\Leftrightarrow$ u $\in$ F(t), т.е. в том случае когда пользователь имеет право использовать терминал t.

3. Пользователь получает доступ к файлу j$\Leftrightarrow$ A(j) $\geq$A(f), C(j)$\supseteq$ C(f) , M(j) $\supseteq$M, f $\in$ F(f) т.е. в случае:

- привилегии выполняемого задания шире привилегий файла или равны им;
- пользователь является членом F(f).

Т.е. пользователь получает доступ к объекту тогда, когда он принадлежит группе пользователей, имеющих доступ к этому объекту, и его задание шире или равны привилегии объекта. Например, наивысшее полномочие доступа к файлу пользователя «сов. секретно», выполняющего задание с «конфиденциального» терминала будет «конфиденциально».

4.2.6. Модель Харстона

Модель имеет пять основных наборов:

A – установленных полномочий;

U - пользователей;

E – операций;

R – ресурсов;

S – состояний.

Область безопасности будет выглядеть как произведение: A×U×E×R×S. Процесс организации доступа можно описать алгоритмически. Он будет состоять из следующих процедур:

1. Вызвать все вспомогательные программы необходимые для предварительного принятия решения.
2. Определить из U те группы, к которым принадлежит u. Затем выбрать из P (набор установленных полномочий) спецификации полномочий, которым соответствует u. Этот набор полномочий F(u) определяет привилегию пользователя u.
3. Из P определить набор полномочий F(e) , устанавливающие e как основную операцию. Такой набор называется привилегией e.
4. Определить из P набор F(R) (привилегию единичного ресурса) – полномочия, определяющие поднабор ресурсов из R^1(определенных единиц ресурсов), имеющие общие элементы с R.
5. Удостоверится, что R полностью включается в D(q) =F(u)∩ F(e)F(R) (домен полномочий).
6. Разбить D(q) на эквивалентные классы, так чтобы два полномочия попадали в эквивалентный класс тогда и только тогда, когда они специфицируют одну единицу ресурса. Новый набор полномочий F(u,q) – привилегия пользователя u по отношению к запросу q .
7. Вычислить EAC – условие фактического доступа, соответствующего запросу q.
8. Оценить EAC и принять решение о доступе:
   - разрешить доступ к R , если R перекрывается;
   - отказать в доступе в противном случае.
9. Произвести запись необходимых событий.
10. Вызвать все программы необходимые для принятия решения.
11. Выполнить все вспомогательные программы.
12. Если решение о доступе – положительное, завершить физическую обработку.

Т.е. пользователь может получить (или не получить) доступ к информации предварительно пройдя соответствующие этапы идентификации (определение группы, его полномочий, условия фактического доступа и т.д.).

Данная модель не всегда необходима в полном объеме. Например, во время регистрации пользователя системы необходим пункт 2 и 6.

4.2.7. Мандатная модель Белла-ЛаПадулы

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных и правительственных учреждениях многих стран. Основным положением политики Белла - ЛаПадулы, взятым ими из реальном жизни, является назначение всем участникам процесса обработки защищаемой информации, и документам, в которых она содержится, специальной метки, например, секретно, сов. секретно и т. д, получившей название уровня безопасности. Все уровни безопасности упорядочиваются с помощью установленного отношения доминирования, например, уровень сов. секретно считается более высоким чем уровень секретно, или доминирует над ним. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух простых правил:

1. Уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.
2. Уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

Первое правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых). Второе правило (далее мы увидим, что оно более важное) предотвращает утечку информации (сознательную или несознательную) со стороны высокоуровневых участников процесса обработки информации к низкоуровневым.

Таким образом, если в дискреционных моделях управление доступом происходит путем наделения пользователей полномочиями осуществлять определенные операции над определенными объектами, то мандатные модели управляют доступом неявным образом — с помощью назначения всем сущностям системы уровнен безопасности, которые определяют все допустимые взаимодействия между ними.

Система в модели безопасности Белла–ЛаПадулы, как и другие модели, представляется в виде множеств субъектов S, объектов O (множество объектов включает множество субъектов, ScO) и прав доступа read и write. В мандатной модели рассматриваются только эти два вида доступа, и, хотя она может быть расширена введением дополнительных прав (например, правом на добавление информации, выполнение программ и т.д.), все они будут отображаться в базовые (чтение и запись)..Использование столь жесткого подхода, не позволяющего осуществлять гибкое управление доступом, объясняется тем, что в мандатной модели контролируются не операции, осуществляемые субъектом над объектом, а потоки информации, которые могут быть только двух видов: либо от субъекта к объекту (запись), либо от объекта к субъекту (чтение).

Уровни безопасности субъектов и объектов задаются с помощью функции уровня безопасности F: $S \cup O \rightarrow L$, которая ставит в соответствие каждому субъекту и объекту уровень безопасности, принадлежащий множеству уровней безопасности L

4.2.8. Решетка уровней безопасности

Решетка уровней безопасности -— это формальная алгебра (L, <, •, ⊕), где L — базовое множество уровней безопасности, а оператор < определяет частичное нестрогое отношение порядка для элементов этого множества, т.е. оператор < — антисимметричен, транзитивен и рефлексивен. Отношение < на L:

1. рефлексивно, если $\forall a \in L: a < a$;

2. антисимметрично, если $\forall\ a_1, a_2 \in L: (a_1<a_2 \wedge a_2<a_1) \Rightarrow a_1 = a_2$;

3.транзитивно,если $\forall\ a_1, a_2, a_3 \in L: (a_1<a_2 \wedge a_2<a_3) \Rightarrow a_1<a_3$.

Другое свойство решетки состоит в том, что для каждой пары a1 и a2 элементов множества L можно указать единственный элемент наименьшей верхней границы и единственный элемент наибольшей нижней границы. Эти элементы также принадлежат L.

Смысл этих определений заключается в том, что для каждой пары элементов всегда можно указать единственный элемент, ограничивающий ее сверху или снизу таким образом, что между ними и этим элементом не будет других элементов.

Функция уровня безопасности F назначает каждому субъекту и объекту некоторый уровень безопасности из L, разбивая множество сущностей системы на классы, в пределах которых их свойства с точки зрения модели безопасности являются эквивалентными. Тогда оператор < определяет направление потоков информации, то есть, если F(A) < F(B), то информация может передаваться от элементов класса A элементам класса B.

Покажем, почему в модели Белла-ЛаПадулы для описания отношения доминирования на множестве уровней безопасности используется решетка.

Если информация может передаваться от сущностей класса A к сущностям класса B, а также от сущностей класса B к сущностям класса A, то классы A и B содержат одноуровневую информацию и с точки зрения безопасности эквивалентны одному классу (AB). Поэтому для удаления избыточных классов необходимо, чтобы отношение < было антисимметричным.

Если информация может передаваться от сущностей класса A сущностям класса B, а также от сущностей класса B к сущностям класса C, то очевидно, что она будет также передаваться от сущностей класса A к сущностям класса C. Таким образом, отношение < должно быть транзитивным.

Так как класс сущности определяет уровень безопасности содержащейся в ней информации, то псе сущности одного и того же класса содержат с точки зрения безопасности одинаковую информацию. Следовательно, нет смысла запрещать потоки информации между сущностями одного и того же класса. Более того, из чисто практических соображений нужно предусмотреть возможность для сущности передавать информацию самой себе. Следовательно, отношение < должно быть рефлексивным.

Использование решетки для описания отношений между уровнями безопасности позволяет использовать в качестве атрибутов безопасности (элементов множества L) не только целые числа, для которых определено отношение "меньше или равно", но и более сложные составные элементы. Например, в государственных организациях достаточно часто в качестве атрибутов безопасности используется комбинации, состоящие из уровня безопасности, представляющие собой целое число, и набора категорий из некоторого множества.

4.2.9. Классическая мандатная модель Белла–ЛаПадулы

В мандатных моделях функция уровня безопасности F вместе с решеткой уровней определяют все допустимые отношения доступа между сущностями системы, поэтому множество состояний системы V представляется в виде набора упорядоченных пар (F,M), где M - это матрица доступа, отражающая текущую ситуацию с правами доступа субъектов к объектам, содержание которой аналогично матрице прав доступа в модели Харрисона – Руззо –Ульмана, но набор прав ограничен правами read и write. Модель системы $\sum(v_0,R,T)$ состоит из начального состояния v_0, множества запросов R и функции перехода $T:(VxR)\rightarrow V$, которая в ходе выполнения запроса переводит систему из одного состояния в другое. Система, находящаяся в состоянии $v \in V$, при получении запроса $r \in R$, переходит в следующее состояние v* = T(v, r).Состояние v достижимо в системе $\sum(v_0,R,T)$ тогда и только тогда, когда существует последовательность $<(r0,Vo),...,(r_n\text{-}_1,Vn\text{-}_1).(r_n,v)>$ такая, что $T(r_i\ v_i) = v_{i+1}$ для $0<i<n$.

Как и для дискреционной модели состояния системы делятся на безопасные, в которых отношения доступа не противоречат установленным в модели правилам, и небезопасные, в которых эти правила нарушаются и происходит утечка информации.

Белл и ЛаПадула предложили следующее определение безопасного состояния:

1. Состояние (F,M) называется безопасным по чтению (или просто безопасным) тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности этого субъекта доминирует над уровнем безопасности этого объекта.
2. Состояние (F,M) называется безопасным по записи(или * - безопасным) тогда и только тогда, когда для каждою субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над уровнем безопасности этого субъекта.
3. Состояние безопасно тогда и только тогда, когда оно безопасно и по чтению, и по записи.

В соответствии с предложенным определением безопасного состояния критерий безопасности системы выглядит следующим образом:

Система $\sum(v_0,R,T)$ безопасна тогда и только тогда, когда ее начальное состояние v_0 безопасно и вct состояния, достижимые из v_0 путем применения конечной последовательности запросов из R безопасны.

Белл и ЛаПадула доказали теорему, формально доказывающую безопасность системы при соблюдении определенных условий, получившую название основной теоремы безопасности.

Основная теорема безопасности Белла-ЛаПадулы [3]

Система Z(Vo,R,T) безопасна тогда и только тогда, когда:

а) начальное состояние. v_0 безопасно и

б) для любого состояния v, достижимого из v_0 путем применения конечной последовательности запросов из R таких, что T(v,r) = v*, v = (F,M) и v* = (F*,M*) для каждого $s \in S$ и $o \in O$ выполняются следующие условия:

1. если read $\in$ M*[s,o] и read $\notin$ M[s,o], то F*(s)> F*(o);
2. если read $\in$ M[s,o] и F*(s)<F*(o), то read $\notin$ M* [s,o];
3. если write $\in$ M*[s,o] и write $\notin$ M[s,o], то F*(o)> F*(s);
4. если write $\in$ M[s,o] и F*(o)<F*(s), то write $\notin$ M* [s,o].

Таким образом, теорема утверждает, что система с безопасным начальным состоянием является безопасной тогда и только тогда, когда при любом переходе системы из одного состояния в другое не возникает никаких новых и не сохраняется никаких старых отношений доступа, которые будут небезопасны по отношению к функции уровня безопасности нового состояния. Формально эта теорема определяет все необходимые и достаточные условия, которые должны быть выполнены для того, чтобы система, начав свою работу в безопасном состоянии, никогда не достигла небезопасного состояния.

4.2.10. Безопасная функция перехода

Недостаток основной теоремы безопасности Белла-ЛаПадулы состоит в том, что ограничения, накладываемые теоремой на функцию перехода, совпадают с критериями безопасности состояния, поэтому данная теорема является избыточной по отношению к определению безопасного состояния. Кроме того, из теоремы следует только то, что все состояния, достижимые из безопасного состояния при определенных ограничения, будут в некотором смысле безопасны, по при этом не гарантируется, что они будут достигнуты без потери свойства безопасности в процессе осуществления перехода. Поскольку у нас нет никаких определенных ограничений на вид функции перехода, кроме указанных в условиях теоремы, и допускается, что уровни безопасности субъектов и объектов могут изменяться, то можно представить такую гипотетическую систему (она получила название Z-системы), в которой при попытке низкоуровневого субъекта прочитать информацию из высокоуровневого объекта будет происходить понижение уровня объект до уровня субъекта и осуществляться чтение. Функция перехода Z-сиегемы удовлетворяет ограничениям основной теоремы безопасности, и все состояния такой системы также являются безопасными в смысле критерия Белла - ЛаПадулы, но вместе с тем в этой системе любой пользователь сможет прочитать любой файл, что, очевидно, несовместимо с безопасностью в обычном понимании.

Следовательно, необходимо сформулировать теорему, которая бы не только констатировала безопасность всех достижимых состояний для системы, соответствующей определенным условиям, но и гарантировала бы безопасность в процессе осуществлении переходов между состояниями. Для этого необходимо регламентировать изменения уровней безопасности при переходе от состояния к состоянию с помощью дополнительных правил.

Такую интерпретацию мандатной модели осуществил Мак-Лин, предложивший свою формулировку основной теоремы безопасности, основанную не на понятии безопасного состояния, а на понятии безопасного перехода.

Функция перехода является безопасной тогда и только тогда, когда она одновременно безопасна и по чтению и по записи и когда она изменяет только один из компонентов состояния, и эти изменения не приводят к нарушению безопасности системы.

Теорема безопасности Мак-Лина. Система безопасна в любом состоянии и в процессе переходов между ними, если ее начальное состояние является безопасным, а ее функция перехода удовлетворяет критерию Мак- Лина.

Обратное утверждение неверно. Система может быть безопасной по определению Белла-ЛаПадулы, но не иметь безопасной функции перехода.

Такая формулировка основной теоремы безопасности предоставляет в распоряжение разработчиков защищенных систем базовый принцип их построения, в соответствии с которым для того, чтобы обеспечить безопасность системы как в любом состоянии, так и в процессе перехода между ними, необходимо реализовать для нее такую функцию перехода, которая соответствует указанным условиям.

4.2.11. Уполномоченные субъекты

Формулировка основной теоремы безопасности в интерпретации Мак-Лина позволяет расширить область ее применения по сравнению с классической теоремой Белла-ЛаПадулы, однако, используемый критерий безопасности перехода не всегда соответствует требованиям контроля доступа, возникающим на практике. Поскольку в процессе осуществления переходов могут изменяться уровни безопасности сущностей системы, желательно контролировать этот процесс, явным образом разрешая или запрещая субъектам осуществлять подобные переходы. Для решения этой задачи Мак-Лин расширил базовую модель путем выделения подмножества уполномоченным субъектов, которым разрешается инициировать переходы, в результате которых у сущностей системы изменяются уровни безопасности. Система с уполномоченными субъектами также описывается множествами S, O, L, смысл которых совпадает с аналогичными понятиями модели Белла-ЛаПадулы, а ее состояние также описывается набором упорядоченных пар (F,M), причем функция перехода F и матрица отношений M доступа играют ту же роль. Новым элементом модели является функция управления уровнями C: SuO > P(S) (здесь и далее P(S) обозначает множество всех подмножеств S). Эта функция определяет подмножество субъектов, которым позволено изменять уровень безопасности, для заданного объекта или субъекта. Модель системы $\sum(vo,R, T^a$ состоит из начального состояния vo, множества запросов R и функции перехода T^a, которая переводит систему из состояния в состояние по мере выполнения запросов.

С точки зрения модели уполномоченных субъектов система

$\sum(vo,R, T^a)$ считается безопасной в том случае, если:

1. Начальное состояние v_0 и все состояния, достижимые из него путем применения конечного числа запросов из R являются безопасными по критерию Белла - ЛаПадулы;

2. Функция перехода T^a является авторизованной функцией перехода согласно предложенному определению.

4.2.12. Модель совместного доступа

Практическое применение всех представленных формулировок мандатной модели безопасности ограничено еще одним фактором — они не учитывают широко распространенные в государственных учреждениях правила, согласно которым доступ к определенной информации или модификация ее уровня безопасности могут осуществляться только в результате совместных действий нескольких пользователей (т. н. групповой доступ).

Для того, чтобы мандатная модель предусматривала совместный доступ необходимо модифицировать се следующим образом. Вместо множества субъектов системы S будем рассматривать множество непустых подмножеств S, которое обозначим как $S=P(S)\backslash\{\varnothing\}$. Расширим матрицу прав доступа, отражающую текущее состояние доступа в системе, путем добавления в нее строк, содержащих права групповых субъектов, и обозначим ее как M Кроме функции уровня безопасности $F:SuO\rightarrow L$ для групповых субъектов вводятся

дополнительные функции: F^L:S→L такая, что F^L(s) есть наибольшая нижняя граница множества {F(s) / s∈S} и F^H:S→L, такая, что F^H(s) есть наименьшая верхняя граница множества{F(s) / s∈S}.

Критерии безопасности состояния для такой системы формулируются следующим образом:

1. Состояние системы является безопасным но чтению тогда и только тогда, когда для каждого индивидуального или группового субъекта, имеющего в этом состоянии доступ чтения к объекту, наибольшая нижняя граница множества уровней безопасности этого субъекта доминирует над уровнем безопасности этого объекта: ∀s∈S, ∀ o∈O, read∈M[s,o] → F^L(s)>F(o).

2. Состояние системы является безопасным по записи тогда и только тогда, когда для каждого индивидуального или группового субъекта, имеющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над наименьшей верхней границей множества уровней безопасности этого субъекта: ∀s∈S, ∀ o∈O, write ∈M[s,o]->F(o)> F^H(s).

Тогда теорема Белла-ЛаПадулы для совместного доступа формулируется следующим образом [3]:

Система∑(vo,R, T) безопасна тогда и только тогда, когда:

а) начальное состояние v_0 безопасно и

б) функция перехода T такоda, чго для любого состояния v, достижимого из v_0 путем применения конечной последовательности запросов из R, таких, что T(v,r) = v*, v=((F,F^H,F^L),M) и v*=((F*,F^{*H},F^{*L})*,M*) для каждого ∀s∈S, ∀ o∈O выполняются следующие условия:

1. если read ∈ M*[s,o] и read ∉ M[s,o], то F^L*(s)> F*(o);
2. если read ∈ M[s,o] и F^L*(s)<F*(o), то read ∉ M* [s,o];
3. если write ∈ M*[s,o] и write ∉ M[s,o], то F*(o)> F^H*(s);
4. если write ∈ M[s,o] и F*(o)<F^H*(s), то write ∉ M* [s,o].

4.2.13 Применение мандатных моделей

В завершении обзора мандатных моделей необходимо отметить трудности, которые связаны с их применением на практике. Все мандатные модели, как и модель Белла - ЛаПалулы, используют только два права доступа – чтение и запись. Па практике информационные системы поддерживают значительно более широкий спектр операций над информацией, например, создание, удаление, передачи и т. д. Следовательно, для того чтобы применить мандатную модель к реальной системе, необходимо установить подходящее соответствие между чтением и записью и операциями, реализованными в конкретной системе. Самым простым примером непрактичности мандатной модели является невозможность ее применения для сетевых взаимодействий — нельзя построить распределенную систему, в которой информация передавалась бы только в одном направлении, потому что всегда будет существовать обратный поток информации, содержащий ответы на запросы, подтверждения получения и т.д.

Поэтому, когда и системе используется мандатная политика, все взаимодействия рассматриваются только на достаточно высоком уровне абстракции, на котором не учитываются детали реализации операций доступа. Такой подход позволяет отобразить любое множество разнообразных операций доступа в обобщенные операции чтения и записи. Для оценки возможности нарушений безопасности с использованием методов, основанных на несоответствии этих абстрактных операций и реальных механизмов доступа, применяется анализ т.н. скрытых каналов утечки информации. Целью этих исследований является

выявление тех способов, с помощью которых информация может передаваться в обход правил мандатной модели.

Чем больше потоков информации мы поставим под контроль мандатной модели, тем менее гибкой будет наша система, но и тем меньше потоков информации придется исследовать в процессе анализа скрытых каналов.

В заключение обзора мандатной модели управления доступом необходимо отметить, что хотя она является базовой моделью безопасности, составляющей основу теории зашиты информации, однако ее применение на практике связано с серьезными трудностями: Поэтому в реальной жизни она используется только в системах, обрабатывающих классифицированную информацию, и применяется только в отношении ограниченного подмножества субъектов и объектов.

4.2.14. Ролевая политика безопасности

Ролевая политика безопасности представляет собой существенно усовершенствованную модель Харрисона–Руззо-Ульмана, однако ее нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов. Поэтому ролевая модель представляет собой совершенно особый тип политики, основанной на компромиссе между гибкостью управления доступом, характерной для дискреционных моделей, и жесткостью правил контроля доступа, присущей мандатным моделям.

В ролевой модели классическое понятие субъект замещается понятиями пользователь и роль. Пользователь -— это человек, работающий с системой и выполняющим определенные служебные обязанности. Роль — это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логически связанный набор полномочий, необходимых для осуществления, определенной деятельности. Самым распространенным примером роли является присутствующий почти в каждой системе административный бюджет (например root для UNIX и Administrator для Windows NT), который обладает специальными полномочиями и может использоваться несколькими пользователями.

Ролевая политика распространена очень широко, потому что она, в отличие от других более строгих и формальных политик, очень близка к «реальной жизни». Ведь на самом деле работающие в системе пользователи действуют не от своего личного имени они всегда осуществляют определенные служебные обязанности, т.е. выполняют некоторые роли, которые никак не связаны с их личностью.

Поэтому вполне логично осуществлять управление доступом и назначать полномочия не реальным пользователям, а абстрактным (не персонифицированным) ролям, представляющим участников определенного процесса обработки информации. Такой подход к политике безопасности позволяет учесть разделение обязанностей и полномочий между участниками прикладного информационного процесса, т. к. с точки зрения ролевой политики имеет значение не личность пользователя, осуществляющего доступ к информации, а то, какие полномочия ему необходимы для выполнения его служебных обязанностей. Например, в реальной системе обработки информации могут работать системный администратор, менеджер баз данных и простые пользователи.

В такой ситуации ролевая политика позволяет распределить полномочия между этими ролями и соответствии с их служебными обязанностями: роли администратора назначаются специальные полномочия, позволяющие ему контролировать работу системы и управлять ее конфигурацией, роль менеджера баз данных позволяет осуществлять

управление сервером БД, а права простых пользователей ограничиваются минимумом, необходимым для запуска прикладных программ. Кроме того, количество ролей в системе может не соответствовать количеству реальных пользователей — один пользователь, если на нем лежат различные обязанности, требующие различных полномочий, может выполнять (одновременно или последовательно) несколько ролей, а несколько пользователей могут пользоваться одной и тон же ролью, если они выполняют одинаковую работу .

При использовании ролевой политики управление доступом осуществляется в две стадии:, во-первых, для каждой роли указывается набор полномочий, представляющий набор прав доступа к объектам, и, во-вторых, каждому пользователю назначается список доступных ему ролей. Полномочия назначаются ролям в соответствии с принципом наименьших привилегий, из которого следует, что каждый пользователь должен обладать только минимально необходимым для выполнения своей работы набором полномочий.

Ролевая модель описывает систему в виде следующих множеств [3]:

- U - множество пользователей;
- R - множество ролей;
- P - множество полномочий на доступ к объектам, представленное, например, и виде матрицы прав доступа;
- S - множество сеансов работ пользователей с системой.

Для перечисленных множеств определяются следующие отношения (рис. 4.6.):

$PA \subseteq PxR$ - отображает множество полномочии на множество ролей, устанавливая для каждой роли набор присвоенных ей полномочий;

$UA \subseteq UxR$ - отображает множество пользователей на множество ролей, определяя для каждого пользователя набор доступных ему ролей.

Правила управления доступом ролевой политики безопасности определяются следующими функциями:

user: $S \rightarrow U$ - для каждого сеанса S эта функция определяет пользователя, который осуществляет этот сеанс работы с системой: **user(s) = u**

roles : $S \rightarrow P(R)$ - lля каждого сеанса S эта функция определяет набор ролей из множества R которые могут быть одновременно доступны пользователю в этом сеансе: **roles(s)={r_i | (user(s), r_i) $\in$UA};**

permissions : $S \rightarrow P$ - для каждого сеанса S эта функция задает набор доступных в нем полномочии, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе: permissions(s) = $U_{r \in roles(s)}${Pi, (Pi, r)$\in$PA)

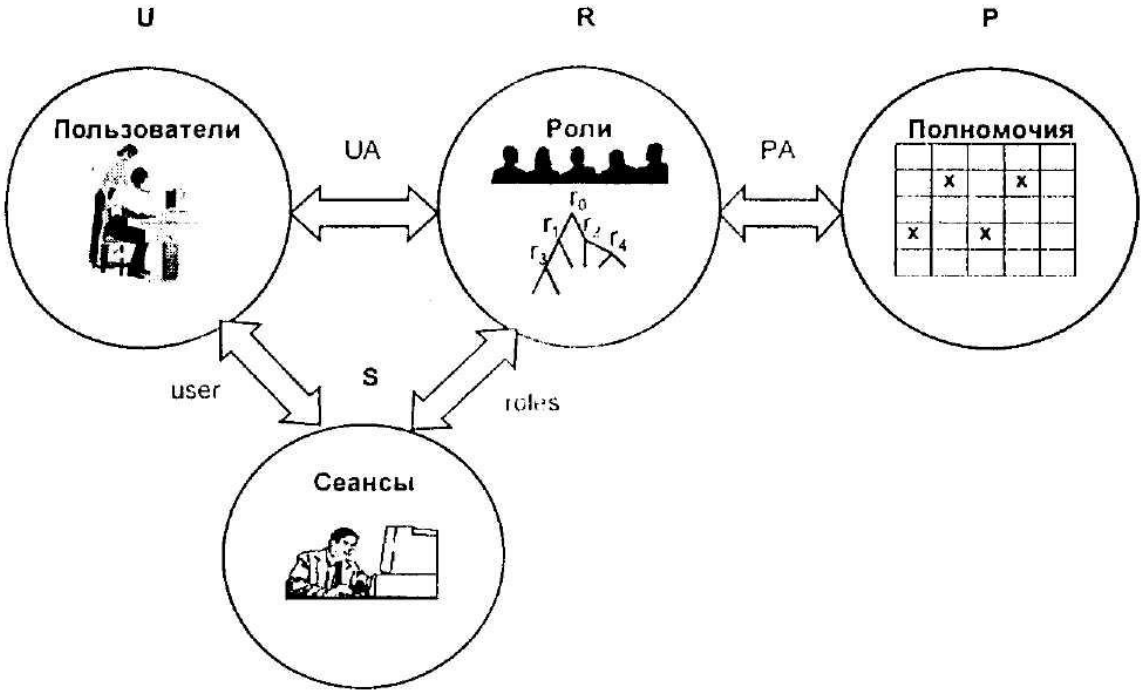


Рис.4.6. Ролевая модель управления доступом.

В качестве критерия безопасности ролевой модели используется следующее правило: *система считается безопасной, если любой пользователь системы, работающий в сеансе S, может осуществлять действия, требующие полномочия p только в том случае, если* **p ∈ permissions(s)**.

Из формулировки критерия безопасности ролевой модели следует, что управление доступом осуществляется главным образом не с помощью назначения полномочий ролям, а путем задания отношения UA, назначающего роли пользователям, и функции **roles,** определяющей доступный в сеансе набор ролей. Поэтому многочисленные интерпретации ролевой модели различаются видом функции **user**, **roles** и **permission,** а также ограничениями, накладываемыми на отношения PA и UA. В качестве примеров рассмотрим ролевую политику управления доступом с иерархической организацией ролей, а также несколько наиболее часто встречающихся типовых ограничений на отношения **PA** и **UA** и **функции user** и **roles.**

Иерархическая организация ролей представляет собой наиболее распространенный тип ролевой модели поскольку она очень точно отражает установившееся в реальном мире отношение подчиненности между участниками процессом обработки информации и разделение между ними сфер ответственности. Роли в иерархии упорядочиваются по уровню предоставляемых полномочий. Чем выше роль находится в иерархии, тем больше с ней связано полномочий, поскольку считается, что если пользователю присвоена некоторая роль, то ему автоматически назначаются и все подчиненные ей по иерархии роли. Иерархия ролей допускает множественное наследование.

Каждому пользователю назначается некоторое подмножество иерархии ролей, а в каждом сеансе доступна совокупность полномочий ролей, составляющих фрагмент этой иерархии. Такой подход позволяет существенно упростить управление доступом за счет неявного назначения полномочий, поскольку в реальной жизни, как правило, пользователи жестко упорядочены по степени ответственности, соответствующей уровню полномочий, которыми они обладают. Причем, более доверенные пользователи, стоящие па служебной лестнице выше, всегда обладают всеми полномочиями менее доверенных, подчиненным им. Иерархия ролей в точности отражает эту ситуацию.

Другие реализации ролевой политики безопасности также связаны с введением различных ограничений на отношения **PA, UA, и функции user, roles и permissions.** Главным для этих ограничений является то, что все они отражают специфику распределения полномочий и сфер ответственности между участниками различных процессов обработки информации. Рассмотрим несколько примеров, демонстрирующих богатые возможности применения ролевой модели управления доступом:

1. Взаимоисключающие роли. Множество ролей разбивается на подмножества, объединяющие роли, которые не могут быть назначены пользователю одновременно и считают несовместимыми. Таким образом пользователю может быть назначено только по одной роли из каждого подмножества несовместимых ролей.)

Взаимоисключающие роли реализуют, т. н. статическое разделение обязанностей, когда конфликт несовместимости полномочий разрешается на стадии назначения ролей. Такая политика хорошо подходит для системы обработки информации, в которой пользователям запрещается совмещать определенные обязанности. Например, в банковской системе одному и тому же пользователю не могут быть одновременно назначены роли оператора, отвечающего за выполнение определенных операций, и аудитора, осуществляющего контроль за их выполнением.

2. Ограничения на одновременное использование ролей в рамках одной сессии. В этом случае множество ролен также разбивается на подмножества несовместимых ролей, но отношение UA может назначить пользователю любую комбинацию ролен. Однако в ходе сеанса работы с системой пользователь может одновременно активировать не более одной роли из каждого подмножества несовместимых ролей.

Поскольку в процессе сеанса пользователь может переключаться между различными ролями, он должен при этом избегать конфликтов несовместимости между ними, эта политика получила название динамического разделения обязанностей. Такая политика является более гибкой по сравнению со статическим разделением обязанностей, поскольку позволяет реализовать более сложные схемы контроля доступа. В частности она позволяет запретить пользователю, обладающему значительным набором ролей и полномочий, пользоваться ими всеми одновременно. В определенных ситуациях это позволяет защититься от атаки «троянского коня» — например, пользователю можно запретить одновременно осуществлять доступ к ценной информации и запускать «недоверенные» программы, внесенные в систему другими пользователями. Правильно подобранные ограничения на одновременное использование ролей позволяют реализовать контроль за информационными потоками, что вообще - то характерно для мандатных моделей безопасности.

3. Количественные ограничения при назначении ролей и полномочий. Эта модель предназначена для тех случаев, когда роль может быть назначена только ограниченному числу пользователей, и/или предоставление некоторых полномочии допускается только для ограниченного числа ролей.

Смысл данных условий состоит и том, что благодаря ограничению количества пользователей, осуществляющих те или иные операции, сужается круг лиц, на которых лежит ответственность за совершение соответствующих действий. Например, в системе не должно быть более одного администратора, или, скажем, право уничтожать документы может быть назначено только одной роли.

4. Группирование ролей и полномочий. Роли и полномочия, которые дополняют друг друга, и назначение которых по отдельности не имеет смысла, объединяются в группы, которые могут быть назначены только целиком. Для этого вводятся дополнительные правила, в соответствии с которыми любая роль может быть назначена пользователю только в том случае, если ему уже присвоен определенный набор ролен, а роль может быть наделена полномочием только тогда, когда с ней уже связан определенный набор полномочии.

Введение подобных ограничений упрощает администрирование системы в тех случаях, когда полномочия должны предоставляться определенным набором, или когда назначение ролей должно производится в определенной последовательности. Например, предоставлять доступ к некоторым объектам (скажем личным каталогам) имеет смысл только сразу и по чтению и по записи. Типичным примером группирования ролей является ситуация, когда некоторый пользователь, осуществляющий руководство работой других пользователей, должен обладать полномочиями, равными совокупности полномочий всех своих подчиненных, т.е. роль руководителя образует одну группу с ролями исполнителей. Следует отметить, что иерархия ролей является частным случаем группирования ролей и полномочий.

Поскольку все перечисленные варианты ограничений, а также любые другие могут использоваться в различных комбинациях, ролевая модель очень легко адаптируется для каждого конкретного случая, что является ее основным преимуществом перед другими моделями. Ролевая политика предоставляет широкий простор для разработчиков систем управления доступом, - с одной стороны, использование матрицы прав доступа может превратить ее в разновидность дискреционной модели, но, с другой с троны, применение жестких правил распределения ролей между сеансами и пользователями, а также полномочий между ролями, позволяет построить на ее основе полноценную нормативную политику. Следовательно, свойства системы, построенной в соответствии с ролевой моделью, определяются исключительно характером используемых ограничений и могут находиться в очень широком диапазоне, что не позволяет провести формальное доказательство безопасности модели для общего случая.

Подводя итоги свойств ролевой политики управления доступом, следует констатировать, что в отличие от других политик она практически не гарантирует безопасность с помощью формального доказательства, а только определяет характер ограничений, соблюдение которых и служит критерием безопасности системы. Такой подход позволяет получать простые и понятные правила контроля доступа, которые легко могут быть применены на практике, но лишает систему доказательной теоретической базы. В некоторых ситуациях это обстоятельство затрудняет использование ролевой политики, однако, в любом случае, оперировать ролями гораздо удобнее, чем субъектами, поскольку это более соответствует распространенным технологиям обработки информации, предусматривающим разделение обязанностей и сфер ответственности между пользователями. Кроме того, ролевая политика может использоваться одновременно с другими политиками безопасности, когда полномочия ролей, назначаемых пользователям, контролируются дискреционной или мандатной политикой, что позволяет строить многоуровневые схемы контроля доступа.

4.2.15. Вероятностные модели

Модели этого типа исследуют вероятность преодоления системы защиты за определенное время. Достоинство моделей – числовая оценка стойкости системы защиты, недостаток – изначальное допущение того, что система может быть вскрыта.

Задача модели – минимизация преодоления системы защиты.

Игровая модель

Модель строится по следующему принципу. Разработчик создает первоначальный вариант системы защиты. После это злоумышленник начинает его преодолевать. Если к моменту времени Т, в который злоумышленник преодолел систему защиты, у разработчика не будет нового варианта система защиты – преодолена. Если нет, то процесс продолжается. Т. е. Модель описывает процесс эволюции системы защиты в течении времени.

Модель системы безопасности с полным перекрытием

В данной модели точно определяется каждая область, требующая защиты, оцениваются средства обеспечения безопасности, их эффективность и вклад в обеспечение безопасности во всей вычислительной системе. С каждым объектом O, требующим защиты, связывается некоторое множество действий, к которым может прибегать злоумышленник для получения несанкционированного доступа к объекту. Основной характеристикой набора угроз T является вероятность появления каждого из злоумышленных действий. В реальной системе эти вероятности можно вычислить с ограниченной степенью точности.

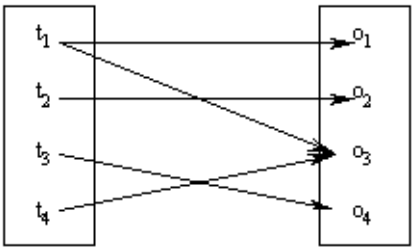


Рис. 4.7. Множество отношений объект-угроза

Множество отношений объект-угроза образуют двухдольный граф, в котором ребро <ti oj> существует тогда и только тогда, когда ti ($\forall ti \in T$) является средством получения доступа к объекту oi ($\forall oi \in O$). Связь между объектами и угрозами типа "один ко многим", т.е. одна угроза может распространяться на любое число объектов и объект может быть уязвим со стороны более чем одной угрозы. Цель защиты состоит в том, чтобы перекрыть каждое ребро графа и воздвигнуть барьер для доступа по этому пути.

Завершает модель третий набор, включающий средства безопасности M, которые используются для защиты информации в вычислительной системе. Идеально каждое mk ($\forall mk \in M$) должно устранять некоторое ребро <ti oj> из графа на рисунке. Набор M средств обеспечения безопасности преобразует двухдольный граф в трехдольный граф. В защищенной системе все ребра представляются в виде <ti mk> и <mk oj>. Любое ребро в форме <ti oj> определяет незащищенный объект. Одно и то же средство обеспечения безопасности может перекрывать более одной угрозы и (или) защищать более одного объекта. Отсутствие ребра <ti oj> не гарантирует полного обеспечения безопасности (хотя наличие такого ребра дает потенциальную возможность несанкционированного доступа за исключением случая, когда вероятность появления ti равна нулю).

Понятие системы с полным перекрытием

Система с полным перекрытием – система в которой имеются средства защиты на каждый путь проникновения [1].

Пусть:

T – набор угроз;

O – набор защищаемых объектов;

M – набор средств обеспечения безопасности;

V – набор уязвимых мест – отображение $T \times O$ на набор упорядоченных пар $V = \{t_i, O\}_i$, представляющих собой пути проникновения в систему;

B – набор барьеров – отображение $T \times O \times M$ или $V \times M$ на набор упорядоченных троек $\{t_i\ o_j\ m_k\}$, представляющих собой точки, в которых требуется осуществить защиту**.**

Если $\{t_i\ o_j\} \in$ V предусматривает $\{t_i\ o_j\ m_k\} \in$ B , то j [ий] объект защищен.

Основное преимущество данного типа моделей состоит в возможности численного получения оценки степени надежности системы защиты информации. Данный метод не

специфицирует непосредственно модель системы защиты информации, а может использоваться только в сочетании с другими типами моделей систем защиты информации.

4.2.16. Информационные модели

Потоковые модели определяют ограничения на отношение ввода/вывода системы, которые достаточны для реализации системы. Данные модели являются результатом применения шенноновской теории информации к проблеме безопасности систем. К данным моделям относятся модели невмешательства и невыводимости.

Модель невмешательства

Невмешательство – ограничение, при котором ввод высокоуровнего пользователя не может смешиваться с выходом низкоуровнего пользователя. Модель невмешательства рассматривает систему, как состоящую из четырех объектов: высокий ввод, низкий ввод, высокий вывод, низкий вывод.

Рассмотрим систему, вывод которой пользователю u определен функцией out(u, hist.read(u)), где hist.read(u) – история ввода системы (traces), чей последний ввод был read(u) - команда чтения, исполненная пользователем u. Безопасность определена в терминах очищения (purge) историй ввода, где purge удаляет команды, исполненные пользователем, чей уровень безопасности не доминирует над уровнем безопасности u.

Для определенных систем, модель невмешательства особенно хороша в том, что если последовательность входа X не смешивается с последовательностью вывода У, и X независима от ввода других пользователей, то I(X, У)=0, где I(X, У) — взаимная для X и У информация.

Модель невыводимости

Модель невыводимости выражается в терминах пользователей и информации, связанных с одним из двух возможных уровней секретности (высокий и низкий).

Система считается невыводимо безопасной, если пользователи с низким уровнем безопасности не могут получить информацию с высоким уровнем безопасности в результате любых действий пользователей с высоким уровнем безопасности. Т.е. утечка информации не может произойти в результате посылки высокоуровневыми пользователями низкоуровневым пользователям высокоуровневой информации.

Такое определение предусматривает неспособность низкоуровневых пользователей к использованию доступной им информации для получения высокоуровневой информации, но не защищает высокоуровневых пользователей от просмотра низкоуровневыми пользователями. Оно просто требует, чтобы низкоуровневые пользователи не были способны использовать доступную им информацию для получения высокоуровневой информации.

4.3 Модели контроля целостности

4.3.1. Модель Биба

Мандатная модель целостности Биба

Данную модель часто называют инверсией модели Бела – Лападула и следовательно основные правила этой модели просто переворачивают правила модели Бела – Лападула: NRU→ «нет чтения снизу(NRD)» и NRD→ «нет записи наверх(NWU)».

Правило NRD определяется как запрет субъектами на чтение информации из объекта с более низким уровнем целостности. Правило NWUопределяется как запрет субъектам на запись информации в объект с более высоким уровнем целостности.

Одним из преимуществ этой модели является то, что она унаследовала многие важные характеристики БЛМ, включая ее простоту и интуитивность. Это значит, что проектировщики реальных систем могут легко понять суть этих правил и использовать их для принятия решений при проектировании. Кроме того, поскольку мандатная модель целостности Биба, подобно БЛМ, основана на простой иерархии, ее легко объяснить и изобразить пользователям системы.

С другой стороны, модель представляет собой очевидное противоречие с правилами NRU и NWD. Это значит, что если необходимо построить систему, которая предотвращает угрозы, как секретности, так и целостности, то одновременное использование правил моделей БЛМ и Биба может привести к ситуации, в которой уровни безопасности и целостности будут использоваться противоположными способами.

Модель понижения уровня субъекта

Вторая модель Биба заключается в небольшом ослаблении правила чтения снизу.

Здесь субъекту разрешается осуществлять чтение снизу, но в результате такого чтения уровень целостности субъекта понижается до уровня целостности объекта. В этой модели, не накладывается ни каких ограничений на то, что может прочитать субъект, и она подразумевает монотонное изменение уровней целостности.

Модель понижения уровня объекта

Последняя модель Биба реализуется в ослаблении правила записи наверх. Модель разрешает совершать запись наверх, но в результате, уровень целостности объекта понижается до уровня целостности субъекта, осуществляющего запись. В этой модели также, не накладывается ни каких ограничений на то, что может прочитать или записать субъект, она также подразумевает монотонное изменение уровней целостности и не содержит ни каких механизмов для повышения уровня целостности объекта.

В практическом применении модель Биба слишком сильно полагается на понятие доверенных процессов. То есть, проблема необходимости создания доверенных процессов для повышения или понижения целостности субъектов или объектов является весьма существенной. Следует отметить тот факт, что данная модель не предусматривает механизмов повышения целостности, что ведет к монотонному снижению целостности системы.

4.3.2. Модель Кларка–Вилсона

Эта модель была создана в 1987г Кларком и Вилсоном. Ее созданию способствовал анализ методов управления коммерческими организациями целостностью своих бумажных ресурсов в неавтоматизированном офисе.

Введем некоторые обозначения:

D – конечное множество данных;

CDI – ограниченные элементы данных;

UDI – неограниченные элементы данных,

Причем: $D = CDI \cup UDI$, $CDI \cap UDI = \varnothing$.

Субъекты включены в модель как множество компонент, инициирующие процедуры преобразования (ПП) – любые ненулевые последовательности элементарных действий (элементарное действие - переход состояния, вызывающий изменения некоторых элементов

данных). ПП могут быть представлены в виде функции, ставящих в соответствие субъект и элемент данных с новым элементом данных следующим образом: ПП: субъекты xD →D.

ПП – действия, которые выполняют субъекты (способные изменить определенные данные) над данными.

У данной модели, как и у других моделей, существуют свои правила. Рассмотрим их.

Правило1: в системе должны иметься процедуры утверждения целостности (IVP (Пример-проверка контрольной суммы) – утверждают, что данный CDI имеет надлежащий уровень целостности, утверждающие любой CDI.

Правило2: применение любого ПП к любому CDI должно сохранять целостность CDI.

Правило3: только ПП может вносить изменения в CDI.

Правило4: субъекты могут инициировать только определенные ПП над определенными CDI.

Правило5: соответствующая политика в отношении разделения обязанностей субъектов. Т.е. компьютерная система определяет такую политику, чтобы не позволить субъектам изменять CDI без соответствующего вовлечения других субъектов.

Правило 6: некоторые специальные ТР могут превращать UDI в CDI.

Это правило позволяет определенным ПП получать на вход UDI и после соответствующего повышения целостности выдавать на выходе CDI.

Правило 7: каждое применение CDI должно регистрироваться в специальном CDI, в который может производиться только добавление информации, достаточной для восстановления картины о процессе работы этого CDI. Т.е. применение специального регистрационного журнала.

Правило 8: система должна распознавать субъекты, пытающая инициализировать ПП.

Это правило определяет механизмы предотвращения атак, при которых один субъект пытается выдать себя за другого.

Правило 9: система должна разрешать производить изменения в списках авторизации только специальным субъектам.

Данные правила определяют как может быть проверена целостность как и кем могут изменятся CDI, и как UDI могут быть превращены вCDI. Т.е. здесь происходит отслеживание всех изменений и тех, кто пытается внести эти изменения.

Преимущество модели в том, что она основана на проверенных временем бизнес – методов обращении с бумажными ресурсами. Недостатком является трудность реализации VIP и методов предотвращения CDI от искажения целостности.

Основным преимуществом данной модели является то, что она основана на проверенных временем бизнес методах обращения с бумажными ресурсами. Поэтому ее не следует рассматривать как академическое исследование, а скорее как комплекс существующих методов. Модель Кларка–Вилсона также предоставляет исследователям методы работы с целостностью, отличные от традиционных уровне - ориентированных подходов, таких как модели Белла–Лападула и Биба.

Основным недостатком модели является то, что IVP и методы предотвращения CDI от искажения целостности нелегко реализовать в реальных компьютерных системах.

4.4. Механизм защиты от угрозы отказа в обслуживании

4.4.1. Мандатная модель

Мандатная модель включает в себя многие характеристики моделей Белла–Лападула и Биба.

Субъектам системы соответствуют приоритеты, которые могут быть одинаковы, ниже или выше по сравнению с приоритетом любого другого субъекта. Объектам соответствуют степени критичности, имеющие аналогичную иерархическую структуру. Субъект может

требовать услугу у вычислительной системы, запрашивая доступ к объектам системы. Говорят, что субъект получает отказ в обслуживании, если его запрос зарегистрирован, но не удовлетворен в течение соответствующего MWT (максимальное время ожидания).

Рассмотрим правила, описывающие эту модель.

1. Правило «никаких отказов вверх» (NDU): ни каким объектам с более низким приоритетом не позволено отказывать в обслуживании субъектам с более высокими приоритетами. Но некоторым субъектам с более высоким приоритетом (например администратору) должна предоставляться возможность отказывать в обслуживании объектам с более низким приоритетом, если первые того желают.

2. Правило NDU(C) – обобщение NDU: субъекты с более низким приоритетом не должны препятствовать запросам услуг субъектов с более высокими приоритетами, производимых через объекты из конкретного множества C. Услуги, предоставляемые для объектов, находящихся в C, никогда не должны устаревать.

Главное преимущество этих правил – введение понятия приоритета. Недостаток – эти правила имеют смысл для систем с несколькими приоритетами.

4.4.2. Модель Миллена – модель распределения ресурсов

В основе модели лежит идея о том, что для выполнения нужного задания субъектам необходимы определенные временные и пространственные требования к ресурсам. Отказ происходит только в том случае, если распределение пространства и времени для некоторого процесса не отвечает соответствующим требованиям.

Введем некоторые обозначения:

P - множество активных процессов;

R - множество пассивных ресурсов;

C – некоторая фиксированная граница (обозначает максимальное число единиц для всех типов ресурсов);

A_p – вектор распределения – число единиц ресурса, выделенных для процесса p в некотором состоянии;

CPU – ресурс, используемый для формирования информации о том является ли процесс текущим или застывшим. Если $A_p(CPU) = 1$, то истинным является running(p), если $A_p(CPU) = 0$, то - asleep(p);

S_{Qp} – вектор пространственных требований - число единиц каждого ресурса, выделенных процессом p для выполнения необходимого задания в некотором состоянии;

T(p) – функция, показывающая когда в последний раз изменились часы для процесса, с целью отражения реального времени;

$^{T}Q_p$ - вектор временных требований – объем времени, необходимого каждому ресурсу процесса p для выполнения работы.

Далее представим восемь правил, необходимых для описания модели.

1. Сумма единиц выделенных ресурсов для всех процессов из P должна быть меньше системной границы C, т.е. $S\ A_p \le C$.

2. Текущие процессы должны иметь нулевые пространственные требования, т.е.

If running(p) then $^{S}Q_p = 0$.

3. В некотором состоянии процесс является текущим и остается текущим и в следующем состоянии, т. е. If running(p) and running$(p)^1$ then $A_p{}^1 = A_p$.

4. Часы процесса изменяются только с изменением CPU, т.е. if $A_p\ (CPU)^1 = A_p\ (CPU)$, then $T(p)^1 = T(p)$.

5. Часы процесса изменяются только для того, чтобы отразить увеличение во времени, т. е. if $A_p\ (CPU)^1 \neq A_p\ (CPU)$ then $T(p)^1 > T(p)$.

6. Пространственные требования устанавливаются для застывших процессов, т.е. if asleep(p) then $^{S}Q_p{}^1 = {}^{S}Q_p + A_p - A_p{}^1$.

7. Временные требования для застывших процессов не устанавливаются, т.е. if asleep(p) then ${}^{T}Q_p{}^{1} = {}^{T}Q_p$.

8. Переходы в результате которых процесс останавливается, перераспределяют только ресурсы CPU, т.е. If running(p) and asleep $(p)^1$ then $A_p{}^1 = A_p$ - CPU.

5. Основные критерии защищенности АС. Классы защищенности

5.1. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»)

"Критерии оценки безопасности компьютерных систем" (Trusted Computer System Evaluation Criteria - TCSEC) [8], получившие неформальное "Оранжевая книга" (по цвету обложки первоначального издания), были разработаны и опубликованы Министерством обороны США в 1983г. с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному программному и информационному обеспечению компьютерных систем, и выработки методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах в основном военного назначения.

"Оранжевая книга" поясняет понятие безопасной системы, которая управляет, посредством соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию. Очевидно, однако, что абсолютно безопасных систем не существует, что это абстракция. Любую систему можно "взломать", если располагать достаточно большими материальными и временными ресурсами. Есть смысл оценивать лишь степень доверия, которое разумно оказать той или иной системе

Общая структура требований TCSEC

В «Оранжевой книге» предложены три категории требований безопасности: политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних - на качество средств защиты. Рассмотрим эти требования подробнее.

Политика безопасности

Требование 1. *Политика безопасности.* Система должна поддерживать точно определенную политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом. Там, где это необходимо, должна использоваться политика мандатного управления доступом, позволяющая эффективно реализовать разграничение доступа к информации различного уровня конфиденциальности.

Требование 2. *Метки.* С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля доступа. Для реализации мандатного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и режимы доступа к этому объекту.

Подотчетность

Требование 3. *Идентификация и аутентификация.* Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

Требование 4. *Регистрация и учет.* Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе (т.е. должен существовать объект компьютерной системы, потоки от которого и к которому доступны только субъекту администрирования). Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

Гарантии (корректность)

Требование 5. *Контроль корректности функционирования средств защиты*. Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

Требование 6. *Непрерывность защиты*. Все средства защиты (в том числе и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одной из ключевых аксиом, используемых для формального доказательства безопасности системы.

Классы защищенности компьютерных систем по TCSEC

«Оранжевая книга» предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа А). Каждая группа включает один или несколько классов. Группы D и А содержат по одному классу (классы D и А соответственно), группа С - классы С1, С2, а группа В три класса - В1, В2, В3, характеризующиеся различными наборами требований защищенности. Уровень защищенности возрастает от группы D к группе А, а внутри группы - с увеличением номера класса. Таким образом имеем всего шесть классов безопасности - С1, С2, Bl, В2, В3, А1. Усиление требований осуществляется с постепенным смещением акцентов от положений, определяющих наличие в системе каких-то определенных механизмов защиты, к положениям обеспечивающих высокий уровень гарантий того, что система функционирует в соответствии требованиям политики безопасности.

Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять приводимым ниже требованиям. Поскольку при переходе к каждому следующему классу требования только добавляются, мы будем выписывать лишь то новое, что присуще данному классу, группируя требования в согласии с предшествующим изложением.

Группа D. Минимальная защита

Класс D. Минимальная защита. Класс D зарезервирован для тех систем, которые были представлены на сертификацию (оценку), но по какой-либо причине ее не прошли.

Группа C. Дискреционная защита

Группа C характеризуется наличием дискреционного управления доступом и аудитом действий субъектов.

Класс C1. Системы на основе дискреционного разграничения доступа. TCB (доверительная база вычислений) систем, соответствующих этому классу защиты, удовлетворяет неким минимальным требованиям безопасного разделения пользователей и данных. Она определяет некоторые формы разграничения доступа на индивидуальной основе, т.е. пользователь должен иметь возможность защитить свою информацию от ее случайного чтения или уничтожения. Пользователи могут обрабатывать данные как по отдельности, так и от имени группы пользователей.

*Политика безопасности***.** Надежная вычислительная база должна управлять доступом именованных пользователей к именованным объектам. Механизм управления (права для владельца/группы/прочих, списки управления доступом) должен позволять пользователям специфицировать разделение файлов между индивидами и/или группами.

Подотчетность. Пользователь должен идентифицировать себя, прежде чем выполнять какие – либо действия, контролируемые надежной вычислительной базой. Для аутентификации должен использоваться какой – либо защитный механизм, например, пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа.

*Гарантии***.** Надежная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы. Ресурсы, контролируемые базой, могут составлять определенное подмножество всех субъектов и объектов системы. Защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты надежной вычислительной базы.

Документация:

- Руководство пользователя по средствам безопасности: отдельный фрагмент документации (глава, том) должен описывать защитные механизмы, предоставляемые надежной вычислительной базой, и их взаимодействие между собой, содержать рекомендации по их использованию.
- Руководство администратора по средствам безопасности: руководство должно содержать сведения о функциях и привилегиях, которыми управляет системный администратор посредством механизмов безопасности.
- Тестовая документация: разработчик системы должен представить экспертному совету документ, содержащий план тестов, процедуры прогона тестов и результаты тестов.
- Описание архитектуры: должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации надежной вычислительной базы. Если база состоит из нескольких модулей, должен быть описан интерфейс между ними.

Класс С2. Системы, построенные на основе управляемого дискреционного разграничения доступа.

Системы, сертифицированные по данному классу, должны удовлетворять всем требованиям, изложенным в классе С1. Однако, системы класса С2 поддерживают более тонкую, чем в классе С1, политику дискреционного разграничения доступа, делающую пользователя индивидуально ответственным за свои действия после процедуры аутентификации в системе, а также аудит событий, связанных с безопасностью системы.

Политика безопасности. В дополнение к С1, права доступа должны гранулироваться с точностью до пользователя. Механизм управления должен ограничивать распространение прав доступа - только авторизованный пользователь (например, владелец объекта) может предоставлять права доступа другим пользователям. Все объекты должны подвергаться контролю доступа. При выделении хранимого объекта из пула ресурсов надежной вычислительной базы необходимо ликвидировать все следы предыдущих использований.

Подотчетность. В дополнение к С1, каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем.

Надежная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой. Должна быть возможность регистрации следующих событий:

- использование механизма идентификации и аутентификации,
- внесение объектов в адресное пространство пользователя (например, открытие файла, запуск программы);
- удаление объектов;
- действия системных операторов, системных администраторов, администраторов безопасности;
- другие события, затрагивающие информационную безопасность.

Каждая регистрационная запись должна включать следующие поля:

- дата и время события;
- идентификатор пользователя;
- тип события;
- результат действия (успех или неудача).

Для событий идентификации/аутентификации регистрируется также идентификатор устройства (например, терминала). Для действий с объектами регистрируются имена объектов. Системный администратор может выбирать набор регистрируемых событий для каждого пользователя.

Гарантии. В дополнение к С1, надежная вычислительная база должна изолировать защищаемые ресурсы в той мере, как это диктуется требованиями контроля доступа и подотчетности. Тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов **и** защиты регистрационной информации.

*Документация***.** Руководство администратора по средствам безопасности в дополнение к С1, должны описываться процедуры обработки регистрационной информации и управления файлами с такой информацией, а также структура записей для каждого типа регистрируемых событий.

Группа В. Мандатное управление доступом

Основные требования этой группы - мандатное (полномочное) управление доступом с использованием меток безопасности, реализация некоторой формальной модели политики безопасности, а также наличие спецификаций на функции ТСВ. В системах этой группы постепенно к классу В3 должен быть реализован монитор ссылок (или МБО), который должен контролировать все доступы субъектов к объектам системы.

Класс B1. Системы класса B1 должны удовлетворять требованиям класса C2. Кроме того, должны быть выполнены следующие дополнительные требования.

Политика безопасности. Надежная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом. Метки являются основой функционирования механизма принудительного управления доступом. При импорте непомеченной информации соответствующий уровень секретности должен запрашиваться у авторизованного пользователя и все такие действия следует протоколировать.

Метки должны адекватно отражать уровни секретности субъектов и объектов. При экспорте информации метки должны преобразовываться в точное и однозначно трактуемое внешнее представление, сопровождающее данные. Каждое устройство ввода/вывода (в том числе коммуникационный канал) должно трактоваться как одноуровневое или многоуровневое. Все изменения трактовки и ассоциированных уровней секретности должны протоколироваться.

Надежная вычислительная база должна обеспечить проведение в жизнь принудительного управления доступом всех субъектов ко всем хранимым объектам. Субъектам и объектам должны быть присвоены метки безопасности, являющиеся комбинацией упорядоченных уровней секретности, а также категорий. Метки являются основой принудительного управления доступом. Надежная вычислительная база должна поддерживать, по крайней мере, два уровня секретности. Субъект может читать объект, если его (субъекта) метка безопасности доминирует над меткой безопасности объекта, то есть уровень секретности субъекта не меньше уровня секретности объекта и все категории объекта входят в метку безопасности субъекта. Субъект может писать в объект, если метка безопасности объекта доминирует над меткой субъекта. Надежная вычислительная база должна контролировать идентификационную и аутентификационную информацию. При создании новых субъектов (например, процессов) их метки безопасности не должны доминировать над меткой породившего их пользователя.

Подотчетность. В дополнение к C2, надежная вычислительная база должна поддерживать метки безопасности пользователей, должны регистрироваться операции выдачи на печать и ассоциированные внешние представления меток безопасности. При операциях с объектами, помимо имен, регистрируются их метки безопасности. Набор регистрируемых событий может различаться в зависимости от уровня секретности объектов.

Гарантии. В дополнение к C2, надежная вычислительная база должна обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств. Группа специалистов, полностью понимающих конкретную реализацию надежной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию. Цель должна состоять в выявлении всех дефектов архитектуры и реализации, позволяющих субъекту без должной авторизации читать, изменять, удалять информацию или приводить базу в состояние, когда она перестает обслуживать запросы других субъектов Все выявленные недостатки должны быть исправлены или нейтрализованы, после чего база подвергается повторному тестированию, чтобы убедиться в отсутствии старых или новых недостатков. Должна существовать неформальная или формальная модель политики безопасности, поддерживаемой надежной вычислительной базой. Модель должна соответствовать основным посылкам политики безопасности на протяжении всего жизненного цикла системы.

Документация. Руководство администратора по средствам безопасности в дополнение к C2 должно описывать функции оператора и администратора, затрагивающие безопасность, в том числе действия по изменению характеристик пользователей. Должны быть представлены рекомендации по взаимодействию друг с другом, по безопасной генерации новых версий надежной вычислительной базы.

Должно быть представлено неформальное или формальное описание модели политики безопасности, проводимой в жизнь надежной вычислительной базой. Необходимо наличие аргументов в пользу достаточности избранной модели для реализации политики безопасности. Должны быть описаны защитные механизмы базы и их место в модели.

Класс B2. Структурированная защита. Выполняются все требования класса защиты B1. Кроме того, в системах класса B2 ТСВ основывается на четко определенной и хорошо документированной формальной модели политики безопасности, требующей, чтобы мандатная и дискреционная системы разграничения доступа были распространены на все субъекты и объекты компьютерной системы. ТСВ должна быть четко структурирована на элементы, критичные с точки зрения безопасности и некритичные. Интерфейс ТСВ должен быть хорошо определен и ее проект и конечный результат должны быть подвергнуты полной проверке и тестированию. Механизм аудита должен быть усилен, введен контроль за конфигурацией; системы. Система должна быть устойчива к внешнему проникновению.

Политика безопасности. В дополнение к B1, помечаться должны все ресурсы системы прямо или косвенно доступные субъектам. Надежная вычислительная база должна немедленно извещать терминального пользователя об изменении его метки безопасности. Пользователь может запросить информацию о своей метке. Надежная вычислительная база должна поддерживать присваивание всем подключенным физическим устройствам минимального и максимального уровня секретности. Эти уровни должны использоваться при проведении в жизнь ограничений, налагаемых физической конфигурацией системы (например, расположением устройств).

Все ресурсы системы (в том числе ПЗУ, устройства ввода/вывода) должны иметь метки безопасности и служить объектами принудительного управления доступом.

Подотчетность. Надежная вычислительная база должна поддерживать надежный коммуникационный путь к себе для пользователя, выполняющего операции начальной идентификации и аутентификации. Инициатива в общении по этому пути должна исходить исключительно от пользователя. В дополнение к B1, должна быть возможность регистрировать события, связанные с организацией тайных каналов с памятью.

Гарантии. В дополнение к B1, надежная вычислительная база должна быть внутренне структурирована на хорошо определенные, относительно независимые модули. Надежная вычислительная база должна эффективно использовать имеющееся оборудование для отделения элементов, критически важных с точки зрения защиты, от прочих компонентов системы. Модули базы должны проектироваться с учетом принципа минимизации привилегий. Для защиты логически раздельных хранимых объектов должны использоваться аппаратные средства, такие как сегментация. Должен быть полностью определен пользовательский интерфейс к надежной вычислительной базе и все элементы базы.

Системный архитектор должен тщательно проанализировать возможности по организации тайных каналов с памятью и оценить максимальную пропускную способность каждого выявленного канала.

Система должна поддерживать разделение функций оператора и администратора.

В дополнение к B1, должна быть продемонстрирована относительная устойчивость надежной вычислительной базы к попыткам проникновения. Модель политики безопасности должна быть формальной. Для надежной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс.

В процессе разработки и сопровождения надежной вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль за изменениями в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации. Конфигурационное управление должно обеспечивать соответствие друг другу всех аспектов текущей версии надежной вычислительной базы.

Должны предоставляться средства генерации новых версий базы по исходным текстам и средства для сравнения версий, чтобы убедиться в том, что произведены только запланированные изменения.

Документация. В дополнение к B1, должны быть указаны модули надежной вычислительной базы, содержащие механизмы проверки обращений. Должна быть описана процедура безопасной генерации новой версии базы после внесения изменений в исходные тексты.

В дополнение к C1, тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

Модель политики безопасности должна быть формальной и доказательной. Должно быть показано, что описательные спецификации верхнего уровня точно отражают интерфейс надежной вычислительной базы. Должно быть показано, как база реализует концепцию монитора обращений, почему она устойчива к попыткам отслеживания ее работы, почему ее нельзя обойти и почему она реализована корректно, Должна быть описана структура базы, чтобы облегчить ее тестирование и проверку соблюдения принципа минимизации привилегий. Документация должна содержать результаты анализа тайных каналов передачи информации и описание мер протоколирования, помогающих выявлять каналы с памятью.

Класс B3. Домены безопасности. В системах класса B3 ТСВ должна удовлетворять всем требованиям предыдущего класса и дополнительно требованиям монитора ссылок, который должен быть:

- защищен от несанкционированного изменения или порчи;
- обрабатывать все обращения;
- прост для анализа и тестирования.

ТСВ должна быть структурирована таким образом, чтобы исключить код, не имеющий отношения к безопасности системы. Дополнительно должно быть обеспечено:

- поддержка администратора безопасности;
- расширение механизма аудита с целью сигнализации о любых событиях, связанных с безопасностью;
- поддержка процедуры восстановления системы.

Политика безопасности. В дополнение к C2, должны обязательно использоваться списки управления доступом с указанием разрешенных режимов. Должна быть возможность явного указания пользователей или их групп, доступ которых к объекту запрещен.

Подотчетность. В дополнение к B2, надежный коммуникационный путь может формироваться по запросу, исходящему как от пользователя, так и от самой базы. Надежный путь может использоваться для начальной идентификации и аутентификации, для изменения текущей метки безопасности пользователя и т.п. Общение по надежному пути должно быть логически отделено **и** изолировано от других информационных потоков. Должна быть возможность регистрации появления или накопления событий, несущих угрозу политике безопасности системы.

Администратор безопасности должен немедленно извещаться о попытках нарушения политики безопасности. А система, в случае продолжения попыток, должна пресекать их наименее болезненным способом.

Гарантии. В дополнение к B2, надежная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой. Этот механизм должен играть центральную роль во внутренней структуризации надежной вычислительной базы и всей системы. База должна активно использовать разделение по

уровням, абстракцию и инкапсуляцию данных. Значительные инженерные усилия должны быть направлены на уменьшение сложности надежной вычислительной базы и на вынесение из нее модулей, не являющихся критически важными с точки зрения защиты.

Должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий. Не относящиеся к защите действия администратора безопасности должны быть по возможности ограничены.

Должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты.

Должна быть продемонстрирована устойчивость надежной вычислительной базы к попыткам проникновения. Не должно быть выявлено архитектурных недостатков. Допускается выявление лишь небольшого числа исправимых недостатков реализации. Должна существовать обоснованная уверенность, что немногие недостатки остались невыявленными.

Документация. Руководство администратора по средствам безопасности в дополнение к B2, должна быть описана процедура, обеспечивающая безопасность начального запуска системы и возобновления ее работы после сбоя. Должно быть неформально продемонстрировано соответствие между описательными спецификациями верхнего уровня и реализацией надежной вычислительной базы.

Группа А. Верифицированная защита

Данная группа характеризуется применением формальных методов верификации, корректности работы механизмов управления доступом (дискреционного и мандатного). Требуется, чтобы было формально показано соответствие архитектуры и реализации ТСВ требованиям безопасности.

Класс А1. Формальная верификация. Критерий защиты класса А1 не определяет дополнительные по сравнению с классом В3 требования к архитектуре или политике безопасности компьютерной системы. Дополнительным свойством систем, отнесенных к классу А1, является проведенный анализ ТСВ на соответствие формальным высокоуровневым спецификациям и использование технологий проверки с целью получения высоких гарантий того, что ТСВ функционирует корректно.

Наиболее важные требования к классу А1 можно объединить в пять групп.

1. Формальная модель политики безопасности должна быть четко определена и документирована, должно быть дано математическое доказательство того, что модель соответствует своим аксиомам и что их достаточно для поддержания заданной политики безопасности.
2. Формальная высокоуровневая спецификация должна включать абстрактное определение выполняемых ТСВ функций и аппаратный и (или) встроенный программный механизм для обеспечения разделения доменов.
3. Формальная высокоуровневая спецификация ТСВ должна демонстрировать соответствие модели политики безопасности с использованием, где это возможно, формальной технологии (например, где имеются проверочные средства) и неформальной во всех остальных случаях.
4. Должно быть неформально показано и обратное - соответствие элементов ТСВ формальной высокоуровневой спецификации. Формальная высокоуровневая спецификация должна представлять собой универсальный механизм защиты, реализующий политику безопасности. Элементы этого механизма должны быть отображены на элементы ТСВ.
5. Должны быть использованы формальные технологии для выявления и анализа скрытых каналов. Неформальная технология может быть использована для анализа скрытых временных каналов. Существование оставшихся в системе скрытых каналов должно быть оправдано.

Более строгие требования предъявляются к управлению конфигурацией системы и конкретному месту дислокации (развертывания) системы

Перечисленные требования не затрагивают группы Политика безопасности и Подотчетность и сконцентрированы в группе Гарантии с соответствующим описанием в группе Документация.

5.2. Концепции защиты автоматизированных систем и средств вычислительной техники по руководящим документам Гостехкомиссии РФ

В 1992 г. Гостехкомиссия (ГТК) при Президенте Российской Федерации разработала и опубликовала пять руководящих документов [9], посвященных вопросам защиты информации в автоматизированных системах (АС) ее обработки. Основой этих документов является концепция защиты средств вычислительной техники (СВТ) и АС от несанкционированного доступа к информации, содержащая систему взглядов ГТК на проблему информационной безопасности и основные принципы защиты компьютерных систем. С точки зрения разработчиков данных документов, основная задача средств безопасности - это обеспечение защиты от несанкционированного доступа к информации. Определенный уклон в сторону поддержания секретности информации объясняется тем, что данные документы были разработаны в расчете на применение в информационных системах силовых структур РФ.

Структура требований безопасности

Руководящие документы ГТК состоят из пяти частей.

1. Защита от несанкционированного доступа к информации. Термины и определения.
2. Концепция защиты СВТ и АС от НСД к информации.
3. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
4. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации.
5. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники.

Наибольший интерес представляют вторая, третья и четвертая части. Во второй части излагается система взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от НСД. Руководящие документы ГТК предлагают две группы требований к безопасности - показатели защищенности СВТ от НСД и критерии защищенности АС обработки данных. Первая группа позволяет оценить степень защищенности отдельно поставляемых потребителю компонентов АС и рассматривается в четвертой части, а вторая рассчитана на более сложные комплексы, включающие несколько единиц СВТ, и представлена в третьей части руководящих документов.

Классы защищенности АС

В третьей части руководящих документов ГТК дается классификация АС и требований по защите информации в АС различных классов. При этом определяются:

1. Основные этапы классификации АС:

разработка и анализ исходных данных;

выявление основных признаков АС, необходимых для классификация

сравнение выявленных признаков АС с классифицируемыми;

присвоение АС соответствующего класса защиты информации от НСД.

2. Необходимые исходные данные для классификации конкретной АС:

перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

перечень лиц, имеющих доступ к штатным средствам АС с указанием их уровня полномочий;

матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

режим обработки данных в АС.

3. Признаки, по которым производится группировка АС в различные классы:

наличие в АС информации различного уровня конфиденциальности;|

уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

режим обработки данных в АС: коллективный или индивидуальный.

Документы ГТК устанавливают девять классов защищенности АС от НСД, распределенных по трем группам. Каждый класс характеризуется определенной совокупностью требований к средствам защиты. В пределах каждой группы соблюдается иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NA, где N- номер группы (от 1 до 3). Следующий класс обозначается NБ и т.д.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и хранимой в АС на носителях различного уровня конфиденциальности. Группа содержит два класса -2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности. Не все пользователи имеют равные права доступа.. Группа содержит пять классов - 1Д, 1 Г, 1 В, 1Б и 1А.

В табл. 5.2 приведены требования к подсистемам защиты для каждого класса защищенности.

На разработку этих документов наибольшее влияние оказал критерий TCSEC ("Оранжевая книга"), однако это влияние в основном отражается в ориентированности этих документов на защищенные системы силовых структур и в использовании единой универсальной шкалы оценки степени защищенности.

К недостаткам руководящих документов ГТК относятся: ориентация на противодействие НСД и отсутствие требований к адекватности реализации политики безопасности. Понятие "политика безопасности" трактуется исключительно как поддержание режима секретности и отсутствие НСД. Из-за этого средства защиты ориентируются только на противодействие внешним угрозам, а к структуре самой системы и ее функционированию не предъявляется четких требований. Ранжирование требований по классам защищенности по сравнению с остальными стандартами информационной безопасности максимально упрощено и сведено до определения наличия или отсутствия заданного набора механизмов защиты, что существенно снижает гибкость требований и возможность их практического применения. Несмотря на указанные недостатки, документы ГТК заполнили "правовой вакуум" в области стандартов информационной безопасности в России и оперативно решили проблему проектирования и оценки качества защищенных АС.

5.3. Критерии оценки безопасности информационных технологий (Common Criteria)

Основные понятия

«Критериев оценки безопасности информационных технологий» [10] (издан 1 декабря 1999 года) - самый полный и современный среди оценочных стандартов. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

По историческим причинам данный стандарт часто называют «Общими критериями» (или даже ОК). Мы также будем использовать это сокращение.

«Общие критерии» на самом деле являются метастандартом, определяющим инструменты оценки безопасности информационной системы (ИС) и порядок их использования. В отличие от «Оранжевой книги», ОК не содержат предопределенных «классов безопасности». Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные «программы» – задания по безопасности, типовые профили защиты и т.п. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, «с нуля», программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и «Общие критерии» предоставили соответствующий инструментарий.

Как и «Оранжевая книга», ОК содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки – аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- проектирование и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

- требованиях безопасности;
- проектировании;
- эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

Чтобы структурировать пространство требований, в «Общих критериях» введена иерархия класс – семейство – компонент - элемент.

Классы определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим нюансам требований.

Компонент – минимальный набор требований, фигурирующий как целое.

Элемент – неделимое требование.

Между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности. Но не все комбинации компонентов имеют смысл.

Как указывалось выше, с помощью библиотек могут формироваться два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Выше мы отмечали, что в ОК нет готовых классов защиты. Сформировать классификацию в терминах «Общих критериев» – значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно, на наш взгляд, сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Функциональный пакет – это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. «Общие критерии» не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в «Общих критериях» представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в «Оранжевой книге».

Перечислим классы функциональных требований ОК:

- идентификация и аутентификация;
- защита данных пользователя;
- защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);

- управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- доступ к объекту оценки;
- приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- использование ресурсов (требования к доступности информации);
- криптографическая поддержка (управление ключами);
- связь (аутентификация сторон, участвующих в обмене данными);
- доверенный маршрут/канал (для связи с сервисами безопасности).

Опишем подробнее два класса, демонстрирующие особенности современного подхода к ИБ.

Класс «Приватность» содержит 4 семейства функциональных требований.

Анонимность. Позволяет выполнять действия без раскрытия идентификатора пользователя другим пользователям, субъектам и/или объектам. Анонимность может быть полной или выборочной. В последнем случае она может относиться не ко всем операциям и/или не ко всем пользователям (например, у уполномоченного пользователя может оставаться возможность выяснения идентификаторов пользователей).

Псевдонимность. Напоминает анонимность, но при применении псевдонима поддерживается ссылка на идентификатор пользователя для обеспечения подотчетности или для других целей.

Невозможность ассоциации. Семейство обеспечивает возможность неоднократного использования информационных сервисов, но не позволяет ассоциировать случаи использования между собой и приписать их одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (и, следовательно, от получения информации на основе подобных профилей).

Скрытность. Требования данного семейства направлены на то, чтобы можно было использовать информационный сервис с сокрытием факта использования. Для реализации скрытности может применяться, например, широковещательное распространение информации, без указания конкретного адресата. Годятся для реализации скрытности и методы стеганографии, когда скрывается не только содержание сообщения (как в криптографии), но и сам факт его отправки.

Еще один показательный (с нашей точки зрения) класс функциональных требований – «Использование ресурсов», содержащий требования доступности. Он включает три семейства.

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В ОК различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

«Общие критерии» – очень продуманный и полный документ с точки зрения функциональных требований. В то же время, хотелось бы обратить внимание и на некоторые недостатки.

Первый – это отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение, как известно из технологии программирования, чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты – одна из форм накопления знаний. Следование в ОК «библиотечному», а не объектному подходу сужает круг фиксируемых знаний, усложняет их корректное использование.

К сожалению, в «Общих критериях» отсутствуют архитектурные требования, что является естественным следствием избранного старомодного программистского подхода «снизу вверх». Технологичность средств безопасности, следование общепризнанным рекомендациям по протоколам и программным интерфейсам, а также апробированным архитектурным решениям, таким как менеджер/агент, – необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности. Без рассмотрения интерфейсных аспектов системы оказываются нерасширяемыми и изолированными. Очевидно, с практической точки зрения это недопустимо. В то же время, обеспечение безопасности интерфейсов – важная задача, которую желательно решать единообразно.

Требования доверия безопасности

Установление доверия безопасности, согласно «Общим критериям», основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

- действия разработчиков;
- представление и содержание свидетельств;
- действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

- разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
- поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
- тестирование;
- оценка уязвимостей (включая оценку стойкости функций безопасности);
- поставка и эксплуатация;
- управление конфигурацией;
- руководства (требования к эксплуатационной документации);
- поддержка доверия (для поддержки этапов жизненного цикла после сертификации);
- оценка профиля защиты;
- оценка задания по безопасности.

Применительно к требованиям доверия в "Общих критериях" сделана весьма полезная вещь, не реализованная, к сожалению, для функциональных требований. А именно, введены так называемые оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Оценочный уровень доверия 1 (начальный) предусматривает анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также

независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.

Оценочный уровень доверия 2, в дополнение к первому уровню, предусматривает наличие проекта верхнего уровня объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.

На уровне 3 ведется контроль среды разработки и управление конфигурацией объекта оценки.

На уровне 4 добавляются полная спецификация интерфейсов, проекты нижнего уровня, анализ подмножества реализации, применение неформальной модели политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.

Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели политики безопасности, полуформальной функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

На уровне 6 реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.

Оценочный уровень 7 (самый высокий) предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

6. Основные этапы построения защищенной информационной системы

Цель мероприятий в области информационной безопасности – защитить интересы субъектов информационных отношений. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов: доступность, целостность, конфиденциальность.

Важность проблематики информационной безопасности (ИБ) объясняется двумя основными причинами:

- ценностью накопленных информационных ресурсов;
- критической зависимостью от информационных технологий.

Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа – все это выливается в крупные материальные потери, наносит ущерб репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей.

Современные информационные системы сложны и, значит, опасны уже сами по себе, даже без учета активности злоумышленников. Постоянно обнаруживаются новые уязвимые места в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Меняются принципы построения корпоративных информационных систем (ИС). Используются многочисленные внешние информационные сервисы; предоставляются вовне собственные.

Подтверждением сложности проблематики ИБ является параллельный (и довольно быстрый) рост затрат на защитные мероприятия и количества нарушений ИБ в сочетании с ростом среднего ущерба от каждого нарушения.

Успех в области информационной безопасности может принести только комплексный подход, сочетающий меры четырех уровней [10 – 12]:

- законодательного;
- административного;

- процедурного;
- программно-технического.

Бурное развитие глобальных сетей, привлекает все больше внимания к сети Internet со стороны частных лиц и различных организаций. Многие организации интегрируют свои сети в глобальную сеть, а также устанавливают свои серверы услуг (www-, FTP-) в глобальных сетях. Использование глобальных сетей в коммерческих целях, при передаче информации, содержащую коммерческую или государственную тайну, влечет за собой необходимость построения квалифицированной системы защиты информации.

При создании информационной инфраструктуры корпоративной автоматизированной системы на базе современных компьютерных сетей неизбежно возникает вопрос о защищенности этой структуры от угроз безопасности информации. Насколько адекватны реализованные в сети механизмы безопасности существующим рискам? Можно ли доверять этой системе обработку (хранение, передачу) конфиденциальной информации? И т.д. этот список велик.

Такими вопросами рано или поздно задаются все специалисты отделов защиты информации и других подразделений, отвечающих за эксплуатацию и сопровождение сетей. Ответы на эти вопросы далеко неочевидны. Анализ защищенности сети от угроз безопасности информации – работа сложная. Умение оценивать и управлять рисками, знание типовых угроз и уязвимостей, критериев и подходов к анализу защищенности, владение методами анализа, знание различных программно-аппаратных платформ, используемых в современных компьютерных сетях – все это далеко не полный перечень качеств, которыми должны обладать специалисты, проводящие работы по анализу защищенности сети. Анализ защищенности является фундаментом на базе, которого проводятся работы по построению защищенной информационной сети и аудиту (или проверке) безопасности этой сети в дальнейшем.

В первом разделе работы приведено достаточно подробное описание каждого уровня (законодательного, административного, процедурного, программно-технического) защиты информационных активов организации в отдельности. Раздел заканчивается примером построения автоматизированной сети предприятия на базе компьютерного оборудования, а также приводится возможная политика безопасности предприятия и список необходимых правил и инструкций для персонала организации.

Во втором разделе приводится классификация видов аудита безопасности и некоторые практические рекомендации по планированию и реализации авторизованного аудита, а также примеры активного аудита безопасности информационных активов организации.

Средства защиты информации делятся на формальные и неформальные. К первым относятся средства, выполняющие защитные функции строго по заранее предусмотренной процедуре и без непосредственного участия человека. К неформальным средствам отнесены такие, которые либо определяются целенаправленной деятельностью людей, либо регламентируют (непосредственно или косвенно) эту деятельность, рисунок 6.1.

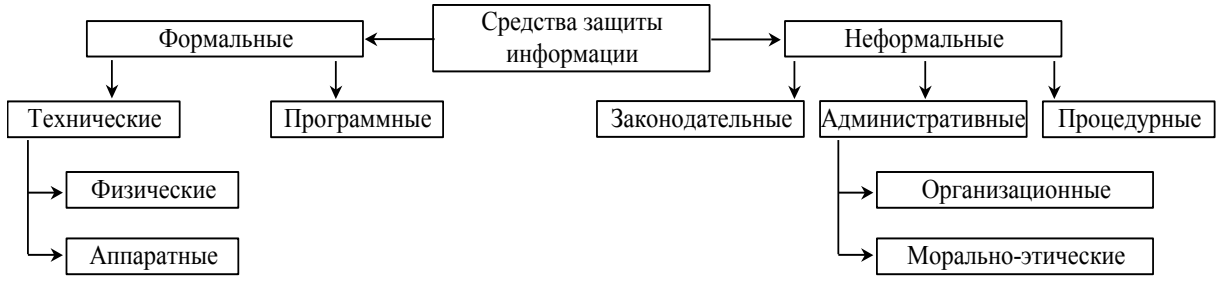


Рис. 6.1. Средства защиты информации

6.1. Законодательный уровень

6.1.1. Закон РФ «Об информации, информатизации и защите информации»

Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» (далее «Закон об информации») является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Основными задачами системы защиты информации, нашедшими отражение в «Законе об информации», являются:

- предотвращение утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п., вмешательства в информацию и информационные системы;
- сохранение полноты, достоверности, целостности информации, ее массивов и программ обработки данных, установленных собственником или уполномоченным им лицом;
- сохранение возможности управления процессом обработки, пользования информацией в соответствии с условиями, установленными собственником или владельцем информации;
- обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, накапливаемой в банках данных;

сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;

- соблюдение прав авторов программно-информационной продукции, используемой в информационных системах.

В частности статья 19 Закона устанавливает обязательность сертификации средств обработки и защиты документированной информации с ограниченным доступом, предназначенных для обслуживания граждан и организаций, а также обязательность получения лицензий для организаций, осуществляющих проектирование и производство средств защиты информации.

Статья 20 определяет основные цели защиты информации. В соответствии с этой статьей таковыми, в частности, являются:

- предотвращение утечки, хищения, утраты, искажения и подделки информации;
- предотвращение угроз безопасности личности, общества и государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- защита конституционных прав на сохранение личной тайны и конфиденциальности персональных сведений;
- сохранение государственной тайны и конфиденциальности информации.

Пункт 3 статьи 21 возлагает контроль за соблюдением требований к защите информации, за эксплуатацией специальных средств защиты информации, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, на органы государственной власти. Это означает, что контроль состояния защиты должен охватывать все три составляющие информации с ограниченным доступом, входящей в государственные информационные ресурсы:

- информацию, составляющую государственную тайну;
- конфиденциальную информацию;
- персональные данные о гражданах.

Очень важна статья 22, которая определяет права и обязанности субъектов в области защиты информации. В частности, пункты 2 и 5 обязывают владельца информационной системы обеспечивать необходимый уровень защиты конфиденциальной информации и оповещать собственников информационных ресурсов о фактов нарушения режима защиты информации. Пунктом 3 риск, связанный с использованием не сертифицированных информационных систем и средств их обеспечения и защиты, возлагается на собственника (владельца) систем и средств. Риск, связанный с использованием информации, полученной из таких систем, относится на потребителя информации. Пункт 4 устанавливает право собственника документов или информационной системы обращаться в организации, осуществляющие сертификацию средств защиты таких систем, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Статья 23 Закона посвящена защите прав субъектов в сфере информационных процессов и информатизации. Статья устанавливает, что защита прав субъектов в данной сфере осуществляется судом, арбитражным судом и третейскими судами, которые могут создаваться на постоянной или временной основе.

6.1.2. Закон РФ «О лицензировании отдельных видов деятельности»

Закон «О лицензировании отдельных видов деятельности» от 8 августа 2001 года номер 128-ФЗ (Принят Государственной Думой 13 июля 2001 года). Начнем с основных определений.

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Рассмотрим следующие виды:
- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;
- выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и (или) производство средств защиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:
- деятельность, связанная с защитой государственной тайны;
- деятельность в области связи;

- образовательная деятельность.

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия России. ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ. Все эти вопросы регламентированы соответствующими указами Президента и постановлениями Правительства РФ.

6.1.3. Пакет руководящих документов Государственной технической комиссии при Президенте Российской Федерации

В 1992 году Государственная техническая комиссия при Президенте РФ опубликовала пять «Руководящих документов», посвященных проблеме защиты от несанкционированного доступа (НСД) к информации, обрабатываемой средствами вычислительной техники (СВТ) и автоматизированными системами (АС) [2]:

«Руководящий документ. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем (АС) от несанкционированного доступа (НСД) к информации».- Гостехкомиссия России, 30 марта 1992 года.

«Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации».- Гостехкомиссия России, 30 марта 1992 года.

«Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».- Гостехкомиссия России, 30 марта 1992 года.

«Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники».- Гостехкомиссия России, 30 марта 1992 года.

«Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения».- Гостехкомиссия России, 30 марта 1992 года.

В 1997 году к этим документам добавился еще один [9]:

«Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

Концепция защиты средств вычислительной техники и АС от НСД к информации

Центральным элементом (идейной основой) набора руководящих документов Гостехкомиссии является «Руководящий документ. Концепция защиты СВТ и АС от НСД к информации» [9]. В этом документе излагается система взглядов и основных принципов, которые закладываются в основу проблемы защиты информации от НСД, являющейся частью общей проблемы безопасности информации.

В «Концепции» различаются два понятия, соответствующие двум группам критериев безопасности:

- показатели защищенности средств вычислительной техники,

- критерии защищенности автоматизированных систем.

«Концепция» предусматривает существование двух относительно самостоятельных и имеющих отличие направлений в проблеме защиты информации от НСД. Это - направление, связанное с СВТ, и направление, связанное с АС. Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

Существуют различные способы покушения на информационную безопасность: радиотехнические, акустические, программные и т.п. Среди них НСД выделяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

В разделе 3 «Концепции» формулируются основные принципы защиты от НСД к информации:

3.1. Защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

3.2. Защита СВТ обеспечивается комплексом программно-технических средств.

3.3. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

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

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

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

3.7. Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

В качестве главного средства защиты от НСД к информации в разделе 6 «Концепции» рассматривается система разграничения доступа (СРД) субъектов к объектам доступа:

6.1. Обеспечение защиты СВТ и АС осуществляется:
- СРД субъектов к объектам доступа;
- обеспечивающими средствами для СРД.

6.2. Основными функциями СРД являются:
- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

6.3. Обеспечивающие средства для СРД выполняют следующие функции:
- идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса; предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

6.4. Ресурсы, связанные как с СРД, так и с обеспечивающими ее средствами, включаются в объекты доступа.

6.5. Способы реализации СРД зависят от конкретных особенностей СВТ и АС. Возможно применение следующих способов защиты и любых их сочетаний:
- распределенная СРД и СРД, локализованная в программно-техническом комплексе (ядро защиты);
- СРД в рамках операционной системы, СУБД или прикладных программ;
- СРД в средствах реализации сетевых взаимодействий или на уровне приложений;
- использование криптографических преобразований или методов непосредственного контроля доступа;
- программная и (или) техническая реализация СРД.

В целом разработка Руководящих документов Гостехкомиссии России явилась следствием бурно развивающегося процесса внедрения новых информационных технологий. Документы достаточно оперативно заполнили правовой вакуум в области стандартов информационной безопасности в стране и на определенном этапе позволили решать актуальную задачу обеспечения безопасности информации. Поскольку разработка документов такого рода для России представляет достаточно новую область деятельности, можно рассматривать их как первую стадию формирования отечественных стандартов в области информационной безопасности.

На разработку этих документов большое влияние оказала «Оранжевая книга» Министерства обороны США, которое выразилось в ориентации на системы военного и специального применения, в использовании единой универсальной шкалы степени защищенности и в игнорировании вопросов ценности и времени жизни информации.

К недостаткам документов, помимо отсутствия требований к защите от угроз работоспособности, относится ориентация только на противодействие НСД и отсутствие требований к адекватности реализации политики безопасности. Собственно «политика безопасности» трактуется в этих документах исключительно как поддержание режима секретности и отсутствие НСД. Из-за этого средства защиты ориентируются на противодействие только внешним угрозам, а к структуре самой системы и ее функционированию не предъявляется никаких требований.

С точки зрения разработчиков данных руководящих документов основная и едва ли не единственная задача средств обеспечения безопасности – это обеспечение защиты от несанкционированного доступа к информации. Если средствам контроля и обеспечения целостности информации в них еще уделяется некоторое внимание, то поддержка работоспособности систем обработки информации (как мера защиты от угроз работоспособности) вообще не упоминается. Определенный уклон в сторону поддержания секретности объясняется тем, что эти документы были разработаны в расчете на

применение в существующих информационных системах Министерства обороны и спецслужб России, а также недостаточно высоким уровнем технологий этих систем.

Документы Гостехкомиссии России о модели нарушителя в АС

Модель нарушителя определяется в 4-м разделе основного Руководящего документа Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» [2].

В качестве *нарушителя* в этом документе рассматривается субъект, имеющий доступ к работе с штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Подчеркивается, что в своем уровне нарушитель является специалистом высшей квалификации, знает все о АС и, в частности, о системе и средствах ее защиты.

Классификация защищенности СВТ. Классификация защищенности АС

Руководящие документы Гостехкомиссии России «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» [2] и «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [2] определяют основные показатели защищенности по классам средств вычислительной техники (Таблица 6.1) и требования к классам защищенности автоматизированных систем (Таблица 6.2).

Таблица 6.1 – Распределение показателей защищенности по классам средств вычислительной техники

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчужденный	-	-	+	=	=	=

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
носитель информации						
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения:
« - » - нет требований к данному классу
« + » - новые или дополнительные требования
« = » - требования совпадают с требованиями к СВТ предыдущего класса

Седьмой класс присваивается средствам вычислительной техники, к которым предъявлялись требования по защите от несанкционированного доступа к информации, но при оценке защищенность средства оказалась ниже уровня требований шестого класса.

Таблица 6.2 – Требования к классам защищенности автоматизированных систем

Подсистемы и требования	Классы								
	3Б	3 А	2Б	2 А	1 Д	1Г	1 В	1Б	1 А
I. Подсистема управления доступом									
Идентификация, проверка подлинности и контроль доступа субъектов:									
В систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ				+		+	+	+	+
к программам				+		+	+	+	+
к томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
Управление потоками информации				+			+	+	+
II. Подсистема регистрации и учета									
Регистрация и учет									
входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
выдачи печатных (графических)		+		+		+	+	+	+

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
выходных документов									
запуска/завершения программ и процессов (заданий, задач)				+		+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи				+		+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
изменения полномочий субъектов доступа							+	+	+
создаваемых защищаемых объектов доступа				+			+	+	+
Учет носителей информации	+	+	+	+	+	+	+	+	+
Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей		+		+		+	+	+	+
Сигнализация попыток нарушения защиты							+	+	+
III. Криптографическая подсистема									
Шифрование конфиденциальной информации				+				+	+
Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах									+
Использование аттестованных (сертифицированных) криптографических средств				+				+	+
IV. Подсистема обеспечения целостности									
Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
Наличие администратора (службы) защиты информации в АС				+			+	+	+
Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
Использование сертифицированных средств защиты		+		+			+	+	+

Обозначения:
« + » - требование к данному классу присутствует.

Показатели защищенности МЭ

В руководящем документе Гостехкомиссии России [9]: «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» устанавливается классификация межсетевых экранов (МЭ) по уровня защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под сетями ЭВМ, распределенными АС, в данном документе понимаются соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя.

МЭ представляет собой локальное (однокомпонентное) или функционально - распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Руководящий документ разработан в дополнение к Руководящим документам Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Документ предназначен для заказчиков и разработчиков МЭ, а также сетей ЭВМ, распределенных автоматизированных систем с целью использования при формулировании и реализации требований по их защите от НСД к информации.

Общие положения

Данные показатели содержат требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации и реализованных в виде МЭ.

Показатели защищенности применяются к МЭ для определения уровня защищенности, который они обеспечивают при межсетевом взаимодействии.

Конкретные перечни показателей определяют классы защищенности МЭ.

Деление МЭ на соответствующие классы по уровням контроля межсетевых информационных потоков с точки зрения защиты информации необходимо в целях разработки и применения обоснованных и экономически оправданных мер по достижению требуемого уровня защиты информации при взаимодействии ЭВМ, АС. Дифференциация подхода к выбору функций защиты в МЭ определяется АС, для защиты которой применяется данный экран.

Устанавливается пять классов защищенности МЭ. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности – пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый – для 1Г, третий – 1В, второй – 1Б, самый высокий – первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой

Требования, предъявляемые к МЭ, не исключают требований, не исключают требований, предъявляемых к СВТ и АС в соответствии с руководящими документами Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться. Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса. Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

- при обработке информации с грифом «секретно» - не ниже 3 класса;
- при обработке информации с грифом «совершенно секретно» - не ниже 2 класса;
- при обработке информации с грифом «особой важности» - не ниже 1 класса.

Таким образом, фактически, обмен информацией, составляющей государственную тайну, между автоматизированными системами классов 1Д – 1А или при наличии такой системы только на одном конце, данным документом не предусмотрен.

Перечень показателей по классам защищенности МЭ

Таблица 6.3.

Показатели защищенности	Классы защищенности				
	5	4	3	2	1
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	=
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Обозначения:
« - » - нет требований к данному классу;
« + » - новые или дополнительные требования;
« = » - требования совпадают с требованиями к МЭ предыдущего класса

6.2. Административный уровень

К *административному уровню* информационной безопасности относятся действия общего характера, предпринимаемые руководством организации. Административный уровень является основой практического построения интегрированной системы, определяющей генеральное направление работ по обеспечению безопасности информации (ОБИ).

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения. Программа представляет официальную политику безопасности, отражающую собственный концептуальный подход организации к ОБИ. Конкретизация политики безопасности выражается в планах по информационной защите АС.

Практические мероприятия по созданию системы ОБИ, включают следующие этапы:

- Разработка политики безопасности.
- Проведение анализа рисков.
- Планирование обеспечения информационной безопасности.
- Планирование действий в чрезвычайных ситуациях.
- Подбор механизмов и средств обеспечения информационной безопасности.
- Собственно первые два этапа обычно трактуются как выработка политики безопасности и составляют административный уровень системы ОБИ предприятия.
- Третий и четвертый этапы заключаются в разработке процедур безопасности, на этих этапах формируется уровень планирования системы ОБИ, этот уровень так же можно назвать *процедурным*.

На последнем этапе практических мероприятий определяется *программно-технический* уровень системы ОБИ.

6.2.1. Политика безопасности

В «Оранжевой книге» *политика безопасности* трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности (ПБ) трактуется несколько шире — как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является высокоуровневый документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Данный документ представляет методологическую основу практических мер (процедур) по реализации ОБИ и содержит следующие группы сведений.

- Основные положения информационной безопасности.
- Область применения.
- Цели и задачи обеспечения информационной безопасности.
- Распределение ролей и ответственности.
- Общие обязанности.

Основные положения определяют важность ОБИ, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

Областью применения политики безопасности являются основные активы и подсистемы АС, подлежащие защите. Типовыми активами являются программно-аппаратное и информационное обеспечение АС, персонал, в отдельных случаях информационная инфраструктура предприятия.

Цели, задачи, критерии ОБИ вытекают из функционального назначения предприятия. Например, для режимных организаций на первое место ставится

соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности (оперативной готовности) подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т.д. Здесь указываются законы и правила организации, которые следует учитывать при проведении работ по ОБИ.

Типовыми целями могут быть следующие:

- обеспечение уровня безопасности, соответствующего нормативным документам предприятия;
- следование экономической целесообразности в выборе защитных мер;
- обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС;
- обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации и др.

Если предприятие не является изолированным, цели и задачи рассматриваются в более широком контексте: должны быть оговорены вопросы безопасного взаимного влияния локальных и удаленных подсистем.

В рассматриваемом документе могут быть конкретизированы некоторые стратегические принципы безопасности (вытекающие из целей и задач ОБИ). Таковыми являются стратегии действий в случае нарушения политики безопасности предприятия и сторонних организаций, взаимодействия с внешними организациями, правоохранительными органами, прессой и др. В качестве примера можно привести две стратегии ответных действий на нарушение безопасности:

- «выследить и осудить», когда злоумышленнику позволяют продолжить действия с целью его компрометации и наказания (данную стратегию одобряют правоохранительные органы!);
- «защититься и продолжить», когда организация опасается за уязвимость информационных ресурсов и оказывает максимальное противодействие нарушению.

Политика безопасности затрагивает всех пользователей компьютеров в организации. Поэтому важно решить так называемые политические вопросы наделения всех категорий пользователей соответствующими правами, привилегиями и обязанностями.

Для этого определяется круг лиц, имеющий доступ к подсистемам и сервисам АС. Для каждой категории пользователей описываются правильные и неправильные способы использования ресурсов — что запрещено и разрешено. Здесь специфицируются уровни и регламентация доступа различных групп пользователей. Следует указать какое из правил умолчания на использование ресурсов принято в организации, а именно:

- что явно не запрещено, то разрешено или
- что явно не разрешено, то запрещено.

Одним из самых уязвимых мест в ОБИ является распределение прав доступа. В политике безопасности должна быть утверждена схема управления распределением прав доступа к сервисам — централизованная или децентрализованная, или иная. Должно быть четко определено, кто распоряжается правами доступа к сервисам и какими именно правами. Целесообразно детально описать практические процедуры наделения пользователей правами. Здесь следует указать должностных лиц, имеющих административные привилегии и пароли для определенных сервисов.

Права и обязанности пользователей определяются применительно к безопасному использованию подсистем и сервисов АС. При определении прав и обязанностей администраторов следует стремиться к некоторому балансу между правом пользователей на тайну и обязанностью администратора контролировать нарушения безопасности.

Важным элементом политики является распределение ответственности. Политика не может предусмотреть всего, однако она должна для каждого вида проблем найти ответственного.

Обычно выделяется несколько уровней ответственности. На первом уровне каждый пользователь обязан работать в соответствии с политикой безопасности (защищать свой счет), подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях. Системные администраторы отвечают за защиту соответствующих информационно-вычислительных подсистем. Администраторы сетей должны обеспечивать реализацию организационно-технических мер, необходимых для проведения в жизнь политики безопасности АС. Более высокий уровень - руководители подразделений отвечают за доведение и контроль положений политики безопасности.

С практической точки зрения, политику безопасности целесообразно разделить на несколько уровней (как правило, выделяют два-три уровня).

Верхний уровень носит общий характер и определяет политику организации в целом. Здесь основное вниманию уделяется: порядку создания и пересмотра политики безопасности; целям, преследуемым организацией в области информационной безопасности; вопросам выделения и распределения ресурсов; принципам технической политики в области выбора методов и средств защиты информации; координированию мер безопасности; стратегическому планированию и контролю; внешним взаимодействиям и другим вопросам, имеющим общеорганизационный характер.

На указанном уровне формулируются главные цели в области информационной безопасности (определяемые сферой деятельности предприятия): обеспечение конфиденциальности, целостности и/или доступности [2].Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Средний уровень политики безопасности выделяют в случае структурной сложности организации либо при необходимости обозначить специфичные подсистемы организации. Это касается отношения к перспективным, еще не достаточно апробированным технологиям. Например, использование новых сервисов Internet, организация связи и обработка информации на домашних и портативных компьютерах, степень соблюдения положений компьютерного права и др. Кроме того, на среднем уровне политики безопасности могут быть выделены особо значимые контуры АС организации, например, обрабатывающие секретную или критично важную информацию. Т.е. к среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения (ПО), последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности.

Позиция организации по данному аспекту. Продолжая пример с неофициальным ПО, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте.

Роли и обязанности. В «политический» документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики

безопасности. Например, если для использования неофициального ПО сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное ПО использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

За разработку и реализацию политики безопасности верхнего и среднего уровней отвечают руководитель службы безопасности, администраторы безопасности АС, администратор корпоративной сети.

Нижний уровень политики безопасности относится к конкретным службам или подразделениям организации и детализирует верхние уровни политики безопасности. Данный уровень необходим, когда вопросы безопасности конкретных подсистем требуют решения на управленческом, а не только на техническом уровне.

Понятно, что на данном уровне определяются конкретные цели, частные критерии и показатели информационной безопасности, определяются права конкретных групп пользователей, формулируются соответствующие условия доступа к информации и т.п. Здесь из конкретных целей выводятся (обычно формальные) *правила безопасности,* описывающие, кто, что и при каких условиях может делать или не может. Более детальные и формальные правила упростят внедрения системы и настройку средств ОБИ.

На этом уровне описываются механизмы защиты информации и используемые программно-технические средства для их реализации (в рамках, конечно, управленческого уровня, но не технического).

За политику безопасности нижнего уровня отвечают системные администраторы.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный раздел, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный раздел, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы физической защиты;

управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;

- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

В рамках разработки политики безопасности проводится анализ рисков. Это делается с целью минимизации затрат на ОБИ. Основной принцип безопасности: затраты

на средства защиты не должны превышать стоимости защищаемых объектов. При этом если ПБ оформляется в виде высокоуровневого документа, описывающего общую стратегию, то анализ рисков (как приложение) оформляется в виде списка активов, нуждающихся в защите.

6.2.2. Анализ рисков

Управление рисками (или их анализ) рассматривается на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Управление рисками и выработка собственной ПБ, актуально только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными. Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами.

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая *оценка рисков* необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения уровень риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Таким образом, суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- оценка рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска;
- уменьшение риска (за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на несколько этапов, рисунок 6.2.

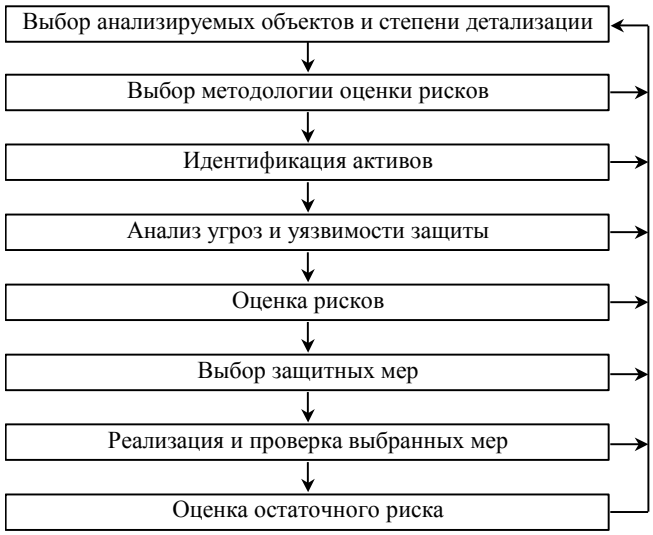


Рис. 6.2. Алгоритм анализа рисков

Два последних этапа (реализация и проверка выбранных мер, оценка остаточного риска) относятся к выбору защитных средств (нейтрализации рисков), остальные – к оценке рисков. Уже перечисление этапов показывает, что управление рисками – процесс циклический. По существу, последний этап – это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

Предварительный этап анализа риска

На начальном этапе методом экспертной оценки решаются общие вопросы проведения анализа риска. Первым делом выбираются компоненты АС и степень детальности их рассмотрения. Всеобъемлющий анализ требует рассмотрения всей информационной инфраструктуры. Но на практике из принципа разумной достаточности могут быть выделены и подвергнуты большей детализации отдельные наиболее важные компоненты и службы, в первую очередь, где риски велики или неизвестны. Более тщательному анализу подвергаются новые и модифицированные компоненты АС, а также компоненты, где имели место новые инциденты и нарушения безопасности.

Далее выбираются методологии оценки рисков как процесса получения количественной или качественной оценки ущерба, который может произойти в случае реализации угроз безопасности АС. Методологии носят частный характер, присущий организации и АС, и зависят от конкретного множества дестабилизирующих факторов и условий функционирования АС, возможности их количественной оценки, степени их неточности, неполноты, нечеткости и т.д. На практике, с учетом допустимой приближенной оценки рисков, часто используют простые наглядные методы, основанные на элементах теории вероятности и математической статистики.

Идентификация активов

Основу процесса анализа риска составляет определение: что надо защищать, от кого и как. Для этого выявляются активы (компоненты АС), нуждающиеся в защите. Ниже представлены основные категории активов АС предприятия.

Аппаратное обеспечение (компьютеры, периферийные устройства, коммуникационные линии, сетевое оборудование и их составные части).

Программное обеспечение (исходные, объектные и загрузочные модули операционных систем, вспомогательных системных и коммуникационных программ, инструментальных средств разработки, прикладных программных пакетов).

Информационное обеспечение (вводимые и обрабатываемые, хранимые, передаваемые и резервные (сохранные копии) данные и метаданные).

Персонал (обслуживающий персонал и пользователи).

Документация (конструкторская, техническая, пользовательская и иная документация).

Расходные материалы (бумага, магнитные носители, картриджи и т.д.).

В некоторых специфичных АС активы, уникальные для организации, могут быть выделены в отдельные группы, например: коммуникационное, алгоритмическое или лингвистическое обеспечение. Кроме того, могут подлежать защите части инфраструктуры, в частности подсистемы электроснабжения и др.

Главным результатом процесса идентификации активов является получение детальной информационной структуры организации и способов использования информации. Дальнейшие этапы анализа риска основываются именно на данной, зафиксированной на некоторый момент времени, информации.

Анализ угроз

После идентификации активов АС следует рассмотреть все возможные угрозы указанным активам, оценить риски и ранжировать их по степени возможного ущерба.

Под *угрозой* обычно понимают любое событие (действие), которое потенциально может нанести ущерб АС путем нарушения нарушению конфиденциальности, целостности или доступности информации. Угрозы могут быть преднамеренными, являющимися следствием умышленных (злонамеренных) действий людей, и непреднамеренные, вызванные ошибками человека или сбоями и отказами работы технических и программных средств, или стихийными действиями. В настоящее время существует огромное количество угроз, способных привести к нарушению конфиденциальности, целостности и доступности информации.

При анализе угроз необходимо выявить их источники и условия реализации. Это поможет в выборе дополнительных средств защиты. Часто одни угрозы могут быть следствием или условием проявления ряда других угроз. Например, несанкционированный доступ (в различных формах его проявления) к ресурсам облегчает реализацию практически любой угрозы: от порчи магнитного носителя до комплексной удаленной атаки.

Оценка рисков

После идентификации угрозы необходимо оценить риск проявления угрозы. В большинстве случаев возможно получить количественную оценку риска. Она может быть получена на базе экспертного опроса, оценена статистически или рассчитана по некоторой математической зависимости (адекватной конкретной угрозе конкретному активу).

Кроме вероятности осуществления угрозы, важен размер ожидаемых потерь. В общем случае ожидаемые потери рассчитываются по следующей формуле:

$$E = P \cdot V, \qquad (6.1)$$

где P – вероятностная оценка риска проявления угрозы,

V – ущерб при реализации угрозы.

Однако, как вероятности угрозы, так и ожидаемые потери не всегда можно оценить количественно. Например, рассчитать замену компьютера достаточно просто, но трудно оценить потенциальный ущерб в случае задержки выдачи данных, искажения

информации, разглашения отдельных сведений и т.д. Некоторые инциденты могут нанести ущерб репутации фирмы, вызвать социальную напряженность в коллективе, повлечь юридическое преследование предприятия со стороны пользователей и т.д.

Существует несколько простых способов оценки вероятностей проявления угроз и возможных потерь:

- Экспертная оценка событий. Методы экспертных оценок применяются при оценке трудно предсказуемых угроз, например стихийных бедствий, и являются самыми неточными.
- Методика определения приемлемости уровня риска по трехбалльной шкале. Согласно методике, оцениваемым рискам и ущербам ставятся оценки по трехбалльной шкале: 1, 2, 3. Полученные два множества оценок рисков и ущербов перемножаются. Множество возможных значений будет следующим: 1, 2, 3, 4, 6, 9. Полагается, что первые два значения характеризуют низкий уровень риска, третий и четвертый – средний, два последних – высокий.

Методика определения приемлемости уровня риска с учетом видимости угроз и их последствий. Здесь вводится понятие видимости угрозы для внешнего мира – мера информации о системе, доступной злоумышленнику (и вызывающей нездоровый интерес). Согласно указанной методике, оцениваемым рискам, видимости, физическим ущербам и моральным ущербам ставятся оценки по трехбалльной шкале 1, 2, 3. Значения рисков умножаются на значения для видимости, а значения для физического ущерба умножаются на значения для морального ущерба. Затем полученные два числа складываются. Считается, что уровень риска низкий, если итоговое число меньше 7, высокий, если итоговое число больше 11, иначе – средний.

Статистическая оценка событий и использование статистических моделей (отражающих законы распределения конкретных типов угроз). Данный метод позволяет получить приемлемые результаты для оценки часто проявляемых регистрируемых угроз, например: сбоев и отказов вычислительного процесса.

Использование аналитических моделей (возможно в виде таблиц) потенциального ущерба в зависимости от заранее определенных коэффициентов.

Следует оговориться, что методы анализа риска обычно не отличаются высокой точностью. Дело в том, что основная задача анализа риска (как инструмента планирования) оценить уровень возможных потерь и уровень затрат на защиту. Для практики, когда разнородные исходные данные имеют приближенный или субъективный характер оценки, высокая точность расчета и не требуется. Иногда вообще невозможно оценить точность результата.

Выбор и проверка защитных мер

Для уменьшения размера ущерба необходим выбор соответствующих мер защиты: организационных, физических, программно-технических и др. Каждая угроза может быть предотвращена различными способами. Поэтому на данном этапе решается задача анализа и синтеза мер, методов и средств защиты по критерию эффективность/стоимость с учетом, конечно, технической политики организации и других жизненно важных характеристик АС.

После выбора способов защиты АС производится проверка их эффективности. Если остаточные риски стали опять-таки неприемлемы, весьма разумно повторить этапы анализа риска.

Завершая подраздел, следует отметить, что разработка политики безопасности и проведение анализа риска являются кропотливыми научно-техническими задачами. Поэтому важно правильно подобрать коллектив разработчиков. Обычно этим профессионально занимается группа информационной безопасности предприятия. Однако

возможно привлечение администраторов и разработчиков систем и сетей, специалистов по аудиту и управлению, психологов, представителей службы режима.

6.3. Процедурный уровень

6.3.1. Основные классы мер процедурного уровня

Эти меры безопасности ориентированы на людей. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому «человеческий фактор» заслуживает особого внимания.

В российских компаниях накоплен богатый опыт регламентирования и реализации процедурных (организационных) мер, однако дело в том, что они пришли из «докомпьютерного» прошлого, поэтому требуют переоценки.

Следует осознать ту степень зависимости от компьютерной обработки данных, в которую попало современное общество. Без всякого преувеличения можно сказать, что необходима информационная гражданская оборона. Спокойно, без нагнетания страстей, нужно разъяснять обществу не только преимущества, но и опасности, связанные с использованием информационных технологий. Акцент следует делать не на военной или криминальной стороне дела, а на гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

На процедурном уровне можно выделить следующие классы мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Управление персоналом

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше – с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надежнее поручить одному сотруднику оформление заявок на подобные платежи, а другому – заверять эти заявки. Другой пример – процедурные ограничения действий суперпользователя. Можно искусственно «расщепить» пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую – другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоем, что снижает вероятность ошибок и злоупотреблений.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно – уменьшить ущерб от случайных или умышленных некорректных действий.

Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов. Чем ответственнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослуживцами и т.д. Подобная процедура может быть длительной и дорогой, поэтому нет смысла дополнительно усложнять ее. В то же время, неразумно и совсем отказываться от предварительной проверки, чтобы случайно не принять на работу человека с уголовным прошлым или психическим заболеванием. Когда кандидат определен, он, вероятно, должен пройти обучение; по крайней мере, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности и т.п. Все это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меняется, что создает трудности при выявлении подозрительных ситуаций. Определенную аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая ликвидировать старые права доступа.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале – одновременно с извещением о наказании или увольнении). Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное хозяйство и, в частности, криптографические ключи, если использовались средства шифрования.

К управлению сотрудниками примыкает администрирование лиц, работающих по контракту (например, специалистов фирмы-поставщика, помогающих запустить новую систему). В соответствии с принципом минимизации привилегий, им нужно выделить ровно столько прав, сколько необходимо, и изъять эти права сразу по окончании контракта. Проблема, однако, состоит в том, что на начальном этапе внедрения «внешние» сотрудники будут администрировать «местных», а не наоборот. Здесь на первый план выходит квалификация персонала организации, его способность быстро обучаться, а также оперативное проведение учебных курсов. Важны и принципы выбора деловых партнеров.

Иногда внешние организации принимают на обслуживание и администрирование ответственные компоненты компьютерной системы, например, сетевое оборудование. Нередко администрирование выполняется в удаленном режиме. Вообще говоря, это создает в системе дополнительные уязвимые места, которые необходимо компенсировать усиленным контролем средств удаленного доступа или, опять-таки, обучением собственных сотрудников.

Физическая защита

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных.

Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как “непрерывность защиты в пространстве и времени”. Ранее мы рассматривали понятие окна опасности. Для физической защиты таких окон быть не должно. Направления физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации, а также отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и т.п.

При проектировании и реализации мер физического управления доступом целесообразно применять *объектный подход*. Во-первых, определяется периметр безопасности, ограничивающий контролируемую территорию. На этом уровне детализации важно продумать внешний интерфейс организации – порядок входа/выхода штатных сотрудников и посетителей, вноса/выноса техники. Все, что не входит во внешний интерфейс, должно быть инкапсулировано, то есть, защищено от нелегальных проникновений.

Во-вторых, производится декомпозиция контролируемой территории, выделяются (под) объекты и связи (проходы) между ними. При такой, более глубокой детализации следует выделить среди подобъектов наиболее критичные с точки зрения безопасности и обеспечить им повышенное внимание. Декомпозиция должна быть семантически оправданной, обеспечивающей разграничение разнородных сущностей, таких как оборудование разных владельцев или персонал, работающий с данными разной степени критичности.

Необходимо, чтобы посетители, по возможности, не имели непосредственного доступа к компьютерам или, в крайнем случае, позаботиться о том, чтобы от окон и дверей не просматривались экраны мониторов и принтеры. Необходимо, чтобы посетителей по внешнему виду можно было отличить от сотрудников.

Средства физического управления доступом – это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального (по критерию стоимость/эффективность) средства целесообразно провести анализ рисков (к этому мы еще вернемся). Кроме того, есть смысл периодически отслеживать появление технических новинок в данной области, стараясь максимально автоматизировать физическую защиту.

Отметим необходимость установки противопожарной сигнализации и автоматических средств пожаротушения. К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры и средства коммуникаций. При размещении компьютеров необходимо принять во внимание расположение водопроводных и канализационных труб и постараться держаться от них подальше. Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных может осуществляться самыми разными способами. Злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок (ПЭМИН) и т.д. Остается уповать на повсеместное использование криптографии (что, впрочем, сопряжено у нас в стране со множеством технических и законодательных проблем), стараться максимально расширить контролируемую территорию, разместившись в тихом особнячке, поодаль от других домов, пытаться держать под контролем линии связи

(например, заключать их в надувную оболочку с обнаружением прокалывания), но самое разумное, вероятно, – постараться осознать, что для коммерческих систем обеспечение конфиденциальности является все-таки не главной задачей.

Мобильные и портативные компьютеры – заманчивый объект кражи. Их часто оставляют без присмотра, в автомобиле или на работе, и похитить такой компьютер совсем несложно. То и дело средства массовой информации сообщают о том, что какой-нибудь офицер английской разведки или американский военный лишился таким образом движимого имущества. Мы настоятельно рекомендуем шифровать данные на жестких дисках таких компьютеров.

Вообще говоря, при выборе средств физической защиты следует производить анализ рисков. Так, принимая решение о закупке источника бесперебойного питания, необходимо учесть качество электропитания в здании, занимаемом организацией (впрочем, почти наверняка оно окажется плохим). Характер и длительность сбоев электропитания, стоимость доступных источников и возможные потери от аварий (поломка техники, приостановка работы организации и т.п.).

В то же время, во многих случаях решения очевидны. Меры противопожарной безопасности обязательны для всех организаций. Стоимость реализации многих мер (например, установка обычного замка на дверь серверной комнаты) либо мала, либо хоть и заметна, но все же явно меньше, чем возможный ущерб. В частности, имеет смысл регулярно копировать большие базы данных.

Поддержание работоспособности

Далее рассмотрим ряд мероприятий, направленных на поддержание работоспособности информационных систем. Именно здесь таится наибольшая опасность. Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных; в лучшем случае они создают бреши в защите, которые делают возможной реализацию угроз.

Недооценка факторов безопасности в повседневной работе – ахиллесова пята многих организаций. Дорогие средства безопасности теряют смысл, если они плохо документированы, конфликтуют с другим программным обеспечением, а пароль системного администратора не менялся с момента установки.

Можно выделить следующие направления повседневной деятельности:

- поддержка пользователей;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Поддержка пользователей подразумевает прежде всего консультирование и оказание помощи при решении разного рода проблем. Иногда в организациях создают для этой цели специальный «справочный стол», но чаще от пользователей отбивается системный администратор. Очень важно в потоке вопросов уметь выявлять проблемы, связанные с информационной безопасностью. Так, многие трудности пользователей, работающих на персональных компьютерах, могут быть следствием заражения вирусами. Целесообразно фиксировать вопросы пользователей, чтобы выявлять их типичные ошибки и выпускать памятки с рекомендациями для распространенных ситуаций.

Поддержка программного обеспечения – одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо следить за тем, какое программное обеспечение установлено на компьютерах. Если пользователи будут

устанавливать программы по своему усмотрению, это может привести к заражению вирусами, а также появлению утилит, действующих в обход защитных средств. Вполне вероятно также, что «самодеятельность» пользователей постепенно приведет к хаосу на их компьютерах, а исправлять ситуацию придется системному администратору.

Второй аспект поддержки программного обеспечения – контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда же можно отнести поддержку эталонных копий программных систем. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и обеспечения целостности.

Конфигурационное управление позволяет контролировать и фиксировать изменения, вносимые в программную конфигурацию. Прежде всего, необходимо застраховаться от случайных или непродуманных модификаций, уметь как минимум возвращаться к прошлой, работающей, версии. Фиксация изменений позволит легко восстановить текущую версию после аварии.

Лучший способ уменьшить количество ошибок в рутинной работе – максимально автоматизировать ее. Автоматизация и безопасность зависят друг от друга; тот, кто заботится в первую очередь об облегчении своей задачи, на самом деле оптимальным образом формирует режим информационной безопасности.

Резервное копирование необходимо для восстановления программ и данных после аварий. И здесь целесообразно автоматизировать работу, как минимум, сформировав компьютерное расписание создания полных и инкрементальных копий, а как максимум – воспользовавшись соответствующими программными продуктами. Нужно также наладить размещение копий в безопасном месте, защищенном от несанкционированного доступа, пожаров, протечек, то есть от всего, что может привести к краже или повреждению носителей. Целесообразно иметь несколько экземпляров резервных копий и часть из них хранить вне территории организации, защищаясь таким образом от крупных аварий и аналогичных инцидентов. Время от времени в тестовых целях следует проверять возможность восстановления информации с копий.

Управлять носителями необходимо для обеспечения физической защиты и учета дискет, лент, печатных выдач и т.п. Управление носителями должно обеспечивать конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем. Под физической защитой здесь понимается не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды (жары, холода, влаги, магнетизма). Управление носителями должно охватывать весь жизненный цикл – от закупки до выведения из эксплуатации.

Документирование – неотъемлемая часть информационной безопасности. В виде документов оформляется почти все – от политики безопасности до журнала учета носителей. Важно, чтобы документация была актуальной, отражала именно текущее состояние дел, причем в непротиворечивом виде.

К хранению одних документов (содержащих, например, анализ уязвимых мест системы и угроз) применимы требования обеспечения конфиденциальности, к другим, таким как план восстановления после аварий – требования целостности и доступности (в критической ситуации план необходимо найти и прочитать).

Регламентные работы – очень серьезная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и на практике очень трудно проконтролировать, какие именно действия он совершает. Здесь на первый план выходит степень доверия к тем, кто выполняет работу.

Реагирование на нарушения режима безопасности

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

В организации должен быть человек, доступный 24 часа в сутки (лично, по телефону, пейджеру или электронной почте), который отвечает за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В общем, как при пожаре, нужно знать, куда звонить, и что делать до приезда пожарной команды.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием выявить нарушителя. В ПБ организации приоритеты действий, совершаемых во время инцидента, должны быть расставлены заранее. Шкала приоритетов может выглядеть следующим образом:

- защита жизни и здоровья людей;
- защита секретных и/или критически важных данных;
- защита прочих данных, включая частную, научную и управленческую информацию;
- предотвращение повреждения систем;
- минимизация урона, нанесенного вычислительным ресурсам.

Идентификации инцидента сопутствует выяснение его масштабов и возможных последствий, а для эффективного противодействия важно правильно определить его границы. Кроме того, оценка возможных последствий позволит установить приоритеты при выделении ресурсов для принятия ответных мер.

Чтобы найти нарушителя, нужно заранее выяснить контактные координаты поставщика сетевых услуг и договориться с ним о самой возможности и порядке выполнения соответствующих действий. Чтобы предотвратить повторные нарушения, необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники вредоносного ПО? Какие пользователи имеют обыкновение выбирать слабые пароли? На подобные вопросы и должны дать ответ результаты анализа.

Необходимо отслеживать появление новых уязвимых мест и как можно быстрее ликвидировать ассоциированные с ними окна опасности. Кто-то в организации должен курировать этот процесс, принимать краткосрочные меры и корректировать программу безопасности для принятия долгосрочных мер.

Враждебные акции, будь то нападение внешних злоумышленников или месть обиженного сотрудника, необходимо предусмотреть заранее. Ничто не может заменить предварительно составленного плана восстановительных работ. В разделах политики безопасности, касающихся реакции на инциденты, должны быть освещены следующие темы:

- обзор (цели, преследуемые ПБ в плане реакции на инциденты);
- оценка (насколько серьезно произошедшее событие);
- извещение (кого следует известить о нем);
- ответные меры (что следует предпринять в ответ);
- правовой аспект (каковы правовые последствия случившегося);

- регистрационная документация (что следует фиксировать до, во время и после инцидента).

Когда есть уверенность, что нарушение режима безопасности действительно имеет место, следует известить соответствующий персонал. Чтобы удержать события под контролем и с технической, и с эмоциональной точек зрения, очень важно, кто и как будет извещен.

Любое сообщение об инциденте должно быть внятным, любая фраза - ясной, точной и полной. Попытки скрыть отдельные моменты, сообщая ложную или неполную информацию, способны не только помешать принятию эффективных ответных мер, но и привести к ухудшению ситуации.

Меры, предпринимаемые для борьбы с нарушением, можно подразделить на основные категории:

сдерживание;

ликвидация;

восстановление;

анализ.

Цель сдерживания - ограничить атакуемую область. Например, как можно быстрее приостановить распространение червя в сети.

Когда задача сдерживания решена, можно приступать к ликвидации. В этом поможет программный инструментарий (в частности, антивирусные пакеты).

После ликвидации атаки наступает время восстановления, т. е. приведения системы в нормальное состояние. Следует предпринять по крайней мере следующие действия:

произвести переучет системных активов, т. е. тщательно проверить состояние систем;

отразить уроки, извлеченные из инцидента, в пересмотренной программе обеспечения безопасности, чтобы не допустить повторения аналогичного нарушения;

произвести новый анализ риска с учетом полученной информации;

начать следствие против виновников инцидента, если это признано необходимым.

Устранить все уязвимые места, сделавшие возможным нарушение режима безопасности, непросто, но необходимо. Ключевым моментом здесь является понимание механизма вторжения.

При восстановлении, возможно, придется вернуться к начальному состоянию системы с последующей ее настройкой. Чтобы облегчить действия даже в таком, наихудшем, случае, целесообразно хранить записи о начальных установках и обо всех внесенных изменениях.

Анализ – одна из самых важных стадий реакции на инциденты, о которой, тем не менее, почти всегда забывают. Она важна потому, что позволяет всем причастным лицам извлечь поучительные уроки, чтобы в будущем в аналогичных ситуациях действовать эффективнее.

Требуется получить ответы по крайней мере на следующие вопросы:

Что именно и когда произошло?

Насколько хорошо сработал персонал?

Какая срочная информация понадобилась в первую очередь, и что способствовало ее скорейшему получению?

Что в следующий раз нужно делать по-другому?

После восстановления системы в ней нередко остаются уязвимости или даже ловушки. На фазе анализа система должна быть тщательно обследована, чтобы выявить проблемы, упущенные при восстановлении. В качестве отправной точки разумно воспользоваться программными средствами контроля защищенности.

Целесообразно документировать все детали, связанные с инцидентом: способы его обнаружения, процедуры исправления ситуации, процедуры мониторинга и усвоенные уроки. Детальное документирование в конечном итоге ведет к экономии времени, позволяет оценить размер нанесенного ущерба.

Планирование восстановительных работ

Ни одна организация не застрахована от серьезных аварий, вызванных естественными причинами, действиями злоумышленника, халатностью или некомпетентностью. В то же время, у каждой организации есть функции, которые руководство считает критически важными, они должны выполняться несмотря ни на что. Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объеме.

Отметим, что меры информационной безопасности можно разделить на три группы, в зависимости от того, направлены ли они на предупреждение, обнаружение или ликвидацию последствий атак. Большинство мер носит предупредительный характер. Оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения (так называемый активный аудит) служат для обнаружения и отражения атак. Планирование восстановительных работ, очевидно, можно отнести к последней из трех перечисленных групп.

Процесс планирования восстановительных работ можно разделить на следующие этапы:

выявление критически важных функций организации, установление приоритетов;

идентификация ресурсов, необходимых для выполнения критически важных функций;

определение перечня возможных аварий;

разработка стратегии восстановительных работ;

подготовка к реализации выбранной стратегии;

проверка стратегии.

Планируя восстановительные работы, следует отдавать себе отчет в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет свое лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить работу после аварии.

Идентифицируя ресурсы, необходимые для выполнения критически важных функций, следует помнить, что многие из них имеют некомпьютерный характер. На данном этапе желательно подключать к работе специалистов разного профиля, способных в совокупности охватить все аспекты проблемы. Критичные ресурсы обычно относятся к одной из следующих категорий:

персонал;

информационная инфраструктура;

физическая инфраструктура.

Составляя списки ответственных специалистов, следует учитывать, что некоторые из них могут непосредственно пострадать от аварии (например, от пожара), кто-то может находиться в состоянии стресса, часть сотрудников, возможно, будет лишена возможности попасть на работу (например, в случае массовых беспорядков). Желательно иметь некоторый резерв специалистов или заранее определить каналы, по которым можно на время привлечь дополнительный персонал.

Информационная инфраструктура включает в себя элементы, описанные в пункте «идентификация активов».

Нужно подготовиться к тому, что на «запасном аэродроме», куда организация будет эвакуирована после аварии, аппаратная платформа может отличаться от исходной. Соответственно, следует продумать меры поддержания совместимости по программам и данным.

Среди внешних информационных сервисов для коммерческих организаций, вероятно, важнее всего получить оперативную информацию и связь с государственными службами, курирующими данный сектор экономики.

Документация важна хотя бы потому, что не вся информация, с которой работает организация, представлена в электронном виде. Скорее всего, план восстановительных работ напечатан на бумаге.

К физической инфраструктуре относятся здания, инженерные коммуникации, средства связи, оргтехника и многое другое. Компьютерная техника не может работать в плохих условиях, без стабильного электропитания и т.п.

Анализируя критичные ресурсы, целесообразно учесть временной профиль их использования. Большинство ресурсов требуются постоянно, но в некоторых нужда может возникать только в определенные периоды (например, в конце месяца или года при составлении отчета).

При определении перечня возможных аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут оказаться масштабы бедствия? Что произойдет с критичными ресурсами? Например, смогут ли сотрудники попасть на работу? Будут ли выведены из строя компьютеры? Возможны ли случаи саботажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

Стратегия восстановительных работ должна базироваться на наличных ресурсах и быть не слишком накладной для организации. При разработке стратегии целесообразно провести анализ рисков, которым подвергаются критичные функции, и попытаться выбрать наиболее экономичное решение.

Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в выработке плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточности критичных ресурсов. Последнее возможно и без большого расхода средств, если заключить с одной или несколькими организациями соглашения о взаимной поддержке в случае аварий – те, кто не пострадал, предоставляют часть своих ресурсов во временное пользование менее удачливым партнерам.

Избыточность обеспечивается также мерами резервного копирования, хранением копий в нескольких местах, представлением информации в разных видах (на бумаге и в файлах) и т.д. Имеет смысл заключить соглашение с поставщиками информационных услуг о первоочередном обслуживании в критических ситуациях или заключать соглашения с несколькими поставщиками. Правда, эти меры могут потребовать определенных расходов.

Проверка стратегии производится путем анализа подготовленного плана, принятых и намеченных мер.

6.4. Программно-технический уровень

В предыдущих разделах по практические мероприятиям построения интегрированной системы информационной были освещены законодательный, административный и процедурный уровни системы ОБИ. Последний уровень формирования защищенной информационной системы отвечает за выработку

программно-технических мер и, соответственно, носит название *программно-технического уровня*.

Работа на данном уровне заключаются в выборе механизмов (подсистем) и средств ОБИ, рисунок 6.3.

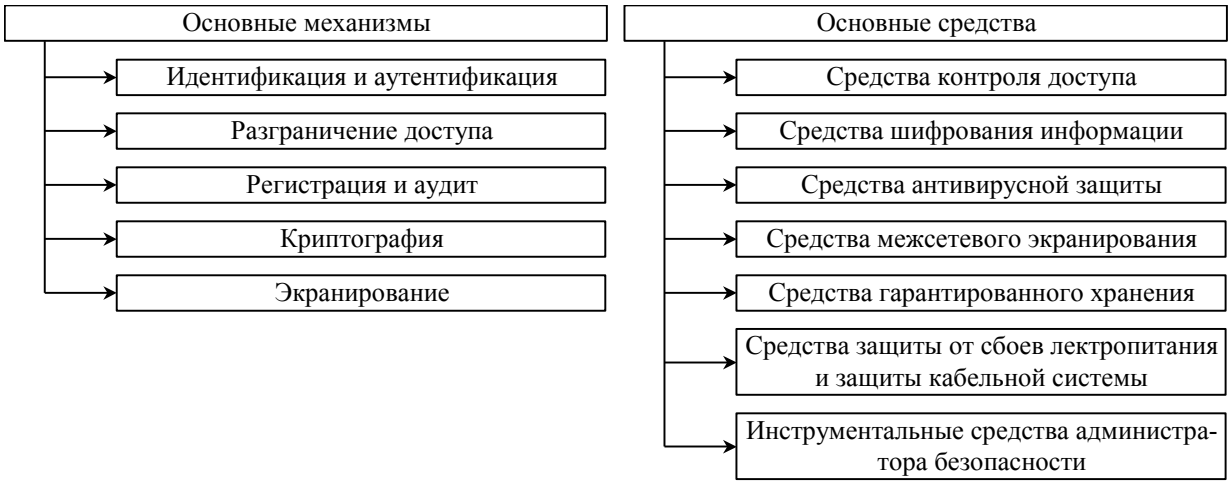


Рис. 6.3. Основные механизмы и средства интегрированной системы информационной безопасности предприятия

Далее рассмотрим более подробно представленные механизмы и средства.

6.4.1. Идентификация и аутентификация

Основой систем ОБИ являются идентификация и аутентификация, так как все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами АС. В качестве *субъектов* АС могут выступать как пользователи, так и процессы, а в качестве *объектов* АС – информация и другие информационные ресурсы системы.

Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется *идентификацией. Идентификатор пользователя* – некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют *именем* пользователя или *именем учетной записи* пользователя. Идентификация обеспечивает выполнение следующих функций ОБИ [2]:

установление подлинности и определение полномочий субъекта при его допуске в систему,

контролирование установленных полномочий в процессе сеанса работы;

регистрация действий и др.

Аутентификацией (*установлением подлинности)* называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Процедура аутентификации

Общая процедура идентификации и аутентификации пользователя при его доступе в АС представлена на рисунке 6.4. Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия

(совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

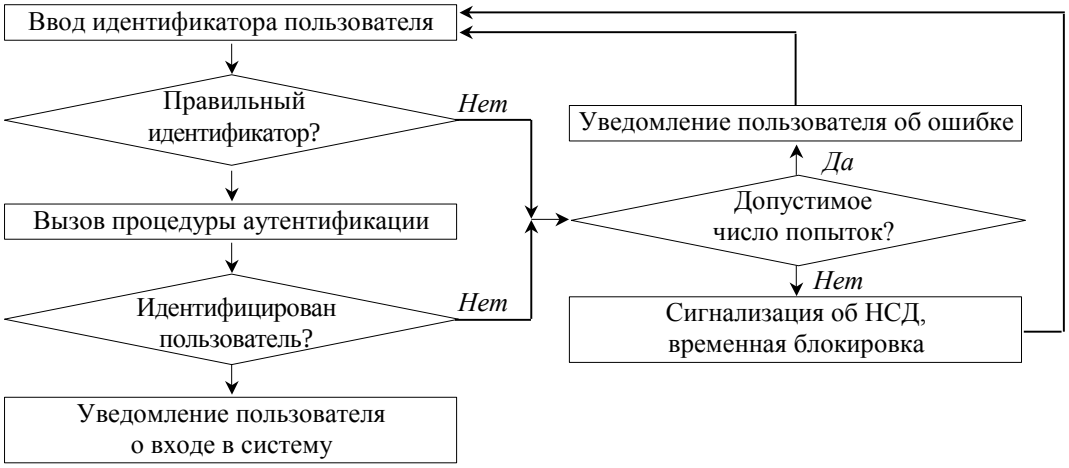


Рис. 6.4. Классическая процедура идентификации и аутентификации

Классификация систем аутентификации

Классифицировать системы аутентификации можно по различным признакам, рисунок 6.5.

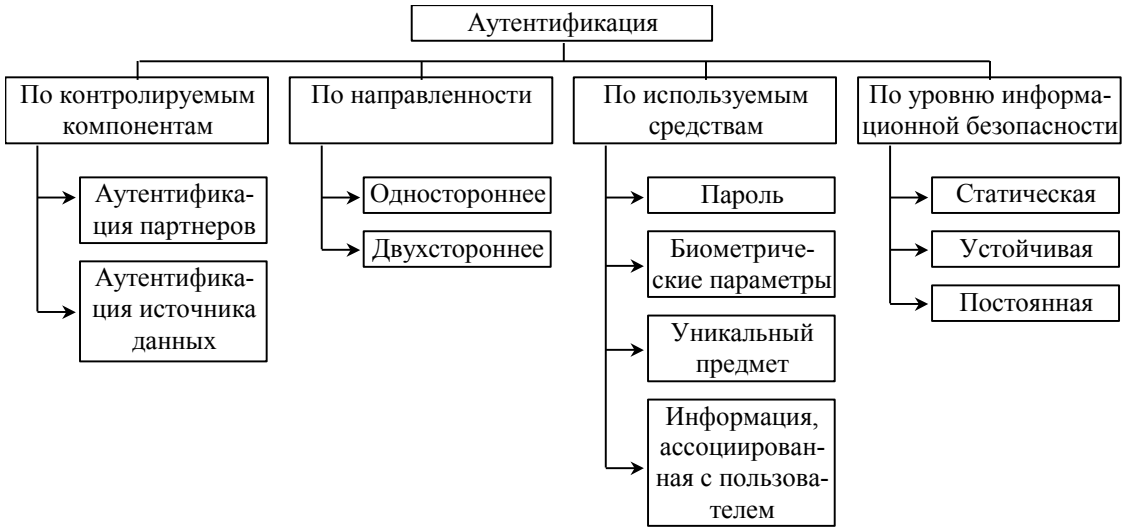


Рис. 6.5.

По *контролируемому компоненту* системы способы аутентификации можно разделить на аутентификацию партнеров по общению и аутентификацию источника данных. *Аутентификация партнеров* по общению используется при установлении (и периодической проверке) соединения во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. *Аутентификация источника данных* – это подтверждение подлинности источника отдельной порции данных.

По *направленности* аутентификация может быть *односторонней* (пользователь доказывает свою подлинность системе, например при входе в систему) и *двусторонней* (взаимной).

Обычно методы аутентификации классифицируют по *используемым средствам*. В этом случае указанные методы делят на четыре группы:

Основанные на знании лицом, имеющим право на доступ к ресурсам системы, некоторой *секретной информации – пароля*.

Основанные на использовании *уникального предмета*: жетона, электронной карточки и др.

Основанные на измерении *биометрических параметров человека* – физиологических или поведенческих атрибутах живого организма.

Основанные на *информации, ассоциированной с пользователем*, например с его координатами.

Рассмотрим эти группы подробнее.

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

Парольные методы следует классифицировать по степени изменяемости паролей:

методы, использующие постоянные (многократно используемые) пароли,

методы, использующие одноразовые (динамично изменяющиеся) пароли.

В большинстве АС используются многоразовые пароли. В этом случае пароль пользователя не изменяется от сеанса к сеансу в течение установленного администратором системы времени его действительности. Это упрощает процедуры администрирования, но повышает угрозу рассекречивания пароля. Известны множество способов вскрытия пароля: от подсмотра через плечо до перехвата сеанса связи. Вероятность вскрытия злоумышленником пароля повышается, если пароль несет смысловую нагрузку (год рождения, имя девушки), небольшой длины, набран на одном регистре, не имеет ограничений на период существования и т.д. Важно, разрешено ли вводить пароль только в диалоговом режиме или есть возможность обращаться из программы. В последнем случае, возможно запустить программу по подбору паролей. Более надежный способ – использование одноразовых или динамически меняющихся паролей. Известны следующие методы парольной защиты, основанные на одноразовых паролях:

методы модификации схемы простых паролей;

методы «запрос-ответ»;

функциональные методы.

В первом случае пользователю выдается список паролей. При аутентификации система запрашивает у пользователя пароль, номер в списке которого определен по случайному закону. Длина и порядковый номер начального символа пароля тоже могут задаваться случайным образом.

При использовании метода «запрос-ответ» система задает пользователю некоторые вопросы общего характера, правильные ответы на которые известны только конкретному пользователю.

Функциональные методы основаны на использовании специальной функции парольного преобразования F(X). Это позволяет обеспечить возможность изменения (по некоторой формуле) паролей пользователя во времени. Указанная функция должна удовлетворять следующим требованиям:

для заданного пароля X легко вычислить новый пароль Y = F(X);

зная X и Y, сложно или невозможно определить функцию F(X).

Наиболее известными примерами функциональных методов являются: метод функционального преобразования и метод “рукопожатия”.

Идея метода функционального преобразования состоит в периодическом изменении самой функции F(X). Последнее достигается наличием в функциональном выражении динамически меняющихся параметров, например функции от некоторой даты и времени. Пользователю сообщается исходный пароль, собственно функция и периодичность смены пароля. Нетрудно видеть, что паролями пользователя на заданных n-периодах времени будут следующие: X, F(X), F(F(X)), ... $F(X)^{n-1}$.

Метод “рукопожатия” состоит в следующем. Функция парольного преобразования известна только пользователю и системе защиты. При входе в АС подсистема аутентификации генерирует случайную последовательность X, которая передается пользователю. Пользователь вычисляет результат функции Y= F(X) и возвращает его в систему. Система сравнивает собственный вычисленный результат с полученным от пользователя. При совпадении указанных результатов подлинность пользователя считается доказанной.

Достоинством метода является то, что передача какой-либо информации, которой может воспользоваться злоумышленник, здесь сведена к минимуму.

В ряде случаев пользователю может оказаться необходимым проверить подлинность другого удаленного пользователя или некоторой АС, к которой он собирается осуществить доступ. Наиболее подходящим здесь является метод «рукопожатия», так как никто из участников информационного обмена не получит никакой конфиденциальной информации.

Отметим, что методы аутентификации, основанные на одноразовых паролях, также не обеспечивают абсолютной защиты. Например, если злоумышленник имеет возможность подключения к сети и перехватывать передаваемые пакеты, то он может посылать последние как собственные.

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

Карточки разделяют на два типа:

пассивные (карточки с памятью);

активные (интеллектуальные карточки).

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

Иногда (обычно для физического контроля доступа) карточки применяют сами по себе, без запроса личного идентификационного номера.

К *достоинству* использования карточек относят то, что обработка аутентификационной информации выполняется устройством чтения, без передачи в память компьютера. Это исключает возможность электронного перехвата по каналам связи.

Недостатки пассивных карточек следующие: они существенно дороже паролей, требуют специальные устройства чтения, их использование подразумевает специальные процедуры безопасного учета и распределения. Их также необходимо оберегать от злоумышленников, в первую очередь, естественно, не оставлять в устройствах. Известны случаи подделки пассивных карточек.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, как-то: многоразовые пароли, динамически меняющиеся пароли, обычно “запрос – ответные” методы. Все карточки обеспечивают двухкомпонентную аутентификацию.

К указанным достоинствам интеллектуальных карточек следует добавить их многофункциональность. Их можно применять не только для целей безопасности, но и, например, для финансовых операций. Сопутствующим недостатком карточек является их высокая стоимость.

3. Методы аутентификации, основанные на измерении *биометрических параметров* человека, обеспечивают почти 100%-ую идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться (имеются проблемы со стандартизацией и распространением), требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах и системах, главным образом в МО РФ.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, формам ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и даже по ДНК рисунок 6.6.

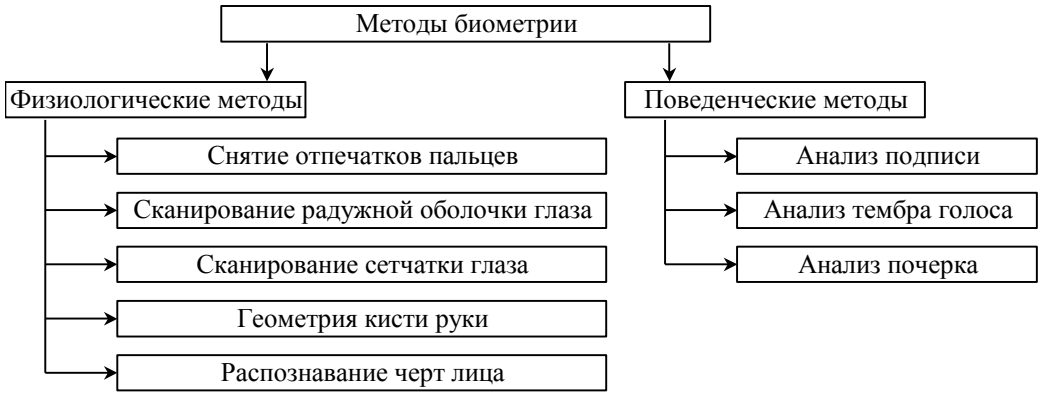


Рис. 6.6. Примеры распространенных методов биометрии

Новым направлением является использование биометрических характеристик в интеллектуальных расчетных карточках, жетонах-пропусках и элементах сотовой связи. Например, при расчете в магазине предъявитель карточки кладет палец на сканер в подтверждение, что карточка действительно его.

Назовем наиболее используемые биометрические атрибуты и соответствующие системы.

Отпечатки пальцев. Такие сканеры имеют небольшой размер, универсальны, относительно недороги. Биологическая повторяемость отпечатка пальца составляет 10^{-5}%. В настоящее время пропагандируются правоохранительными органами из-за крупных ассигнований в электронные архивы отпечатков пальцев.

Геометрия руки. Соответствующие устройства используются, когда из-за грязи или травм трудно применять сканеры пальцев. Биологическая повторяемость геометрии руки около 2-х %.

Радужная оболочка глаза. Данные устройства обладают наивысшей точностью. Теоретическая вероятность совпадения двух радужных оболочек составляет 1 из 10^{78}.

Термический образ лица. Системы позволяют идентифицировать человека на расстоянии до десятков метров. В комбинации с поиском данных по базе данных такие системы используются для опознания авторизованных сотрудников и отсеивания посторонних. Однако при изменении освещенности сканеры лица имеют относительно высокий процент ошибок.

Голос. Проверка голоса удобна для использования в телекоммуникационных приложениях. Необходимые для этого 16-разрядная звуковая плата и конденсаторный микрофон стоят менее 25 $. Вероятность ошибки составляет 2-5%. Данная технология подходит для верификации по голосу по телефонным каналам связи, она более надежна по сравнению с частотным набором личного номера. Сейчас развиваются направления идентификации личности и его состояния по голосу — возбужден, болен, говорит правду, не в себе и т.д.

Ввод с клавиатуры. Здесь при вводе, например, пароля отслеживаются скорость и интервалы между нажатиями.

Подпись. Для контроля рукописной подписи используются дигитайзеры.

4. Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что сводит на нет их перехват. В данном случае, есть мнение, что изящная территориально-распределенная атака на компьютерные системы под силу лишь программистам Ракетно-Космических Сил.

Аппаратура GPS проста и надежна в использовании и сравнительно недорога. Это позволяет ее использовать в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Суммируя возможности средств аутентификации, ее можно классифицировать по уровню информационной безопасности на три категории:

Статическая аутентификация;

Устойчивая аутентификация;

Постоянная аутентификация.

Первая категория обеспечивает защиту только от НСД в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Для компрометации статической аутентификации нарушитель может подсмотреть, подобрать, угадать или перехватить аутентификационные данные и т.д.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Усиленная аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и силиться использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

6.4.2. Разграничение доступа

После выполнения идентификации и аутентификации необходимо установить полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования вычислительных ресурсов, доступных в АС. Такой процесс называется *разграничением (логическим управлением) доступа*.

Обычно полномочия субъекта представляются: списком ресурсов, доступным пользователю, и правами по доступу к каждому ресурсу из списка. В качестве вычислительных ресурсов могут быть программы, информация, логические устройства, объем памяти, время процессора, приоритет и т.д.

Можно выделить следующие методы разграничения доступа:

разграничение доступа по спискам,

использование матрицы установления полномочий,

разграничения доступа по уровням секретности и категориям,

парольное разграничение доступа.

Рассмотрим подробнее приведенные методы разграничения доступа.

1. При *разграничении доступа по спискам* задаются соответствия:

каждому пользователю — список ресурсов и прав доступа к ним;

каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в большинстве ОС и СУБД.

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

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

3. *Разграничения доступа по уровням секретности и категориям* состоят в том, что ресурсы АС разделяются в соответствии с уровнями секретности или категорий.

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

При разграничении по категориям задается и контролируется ранг категории, соответствующей пользователю. Соответственно, все ресурсы АС декомпозируют по уровню важности, причем определенному уровню соответствует некоторый ранг персонала (типа: руководитель, администратор, пользователь).

4. *Парольное разграничение*, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты.

Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

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

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

дискретное управление доступом,

мандатное управление доступом.

Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

Мандатное управление доступом — разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. Иначе, для реализации мандатного управления доступом каждому субъекту и каждому объекту присваивают классификационные метки, отражающие их место в соответствующей иерархии. С помощью этих меток субъектам и объектам должны быть назначены классификационные уровни, являющиеся комбинациями уровня иерархической классификации и иерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа. Ясно, что методы разграничения доступа по уровням секретности и категориям являются примерами мандатного управления доступом.

Ролевое управление доступом

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

Таким решением является *ролевое управление доступом* (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – *роли*. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (рисунок 6.7).

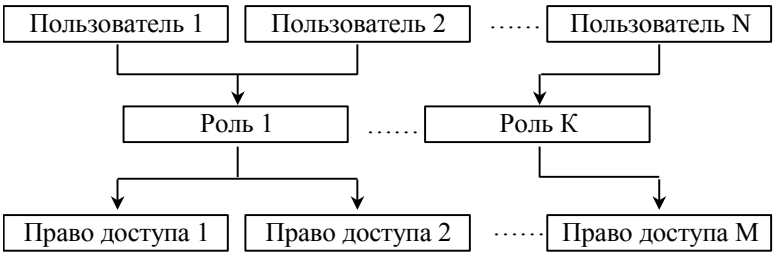


Рис. 6.7. Пользователи, объекты и роли.

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

установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно.

Ролевой доступ развивается более 10 лет (сама идея ролей, разумеется, значительно старше) как на уровне операционных систем, так и в рамках СУБД и других информационных сервисов. В частности, существуют реализации ролевого доступа для Web-серверов.

В 2001 году Национальный институт стандартов и технологий США предложил проект стандарта ролевого управления доступом, основные положения которого приведены ниже.

Ролевое управление доступом оперирует следующими основными понятиями:

пользователь (человек, интеллектуальный автономный агент и т.п.);

сеанс работы пользователя;

роль (обычно определяется в соответствии с организационной структурой);

объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);

операция (зависит от объекта: для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п.);

право доступа (разрешение выполнять определенные операции над определенными объектами).

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

Между ролями может быть определено отношение частичного порядка, называемое *наследованием*. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1. *Наследование ролей* соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям – объекты (экземпляры) классов.

Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить себе формирование *иерархии ролей***,** начиная с минимума прав (и максимума пользователей), приписываемых роли «сотрудник», с постепенным уточнением состава пользователей и добавлением прав (роли «системный администратор», «бухгалтер» и т.п.), вплоть до роли «руководитель» (что, впрочем, не значит, что руководителю предоставляются неограниченные права, как и другим ролям, в соответствии с принципом *минимизации привилегий*, этой роли целесообразно разрешить только то, что необходимо для выполнения служебных обязанностей).

Существует масса принципов информационной безопасности, в частности *разделение обязанностей*, причем в двух видах: статическом и динамическом.

Статическое разделение обязанностей налагает ограничения на приписывание пользователей ролям. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара «множество ролей – число» (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан указанному (или большему) числу ролей из заданного множества.

Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь 3).

При наличии наследования ролей ограничение приобретает несколько более сложный вид, но суть остается простой: при проверке членства в ролях нужно учитывать приписывание пользователей ролям-наследницам.

Динамическое разделение обязанностей отличается от статического только тем, что рассматриваются роли, одновременно активные (быть может, в разных сеансах) для данного пользователя, а не те, которым пользователь статически приписан. Например, один пользователь может играть роль и кассира, и контролера, но не одновременно; чтобы стать контролером, он должен сначала закрыть кассу. Тем самым реализуется так называемое *временное ограничение доверия*, являющееся аспектом минимизации привилегий.

Рассматриваемый проект стандарта содержит спецификации трех категорий функций, необходимых для администрирования РУД:

Административные функции (создание и сопровождение ролей и других атрибутов ролевого доступа): создать/удалить роль/пользователя, приписать пользователя/право роли или ликвидировать существующую ассоциацию, создать/удалить отношение наследования между существующими ролями, создать новую роль и сделать ее наследницей/предшественницей существующей роли, создать/удалить ограничения для статического/динамического разделения обязанностей.

Вспомогательные функции (обслуживание сеансов работы пользователей): открыть сеанс работы пользователя с активацией подразумеваемого набора ролей; активировать новую роль, деактивировать роль; проверить правомерность доступа.

Информационные функции (получение сведений о текущей конфигурации с учетом отношения наследования). Здесь проводится разделение на обязательные и необязательные функции. К числу первых принадлежат получение списка пользователей, приписанных роли, и списка ролей, которым приписан пользователь.

Все остальные функции отнесены к разряду необязательных. Это получение информации о правах, приписанных роли, о правах заданного пользователя (которыми он обладает как член множества ролей), об активных в данный момент сеанса ролях и правах, об операциях, которые роль/пользователь правомочны совершить над заданным объектом, о статическом/динамическом разделении обязанностей.

6.4.3. Регистрация и аудит

Регистрация (или протоколирование) представляет собой механизм подотчетности системы ОБИ, фиксирующий все события, касающиеся безопасности, такие как: вход и выход субъектов доступа, запуск и завершение программ, выдача печатных документов, попытки доступа к защищаемым ресурсам, изменение полномочий субъектов доступа и статуса объектов доступа и т.д.

Эффективность системы ОБИ принципиально повышается в случае дополнения регистрации *аудитом* — анализом протоколируемой информации. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защите, анализировать закономерности системы, оценивать работу пользователей и т.д.

Реализация механизма регистрации и аудита преследует следующие цели:

обеспечение подотчетности пользователей и администраторов;

обеспечение возможности реконструкции последовательности событий;

обнаружение попыток нарушений информационной безопасности;

предоставление информации для выявления и анализа проблем.

Кроме того, механизм регистрации и аудита является психологическим средством, напоминающим потенциальным нарушителям о неотвратимости возмездия за проступки и оплошности.

Практическими средствами регистрации и аудита могут быть следующие:
различные системные утилиты и прикладные программы,
регистрационный (системный или контрольный) журнал.

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

Регистрационный журнал — это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата. Типовая запись регистрационного журнала включает в себя:

тип записи,
дата,
время,
терминал,
пользователь,
событие,
результат.

Процесс ведения регистрационного журнала состоит из четырех этапов:
Сбор и хранение;
Защита;
Интеграция;
Анализ.

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

Регистрируемые данные должны быть защищены, в первую очередь от несанкционированной модификации и, возможно, раскрытия. Дополнительные требования по безопасности определяются концентрацией информации обо всей АС, множеством сегментов АС с различными уровнями доступа, разницей зон административной ответственности и др.

Этап интеграции необходим для объединения и согласования форматов регистрируемых данных из различных систем. Некоторые системы не имеют механизмов контроля и регистрации данных. Возможно, здесь придется разработать программы дополнительного контроля данных и программы трансформации данных в единый формат.

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

Статистические методы. Здесь накапливается среднестатистические параметры функционирования подсистем (исторический профиль трафика) и сравниваются с текущими. Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз. Например, так выявляются: сбои в работе сервера из-за лавинного потока запросов, быстро распространяемый компьютерный вирус, нарушитель, маскирующиеся под легального пользователя, но ведущий себя иначе («маскарад») и др.

Эвристические методы. В данном случае в логических правилах системы поддержки принятия решений закодированы известные сценарии НСД, характеристики наблюдаемой системы, сигнализирующие о нарушениях, или модели действий, по совокупности приводящие к НСД. Понятно, что данные методы идентифицируют только известные угрозы, определенные в базе знаний системы поддержки принятия решений.

Аудиту информационной безопасности посвящен второй раздел работы (см. ниже).

6.4.4. Криптография

В этом пункте будут рассмотрены криптографические сервисы безопасности, точнее, элементарные сведения, помогающие составить общее представление о компьютерной криптографии и ее месте в общей архитектуре информационных систем.

Криптография необходима для реализации, по крайней мере, трех сервисов безопасности:

шифрование;

контроль целостности;

аутентификация (этот сервис был рассмотрен ранее).

Шифрование

Шифрование – наиболее мощное средство обеспечения конфиденциальности. Во многих отношениях оно занимает центральное место среди программно-технических регуляторов безопасности, являясь основой реализации многих из них, и в то же время последним (а подчас и единственным) защитным рубежом. Например, для портативных компьютеров только шифрование позволяет обеспечить конфиденциальность данных даже в случае кражи.

В большинстве случаев и шифрование, и контроль целостности играют глубоко инфраструктурную роль, оставаясь прозрачными и для приложений, и для пользователей. Типичное место этих сервисов безопасности – на сетевом и транспортном уровнях реализации стека сетевых протоколов.

Различают два основных метода шифрования:

симметричный,

асимметричный.

При *симметричном* шифровании один и тот же ключ (хранящийся в секрете) используется и для зашифрования, и для расшифрования данных. Разработаны весьма эффективные (быстрые и надежные) методы симметричного шифрования. Национальный стандарт на подобные методы – ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это создает новую проблему распространения ключей. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно.

В *асимметричных* методах используются два ключа. Один из них, несекретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) – для расшифрования. Самым популярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями.

Существенным недостатком асимметричных методов шифрования является их низкое быстродействие, поэтому данные методы приходится сочетать с симметричными (асимметричные методы на 3 – 4 порядка медленнее). Так, для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети [3].

Контроль целостности

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких как поток сообщений); определять подлинность источника данных; гарантировать невозможность отказаться от совершенных действий – «неотказуемость».

В основе криптографического контроля целостности лежат два понятия:

хэш-функция;

электронная цифровая подпись (ЭЦП).

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

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый дайджест). Обозначим хэш-функцию через h, исходные данные – через T, проверяемые данные – через T'. Контроль целостности данных сводится к проверке равенства h(T') = h(T). Если оно выполнено, считается, что T' = T. Совпадение дайджестов для различных данных называется коллизией. В принципе, коллизии, конечно, возможны, поскольку мощность множества дайджестов меньше, чем мощность множества хэшируемых данных, однако то, что h есть функция односторонняя, означает, что за приемлемое время специально организовать коллизию невозможно.

Два российских стандарта, ГОСТ Р 34.10-94 «Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» и ГОСТ Р 34.11-94 «Функция хэширования», объединенные общим заголовком «Информационная технология. Криптографическая защита информации», регламентируют вычисление дайджеста и реализацию ЭЦП. В сентябре 2001 года был утвержден, а 1 июля 2002 года вступил в силу новый стандарт ЭЦП – ГОСТ Р 34.10-2001, разработанный специалистами ФАПСИ.

6.4.5. Экранирование

Механизмом обеспечения целостности данных в информационно-вычислительных сетях является *экранирование*, выполняющее функции разграничения информационных потоков на границе защищаемой сети. С одной стороны, это повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды. Указанное уменьшает уязвимость внутренних объектов потому, что сторонний нарушитель должен преодолеть некоторый защитный барьер — *межсетевой экран*, в котором механизмы ОБИ сконфигурированы особо тщательно и жестко. С другой стороны, экранирование позволяет контролировать информационные потоки, исходящие во внешнюю среду, что повышает режим конфиденциальности АС. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет *межсетевой экран* или *брандмауэр* (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в АС и/или выходящих из АС, и обеспечивает защиту АС посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее распространении в/из АС.

В общем случае межсетевой экран выполняет свои функции, контролируя все информационные потоки между двумя сегментами сети или сетями.

Межсетевые экраны классифицируют следующим образом:

на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети,

по уровню фильтрации, соответствующему эталонной модели OSI/ ISO.

Говоря о внешних и внутренних сетевых экранах, следует отметить следующее. *Внешние* обычно имеют дело только с протоколом TCP/IP сети Internet. Для *внутренних* сетевых экранов может иметь место многопротокольность.

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI (таблица 6.4). Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

межсетевые экраны с фильтрацией пакетов;

шлюзы сеансового уровня;

шлюзы прикладного уровня;

межсетевые экраны экспертного уровня.

Таблица 6.4. Типы межсетевых экранов и уровни модели ISO/OSI

Уровень модели OSI	Протоколы Internet	Тип межсетевого экрана
Прикладной	Telnet, FTP, DNS, NFS, PING, SMTP, HTTP	Шлюз прикладного уровня Межсетевой экран экспертного уровня
Представления данных		
Сеансовый	TCP, UDP	Шлюз сеансового уровня
Транспортный	TCP, UDP	
Сетевой	IP, ICMP	Межсетевой экран с фильтрацией пакетов
Канальный		
Физический		

1. *Межсетевые экраны с фильтрацией пакетов* (packet-filtering firewall) представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их с сконфигурированной таблицей правил.

Данные системы просты в использовании, дешевы, оказывают минимальное влияние на производительность АС. Основным недостатком является их уязвимость для IP-спуфинга - замены адресов IP. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

2. *Шлюзы сеансового уровня* (circuit-level gateway) контролируют допустимость *сеанса* связи. Они следят за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функции трансляции сетевых адресов, которая скрывает внутренние IP-адреса, т.е. исключают IP-спуфинг. Однако, т.к. системы контролируют пакеты только на сеансовом уровне, то и отсутствует контроль содержимого пакетов, генерируемых

различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

3. *Шлюзы прикладного уровня* (application-level gateway) проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип брандмауэра, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб Internet (HTTP, FTP, telnet и т.д.) и служат для проверки сетевых пакетов на наличие достоверных данных. Однако шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Internet из-за узости каналов связи, но существенно при работе во внутренней сети - Intranet. К недостаткам можно добавить необходимость (а значит и дополнительные временные и экономические затраты) в разработке новых программ-посредников при внедрении новой службы Internet.

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

Специфика указанных межсетевых экранов состоит в том, что для обеспечения защиты они перехватывают и анализируют каждый пакет на прикладном уровне модели OSI. Вместо применения связанных с приложениями программ-посредников, брандмауэры экспертного уровня используют *специальные алгоритмы распознавания и обработки данных* на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что, теоретически, должно обеспечить более эффективную фильтрацию пакетов.

Поскольку брандмауэры экспертного уровня допускают прямое соединение между авторизованным клиентом и внешним хостом, то они оказывают меньшее влияние на производительность, чем шлюзы прикладного уровня. Спорным остаются вопрос: обеспечивают они меньшую безопасность АС по сравнению со шлюзами прикладного уровня или нет [2].

6.4.6. Антивирусная защита

Известно, что нельзя добиться 100 %-ой защиты ПК от компьютерных вирусов отдельными программными средствами. Поэтому для уменьшения потенциальной опасности внедрения компьютерных вирусов и их распространения по корпоративной сети необходим комплексный подход, сочетающий различные административные меры, программно-технические средства антивирусной защиты, а также средства резервирования и восстановления. Делая акцент на программно-технических средствах, можно выделить три основных уровня антивирусной защиты:

Поиск и уничтожение известных вирусов.

Поиск и уничтожение неизвестных вирусов.

Блокировка проявления вирусов.

Поиск и уничтожение известных вирусов

При поиске и уничтожении известных вирусов наиболее распространенным является *метод сканирования*. Указанный метод заключается в выявлении компьютерных вирусов по их уникальному фрагменту программного кода (сигнатуре, программному штамму). Для этого создается некоторая *база данных сканирования* с фрагментами кодов известных компьютерных вирусов. Обнаружение вирусов осуществляется путем сравнения данных памяти компьютера с фиксированными кодами базы данных сканирования. В случае выявления и идентификации кода нового вируса, его сигнатура может быть введена в базу данных сканирования. В виду того, что сигнатура известна, то существует возможность корректного восстановления (обеззараживания) зараженных файлов и областей. Следует добавить, что некоторые системы хранят не сами сигнатуры, а, например, контрольные суммы или имитоприставки сигнатур.

Антивирусные программы, выявляющие известные компьютерные вирусы, называются *сканерами* или *детекторами*. Программы, включающие функции восстановления зараженных файлов, называют *полифагами* (фагами), докторами или дезинфекторами. Примером сканера-полифага является знакомая программа Aidstest.

Принято разделять сканеры на следующие:

транзитные, периодически запускаемые для выявления и ликвидации вирусов,

резидентные (постоянно находящиеся в оперативной памяти), проверяющие заданные области памяти системы при возникновении связанных с ними событий (например, проверка файла при его копировании или переименовании).

К недостаткам сканеров следует отнести то, что они позволяют обнаружить вирусы, которые уже проникали в вычислительные системы, изучены и для них определена сигнатура. Для эффективной работы сканеров необходимо оперативно пополнять базу данных сканирования. Однако с увеличением объема базы данных сканирования и числа различных типов искомых вирусов снижается скорость антивирусной проверки. Само собой, если время сканирования будет приближаться ко времени восстановления, то необходимость в антивирусном контроле может стать не столь актуальной.

Некоторые вирусы (мутанты и полиморфные) кодируют или видоизменяют свой программный код. Это затрудняет или делает невозможным выделить сигнатуру, а следовательно, обнаружить вирусы методом сканирования.

Для выявления указанных маскирующихся вирусов используются специальные методы. К ним можно отнести метод эмуляции процессора. Метод заключается в имитации выполнения процессором программы и подсовывания вирусу фиктивных управляющих ресурсов. Обманутый таким образом вирус, находящийся под контролем антивирусной программы, расшифровывает свой код. После этого, сканер сравнивает расшифрованный код с кодами из своей базы данных сканирования.

Поиск и уничтожение неизвестных вирусов

Выявление и ликвидация неизвестных вирусов необходимы для защиты от вирусов, пропущенных на первом уровне антивирусной защиты. Наиболее эффективным методом является контроль целостности системы (обнаружение изменений). Данный метод заключаются в проверке и сравнении текущих параметров вычислительной системы с эталонными, соответствующими ее незараженному состоянию. Понятно, что контроль целостности не являются прерогативой исключительно системы антивирусной защиты. Он обеспечивает защищенность информационного ресурса от несанкционированных модификации и удаления в результате различного рода нелегитимных воздействий, сбоев и отказов системы и среды.

Для реализации указанных функций используются программы, называемые *ревизорами*. Работа ревизора состоит из двух этапов: фиксирование эталонных характеристик вычислительной системы (в основном диска) и периодическое сравнение их с текущими характеристиками. Обычно контролируемыми характеристиками являются контрольная сумма, длина, время, атрибут “только для чтения” файлов, дерево каталогов, сбойные кластеры, загрузочные сектора дисков. В сетевых системах могут накапливаться среднестатистические параметры функционирования подсистем (в частности исторический профиль сетевого трафика), которые сравниваются с текущими.

Ревизоры, как и сканеры, делятся на транзитные и резидентные.

К недостаткам ревизоров, в первую очередь резидентных, относят создаваемые ими всякие неудобства и трудности в работе пользователя. Например, многие изменения параметров системы вызваны не вирусами, а работой системных программ или действиями пользователя-программиста. По этой же причине ревизоры не используют для контроля зараженности текстовых файлов, которые постоянно меняются. Таким образом, необходимо соблюдение некоторого баланса между удобством работы и контролем целостности системы.

Ревизоры обеспечивают высокий уровень выявления неизвестных компьютерных вирусов, однако они не всегда обеспечивают корректное лечение зараженных файлов. Для лечения зараженных файлов неизвестными вирусами обычно используются эталонные характеристики файлов и предполагаемые способы их заражения.

Кроме этого ревизоры не определяют зараженные файлы, создаваемые или копируемые в систему.

Разновидностью контроля целостности системы является метод программного самоконтроля, именуемые вакцинацией. Идея методов состоит в присоединении к защищаемой программе модуля (*вакцины*), контролирующего характеристики программы, обычно ее контрольную сумму.

Помимо статистических методов контроля целостности, для выявления неизвестных и маскирующихся вирусов используются эвристические методы. Они позволяет выявить по известным признакам (определенным в базе знаний системы) некоторые маскирующиеся или новые модифицированные вирусы известных типов. В качестве примера признака вируса можно привести код, устанавливающий резидентный модуль в памяти, меняющий параметры таблицы прерываний и др. Программный модуль, реализующий эвристический метод обнаружения вирусов, называют *эвристическим анализатором*.

К недостаткам эвристических анализаторов можно отнести ошибки 1-го и 2-го рода: ложные срабатывания и пропуск вирусов. Соотношение указанных ошибок зависит от уровня эвристики.

Понято, что если для обнаруженного эвристическим анализатором компьютерного вируса сигнатура отсутствует в базе данных сканирования, то лечение зараженных данных может быть некорректным.

Блокировка проявления вирусов

Блокировка проявления вирусов предназначена для защиты от деструктивных действий и размножения компьютерных вирусов, которым удалось преодолеть первые два уровня защиты. Методы основаны на перехвате характерных для вирусов функций. Известны два вида указанных антивирусных средства:

программы-фильтры,

аппаратные средства контроля.

Программы-фильтры, называемые также резидентными сторожами и мониторами, постоянно находятся в оперативной памяти и перехватывают заданные прерывания, с целью контроля подозрительной действий. При этом они могут блокировать “опасные” действия или выдавать запрос пользователю.

Действия, подлежащие контролю, могут быть следующими: модификация главной загрузочной записи (MBR) и загрузочных записей логических дисков и ГМД, запись по абсолютному адресу, низкоуровневое форматирование диска, оставление в оперативной памяти резидентного модуля и др. Как и ревизоры, фильтры часто являются “навязчивыми” и создают определенные неудобства в работе пользователя.

Встроенные аппаратные средства ПК обеспечивают контроль модификации системного загрузчика и таблицы разделов жесткого диска, находящихся в главном загрузочном секторе диска (MBR). Включение указанных возможностей в ПК осуществляется с помощью программы Setup, расположенной в ПЗУ. Следует указать, что программу Setup можно обойти в случае замены загрузочных секторов путем непосредственного обращения к портам ввода-вывода контроллеров жесткого и гибкого дисков.

Наиболее полная защита от вирусов может быть обеспечена с помощью специальных контроллеров аппаратной защиты. Такой контроллер подключается к ISA-шине ПК и на аппаратном уровне контролирует *все* обращения к дисковой подсистеме компьютера. Это не позволяет вирусам маскировать себя. Контроллер может быть сконфигурирован так, чтобы контролировать отдельные файлы, логические разделы, “опасные” операции и т.д. Кроме того, контроллеры могут выполнять различные дополнительные функции защиты, например, обеспечивать разграничение доступа и шифрование.

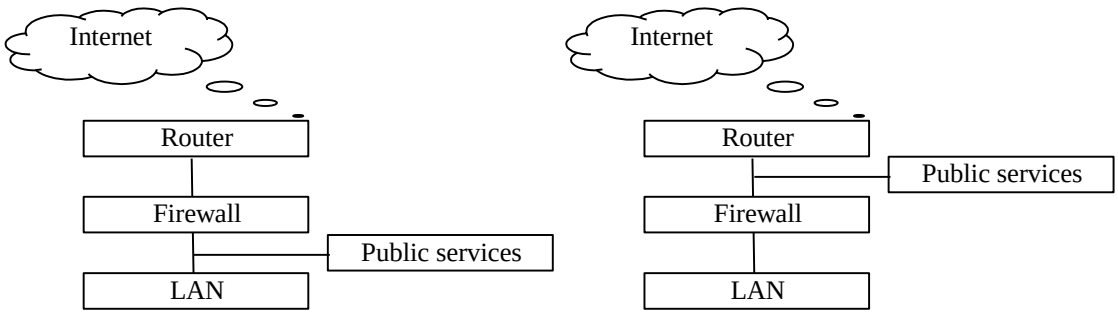
К недостаткам указанных контроллеров, как ISA-плат, относят отсутствие системы авто конфигурирования, и как следствие, возможность возникновения конфликтов с некоторыми системными программами, в том числе антивирусными [2].

6.5. Модель безопасности информационной сети предприятия

В данном разделе будет рассмотрен один из возможных вариантов построения защищенной информационной сети предприятия на базе компьютерного оборудования и программных средств.

Компьютерная сеть предприятия малого/среднего бизнеса включает в себя несколько локальных сетей объединенных в единую сеть организации и функционирующих как единое целое. Как правило, сеть включает в себя различного рода коммутационное оборудование, такое как маршрутизатор, хосты, коммутаторы, сетевые карты и т.д., а также всевозможные сервисы и программы.

Из предыдущего раздела известно, что в качестве первого рубежа защиты сети, от угроз из Internet, служит межсетевой экран. В общем случае существует два варианта постановки экрана в сеть, эти варианты приведены на рисунке 6.8.



а) Простое включение МЭ

б) Подключение МЭ с вынесением общедоступных серверов

Рис. 6.8. Варианты постановки МЭ в сеть

Наиболее простым является решение, при котором межсетевой экран просто экранирует локальную сеть от глобальной (6.8а). При этом публичные сервисы (Public services: WWW, FTP, e-mail) оказываются защищены межсетевым экраном. Требуется уделить много внимания на предотвращение проникновения на защищаемые станции локальной сети при помощи средств легкодоступных публичных серверов.

Для предотвращения доступа в локальную сеть, используя ресурсы публичных серверов, рекомендуется общедоступные серверы подключать перед межсетевым экраном, так как показано на рисунке 6.8б. Данный способ обладает более высокой защищенностью локальной сети, но низким уровнем защищенности общедоступных серверов.

Экскурс в технологию WWW. WWW представляет собой клиент-серверную технологию, основанную на прикладном протоколе HTTP. В нем имеется два вида сообщений: запросы от клиента к серверу и ответы сервера клиенту. Для передачи сообщений используется протокол TCP, стандартный порт HTTP-сервера – 80.

Очевидно, что не все информационные ресурсы WWW могут быть открыты для всеобщего просмотра. Для того чтобы ограничить доступ к какому-либо ресурсу, используется аутентификация клиента, т.е. клиент должен предоставить имя пользователя и пароль, прежде чем его пароль будет обслужен HTTP-сервером.

Почтовый сервис (e-mail) использует протоколы: SMPT (Simple Mail Transfer Protocol) и POP3 (Post Office Protocol).

Главной целью протокола SMTP служит надежная и эффективная доставка электронных почтовых сообщений. SMTP является довольно независимой системой и требует только надежного канала связи. Средой для SMTP может служить отдельная локальная сеть, система сетей или весь Internet.

SMTP базируется на следующей модели коммуникаций: в ответ на запрос пользователя почтовая программа-отправитель устанавливает двухстороннюю связь с программой-приемником (TCP, порт 25). Получателем может быть оконечный или промежуточный адресат. SMTP-команды генерируются отправителем и посылаются получателю. На каждую команду должен быть отправлен и получен отклик.

В некоторых небольших узлах Internet бывает непрактично поддерживать систему передачи сообщений MTS (Message Transport System). Рабочая станция может не иметь достаточных ресурсов для обеспечения непрерывной работы SMTP-сервера. Для “домашних ЭВМ” слишком дорого поддерживать связь с Internet круглые сутки.

POP3 обеспечивает доступ к электронной почте малых узлов и индивидуальных ЭВМ. Этот протокол обеспечивает доступ узла к базовому почтовому серверу. POP3 получает и стирает почтовые сообщения. Когда пользователь ЭВМ-клиента хочет послать сообщение, он устанавливает SMTP связь с почтовым сервером непосредственно и посылает все, что нужно через него. При этом ЭВМ POP3-сервер не обязательно является почтовым сервером. В исходный момент ЭВМ POP3-сервер прослушивает TCP-порт 110. Если ЭВМ-клиент хочет воспользоваться услугами POP3-сервера, то устанавливает с ним TCP связь. По установлении связи POP3-сервер посылает клиенту уведомление и сессия переходит в фазу авторизации. После этого может производиться обмен командами и откликами.

Преследуя своей целью защитить активы внутренней сети организации, а так же не загружать firewall – поставим экран после публичных сервисов.

Система защиты информации на уровне “периметра”, кроме межсетевого экрана, включает в себя такие защитные средства (Security services):

автоматизированное рабочее место администратора,

антивирусный шлюз,

сервер аудита безопасности системы,

средства адаптивного управления безопасностью ANS (Adaptive Network Security) и обнаружения атак IDS (Intrusion Detection System),

средства проверки почты,

и др.

В качестве внутреннего сервиса выступает сервис распределенных баз данных.

Разбивка сети на сегменты достигается за счет коммутатора (Switch), посредствам которого так же осуществляется доступ/запрет:

из одного локального сегмента в другой,

из внутренней сети к внутренним сервисам (например, к распределенной базе данных предприятия),

из внутренней сети к публичным сервисам,

из внутренней сети в Internet.

Благодаря коммутатору можно задавать любую политику безопасности.

Описанная структура информационной сети организации представлена на рисунке 6.9.

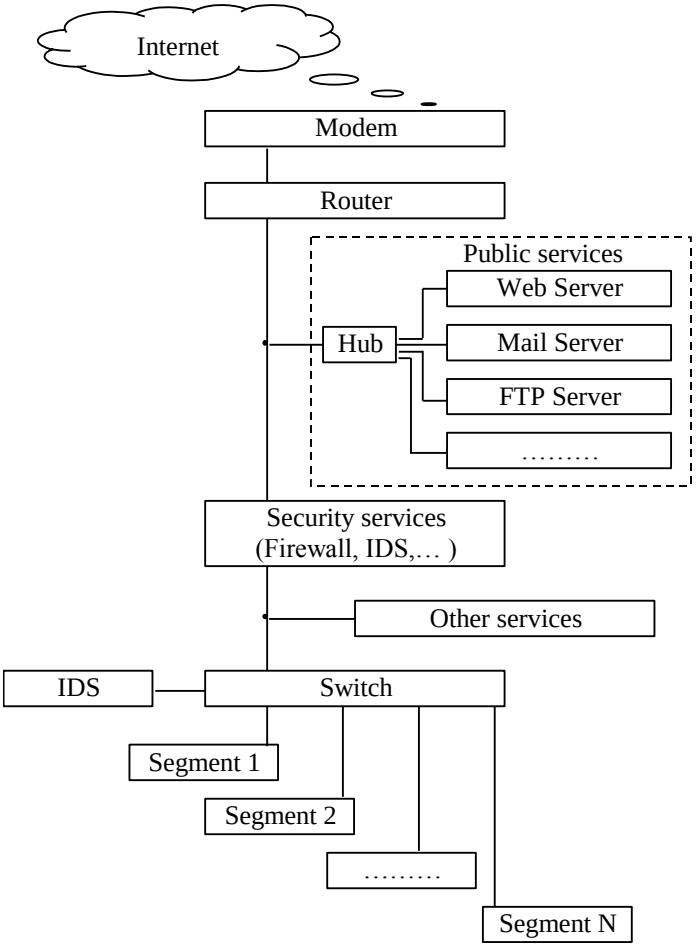


Рис. 6.9. Модель безопасности информационной сети предприятия

6.6. Типовая политика безопасности предприятия малого и среднего бизнеса – комплект документов и инструкций

Для модели безопасности информационной сети предприятия, представленной в предыдущем пункте (рисунок 6.9) необходимо предоставить:

Типовую политику безопасности.

Типовые документы и инструкции.

Основные средства, методы и элементы информационной защиты.

6.6.1. Типовая политика безопасности

Типовая политика безопасности разработана для организации, имеющей выход в Internet и обладающая ресурсами, к которым необходим доступ из Internet.

Сетевая безопасность

Доступ из Internet в корпоративную сеть компании:

Доступ во внутреннюю сеть извне запрещен.

Доступ к межсетевому экрану извне запрещен.

Доступ к следующим сервисам: антивирусному шлюзу, серверу аудита безопасности системы, средствам адаптивного управления безопасностью и обнаружения атак, средствам проверки почты доступ извне запрещен.

Доступ к WWW, FTP, e-mail сервисам извне разрешен по следующим правилам.

Для WWW сервиса:

доступ извне разрешен всем только к 80 порту,

доступ администратора WWW-сервера разрешен только из сегмента административного управления при прохождении процедуры аутентификации/идентификации на firewall.

Для e-mail сервера:

разрешен доступ из внутренней сети компании к POP3-сервису через 110 порт,

разрешен доступ из внутренней сети компании к SMTP-сервису через 25 порт.

Межсетевой экран:

Firewall администрируется только локально с автоматизированного рабочего места администратора сети (процедура администрирования возможна при прохождении аутентификации/идентификации пользователем (администратором)). Регулярно ставятся и обновляются антивирусные программы и необходимые патчи, поддерживается максимально безопасная конфигурация операционной системы.

Средства адаптивного управления безопасностью:

Система анализа защищенности (Internet Scanner) администрируется локально с автоматизированного рабочего места администратора сети. Анализ всесторонних и/или выборочных тестов операционных систем, используемого прикладного ПО, маршрутизатора, межсетевого экрана, всех серверов и т.д., производится администратором безопасности регулярно (раз в неделю).

Система обнаружения атак IDS служащая для автоматической реконфигурации межсетевого экрана в случае обнаружения атак. Сервис контролирует весь входящий трафик из сети Internet.

Средства протоколирования:

Ведутся специальные файлы.

на межсетевом экране ведется запись в лог-файл обо всех обращениях и попытках связи (удачных и нет) из корпоративной сети и в корпоративную сеть,

система обнаружения атак запоминает все атаки и подозрительные активности (так же в лог-файле),

на Web-сервисе храниться информация обо всех посетителях (лог-файл),

администратор безопасности должен вести файл, содержащий информацию обо всех изменениях и попытках изменить информацию в лог-файлах предыдущих сервисов.

Коммутатор (Switch):

разрешен доступ из всех сегментов сети к Internet без ограничений,

доступ из сетей пользователей в сети администраторов (управления, безопасности) запрещен.

Локальная безопасность

Локальная безопасность направлена на защиту каждого компьютера сети.

Антивирусный контроль:

Антивирусный контроль на всех рабочих станциях.

Защита от НСД:

Необходимо поставить систему защиты от НСД, которая должна контролировать и разграничивать доступ к каждой рабочей станции и серверу. Система должна быть:

при загрузке идентификация простого пользователя должна производиться при помощи при помощи пароля,

блокировать доступ в setup всех рабочих станций и серверов всем пользователям кроме администратора,

блокировать компьютер, в случае если пользователь покинул свое место.

Криптографическая защита данных:

Сотрудники компании должны сохранять информацию начиная с уровня “строго конфиденциально» (см. п.6.2) на специальном криптодиске.

Защита персональным firewall:

Все рабочие станции должны быть защищены персональным firewall (реализованным программно).

Резервирование данных

Обязательным является резервирование пользователями важных данных на персональных компьютерах на внутреннем сервере данных компании.

Протоколирование доступа:

При локальном доступе пользователя к рабочей станции (администратора к серверам) ведется лог-файл его посещений (протоколируются все удачные и неудачные попытки входа в систему).

Физическая безопасность

Все сервисы безопасности и данных должны находится в отдельном помещении, доступ в которое разрешен только администраторам (у которых есть ключ или магнитная карта к этой комнате).

Необходимо введение отдельной должности администратора безопасности, все изменения в системах ИТ – администратор и администратор безопасности будут делать в паре (пароль разбит на две части: по одному сегменту на специалиста).

Помещение должно быть оборудовано принудительной вентиляцией и пожарной защитой (полуавтоматической или автоматической), возможно, видео наблюдением за действиями администраторов.

Необходимо контролировать поток служащих и посетителей компании (либо по специальным пропускам, либо по магнитным картам).

6.6.2. Типовые документы и инструкции

В соответствии с рекомендациями Британского стандарта BS 7799:1995 включим в документ, характеризующий политику безопасности организации, следующие разделы:

1 Вводный раздел.

2 Организационный раздел.

3 Классификационный.

4 Штатный раздел.

5 Раздел инструкций и требований по обеспечению внутренней информационной безопасности компании.

Соответствие четырех уровневой модели обеспечения безопасности информационной сети предприятия. Первые три раздела соответствуют административному уровню защиты информации, четвертый раздел – процедурному уровню, а программно-техническому уровню соответствует пятый раздел документов.

Ранее говорилось, что ПБ состоит из двух (трех) уровней, чем больше предприятие, тем сложнее структура политики. Для малого и среднего бизнеса достаточно привести двухуровневую структуру политики безопасности, назовем условно верхний уровень «административным», а нижний «техническим». Таким образом, в «административный» раздел войдут документы вводного, организационного, классификационного и штатного разделов. «Технический» раздел охватит свод правил, инструкций и требований по обеспечению информационной безопасности организации.

Вводный раздел

Позиция администрации предприятия по вопросу защиты информационных активов:

Надежное функционирование информационной компьютерной сети предприятия является частью производственного процесса. Защита информационных активов предприятия необходима.

Типовые цели предприятия в области защиты информации:

Приоритетной целью любого предприятия является обеспечение целостности, конфиденциальности, доступности информации. В качестве частных целей:

следование экономической целесообразности в выборе защитных мер,

обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации,

и др.

Организационный раздел

Данный раздел включает описание всех групп пользователей имеющих отношение к работам в области информационной безопасности. В принципе данную формулировку можно трактовать по-разному, так как каждый пользователь сети так или иначе несет ответственность за некоторую часть производственной информации, с которой он работает. В таком контексте данный документ можно рассматривать как положение о категорировании пользователей автоматизированной системы.

Этот документ также может содержать положение о категорировании ресурсов.

Положение о категорировании пользователей АС:

В АС входят следующие группы пользователей:

Группа Администраторы. В нее входят администраторы информационных технологий и безопасности. Администраторы имеют полный доступ к ресурсам АС для ее администрирования.

Группа Топ-менеджеры. В группу входят: президент компании, генеральный директор, технический директор, заместители и т.д.

Группа Сотрудники. В группу входят все сотрудники компании (экономисты, бухгалтеры, сотрудники отдела кадров, …).

Каждая группа пользователей обладает различными правами доступа к информации различного уровня секретности. Уровень секретности определяется положением о категорировании ресурсов организации.

Положение о категорировании ресурсов:

В компании вводятся следующие уровни категорий секретности информации:

общедоступно,

конфиденциально,

строго конфиденциально,

секретно.

Сотрудникам компании строго запрещается разглашать кому-либо информацию, начиная с уровня «конфиденциально».

Общедоступной информацией является информация, уже опубликованная в средствах массовой информации, а также на Web-сайте компании. Решение о придании статуса «Общедоступно» принимает генеральный или технический директор.

Конфиденциальной информацией в компании является любая внутренняя информация компании (служебная, штатная,…).

Строго конфиденциальной информацией в компании является:

коммерческая информация (тексты договоров и соглашений с партнерами и клиентами),

техническая информация (тексты отчетов, ТЗ, значимые документы, продукты, ключи лицензирования и т.д.).

Решение о придание статуса «Строго конфиденциально» коммерческой информации принимает генеральный директор. Решение о придание статуса «Строго конфиденциально» технической информации принимает технический директор.

Порядок обращения с информацией, подлежащей защите

Должны быть четко описаны и классифицированы следующие действия с информацией:

1. копирование;
2. хранение;
3. передача почтой, факсом, е-мейлом;
4. передача голосом, включая мобильные телефоны, голосовую почту;
5. уничтожение.

1. Информация уровня «общедоступно». Доступ, копирование и любая передача информации данного уровня не ограничены. Уничтожение информации возможно только ее владельцем.

2. Информация уровня «конфиденциально». Подлежит защите от НСД средствами разграничения доступа.

Доступ к данной информации может осуществляться сотрудниками компании локально и удаленно. Удаленный доступ из корпоративной сети осуществляется без применения средств шифрования трафика. Удаленный доступ из Internet осуществляется с применением средств шифрования трафика.

Доступ к информации уровня «конфиденциально» осуществляется категориями пользователей: Администраторы, Топ-менеджеры, Сотрудники.

Копирование и любая передача информации данного уровня ограничены периметром компании. Уничтожение информации возможно только ее владельцем.

3. Информация уровня «строго конфиденциально». Подлежит защите от НСД средствами разграничения доступа и криптографической защите.

Удаленный доступ из корпоративной сети осуществляется с применением средств шифрования трафика. Удаленный доступ сотрудников из Internet осуществляется с применением средств шифрования трафика. Копирование и любая передача информации данного уровня возможно только в пределах компании и только авторизованным персонам. Уничтожение информации возможно только ее владельцем.

Право на удаление информации уровня “секретно” имеет только администратор безопасности вместе с ИТ – администратором (пароль разделен на две части между ними) с разрешения тех. Директора.

Доступ к информации уровня «строго конфиденциально» осуществляется категориями пользователей: Топ-менеджеры, Сотрудники (с разрешения тех. директора).

4. Информация уровня «секретно» подлежит защите от НСД, криптографической защите и обязательному протоколированию доступа.

Удаленный доступ из корпоративной сети осуществляется с применением средств шифрования трафика. Удаленный доступ из Internet запрещен. Копирование и любая передача информации данного уровня возможно только в пределах компании и только авторизованным персонам. Уничтожение информации возможно только ее владельцем.

Право на удаление информации уровня «секретно» имеет только администратор безопасности вместе с ИТ-администратором администратором (пароль разделен на две части между ними) с разрешения тех. директора.

Доступ к информации уровня «строго конфиденциально» осуществляется категориями пользователей: Топ-менеджеры.

Классификационный раздел

Данный раздел описывает имеющиеся в организации материальные, информационные ресурсы и необходимый уровень их защиты.

В качестве материальных ресурсов могут выступать элементы, описанные выше. В проекции на организацию с моделью безопасности информационной сети (рисунок 6.9) данный список может принять вид:

Аппаратное обеспечение:
компьютеры,
принтеры,
сканеры,
факсы и телефоны,
коммуникационные линии,
сетевое оборудование (сетевые карты) и их составные части.
Программное обеспечение:
операционные системы: Windows 2000, Server, NT, 98/95 (для рабочих станций),
прикладные программы: офисные приложения (MS Word, MS Excel, …), базы данных (1С, MS Access, Oracle, …), другое (…),
почтовые протоколы POP3, SMTP,
сетевые протоколы: стек TCP/IP,
система анализа защищенности (Internet Scanner),
система обнаружения атак IDS,
…
Информационное обеспечение (вводимые и обрабатываемые, хранимые, передаваемые и резервные (сохранные копии) данные и метаданные):
данные о сотрудниках (информация о личности (ФИО, …), занимаемой должности, правах доступа к информации, заработанной плате, …),
данные о клиентах/партнерах,
данные о соглашениях/контрактах с клиентами/партнерами,
промежуточные данные (при обработке какой бы то ни было информации),
данные о конфигурации системы, используемом оборудовании и программах,
….
Персонал:
обслуживающий персонал (ИТ – администраторы, администраторы безопасности),
пользователи (администрация организации, топ-менеджеры, экономисты, юристы, кладовщики, клиенты,…).
Документация (конструкторская, техническая, пользовательская, …).
Расходные материалы:
бумага,

магнитные носители,
картриджи,
др.

Штатный раздел

Данный раздел характеризует меры безопасности, применяемые к персоналу, иначе говоря, эти документы функционируют на процедурном уровне защиты информации. Типовые документы:

Описание должностей с точки зрения информационной безопасности,
Организация обучения и переподготовки персонала,
Порядок реагирования на нарушения режима безопасности и т.п.
Данный уровень был подробно рассмотрен ранее (см. п.3).

Раздел инструкций и требований по обеспечению внутренней информационной безопасности компании

Приведу перечень всех типовых инструкций:
Правила парольной защиты
Правила защиты от вирусов и злонамеренного программного обеспечения
Требования по контролю за физического доступом
Требования по физической защите оборудования
Инструкция по безопасному уничтожению информации или оборудования
Инструкция по безопасности рабочего места (документов на рабочем столе и на экране монитора)
Правила осуществления удаленного доступа
Правила осуществления локального доступа
Требования резервного сохранения информации
Требования мониторинга и ведения диагностических лог файлов
Требование мониторинга доступа и использования систем и ведения лог файлов
Требования при обращении с носителями данных
Требования по неэлектронному информационному обмену
Требования при регистрации пользователей
Требования по проверке прав пользователей
Требования по контролю доступа в операционную систему
Требование к процедуре входа в систему (log on)
Правила использования системных утилит
Правила удаленной работы мобильных пользователей
Следующие требования должны быть предусмотрены:
Требование распределения ответственности при обеспечении безопасности
Правила безопасности при выборе персонала
Требования контроля оперативных изменений
Требования проверки входных данных
Требования к применению криптографических средств управления
Требования по контролю программ операционной системы
Требования по контролю доступа к исходным текстам программ и библиотек
Требования контроля вносимых изменений
Требование обеспечения непрерывности бизнеса
Требования соблюдения авторского права на программное обеспечение
Требования обеспечения сохранности улик (свидетельств, доказательств)
Требования по управлению системным аудитом

Инструкции

По приему на работу и допуску новых сотрудников к работе в АС и наделения их необходимыми полномочиями по доступу к ресурсам системы.

По увольнению работников и лишения их прав доступа в систему.

По действиям различных категорий персонала, включая сотрудников отдела безопасности информации, по ликвидации последствий кризисных (аварийных или нештатных) ситуаций, в случае их возникновения.

Действия персонала по ликвидации последствий кризисных (аварийных или нештатных) ситуаций в случае их возникновения.

Процедуры контроля в случае инцидентов.

7. Контроль безопасности информационной системы

7.1. Нормативная база аудита

7.1.1. Законодательство в области аудита безопасности

Наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности АС, и требования, предъявляемые к механизмам защиты, являются:

Общие критерии оценки безопасности информационных технологий (The Common Criteria for Information Technology Security Evaluation/ISO 15408);

Практические правила управления информационной безопасностью (Code of practice for Information Security Management/ISO 17799);

Кроме этого, в нашей стране первостепенное значение имеют Руководящие документы (РД) Гостехкомиссии России. В других странах их место занимают соответствующие национальные стандарты (там, где они есть).

ISO 15408: Common Criteria for Information Technology Security Evaluation

Наиболее полно критерии для оценки механизмов безопасности программно-технического уровня представлены в международном стандарте ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий), принятом в 1999 году.

Общие критерии оценки безопасности информационных технологий (далее «Общие Критерии») определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements).

При проведении работ по анализу защищенности АС, а также СВТ «Общие критерии» целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности АС (СВТ) с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций.

Хотя применимость «Общих критериев» ограничивается механизмами безопасности программно-технического уровня, в них содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосредственно связаны с описываемыми функциями безопасности.

Первая часть «Общих критериев» содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В ней вводится понятийный аппарат, и определяются принципы формализации предметной области.

Требования к функциональности средств защиты приводятся во второй части «Общих критериев» и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в АС (СВТ) функций безопасности.

Третья часть «Общих критериев» содержит классы требований гарантированности оценки, включая класс требований по анализу уязвимостей средств и механизмов защиты под названием AVA: Vulnerability Assessment. Данный класс требований определяет методы, которые должны использоваться для предупреждения, выявления и ликвидации следующих типов уязвимостей:

Наличие побочных каналов утечки информации;

Ошибки в конфигурации либо неправильное использование системы, приводящее к переходу в небезопасное состояние;

Недостаточная надежность (стойкость) механизмов безопасности, реализующих соответствующие функции безопасности;

Наличие уязвимостей («дыр») в средствах защиты информации, дающих возможность пользователям получать НСД к информации в обход существующих механизмов защиты.

Соответствующие требования гарантированности оценки содержатся в следующих четырех семействах требований:

Семейство AVA_CCA: Covert Channel Analysis (Анализ каналов утечки информации);

Семейство AVA_MSU: Misuse (Ошибки в конфигурации либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние);

Семейство AVA_SOF: Strength of TOE Security Functions (Стойкость функций безопасности, обеспечиваемая их реализацией);

Семейство AVA_VLA: Vulnerability Analysis (Анализ уязвимостей).

При проведении работ по аудиту безопасности перечисленные семейства требований могут использоваться в качестве руководства и критериев для анализа уязвимостей АС (СВТ).

ISO 17799: Code of Practice for Information Security Management

Наиболее полно критерии для оценки механизмов безопасности организационного уровня представлены в международном стандарте ISO 17799: Code of Practice for Information Security Management (Практические правила управления информационной безопасностью), принятом в 2000 году. ISO 17799 является ни чем иным, как международной версией британского стандарта BS 7799.

ISO 17799 содержит практические правила по управлению информационной безопасностью и может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты (об этом упоминалось в первом разделе).

Практические правила разбиты на следующие 10 разделов:

Политика безопасности;

Организация защиты;

Классификация ресурсов и их контроль;

Безопасность персонала;

Физическая безопасность;

Администрирование компьютерных систем и вычислительных сетей;

Управление доступом;

Разработка и сопровождение информационных систем;

Планирование бесперебойной работы организации;

Контроль выполнения требований политики безопасности.

В этих разделах содержится описание механизмов безопасности организационного уровня, реализуемых в настоящее время в правительственных и коммерческих организациях во многих странах мира.

Десять средств контроля, предлагаемых в ISO 17799 (они обозначены как ключевые), считаются особенно важными. Под средствами контроля в данном контексте понимаются механизмы управления информационной безопасностью организации.

При использовании некоторых из средств контроля, например, шифрования данных, может потребоваться оценка рисков, чтобы определить нужны ли они и каким образом их следует реализовывать. Для обеспечения более высокого уровня защиты особенно ценных ресурсов или оказания противодействия особенно серьезным угрозам безопасности в ряде случаев могут потребоваться более сильные средства контроля, которые выходят за рамки ISO 17799.

Десять ключевых средств контроля, перечисленные ниже, представляют собой либо обязательные требования, например, требования действующего законодательства, либо считаются основными структурными элементами информационной безопасности, например, обучение правилам безопасности. Эти средства контроля актуальны для всех организаций и сред функционирования АС и составляют основу системы управления информационной безопасностью. Они служат в качестве основного руководства для организаций, приступающих к реализации средств управления информационной безопасностью.

Ключевыми являются следующие средства контроля:

Документ о политике информационной безопасности;

Распределение обязанностей по обеспечению информационной безопасности;

Обучение и подготовка персонала к поддержанию режима информационной безопасности;

Уведомление о случаях нарушения защиты;

Средства защиты от вирусов;

Планирование бесперебойной работы организации;

Контроль над копированием программного обеспечения, защищенного законом об авторском праве;

Защита документации организации;

Защита данных;

Контроль соответствия политике безопасности.

Процедура аудита безопасности АС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности АС также является анализ и управление рисками.

РД Гостехкомиссии России

В общем случае в нашей стране при решении задач защиты информации должно обеспечиваться соблюдение следующих указов Президента, федеральных законов, постановлений Правительства Российской Федерации, РД Гостехкомиссии России и других нормативных документов (см. также раздел 1):

Доктрина информационной безопасности Российской Федерации;

Указ Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»;

Закон Российской Федерации «Об информации, информатизации и защите информации» от 20.02.95 N 24-ФЗ;

Закон Российской Федерации «О связи» от 16.02.95 N 15-ФЗ;

Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 N3523-1;

Закон Российской Федерации «Об участии в международном информационном обмене» от 04.07.96 N 85-ФЗ;

Постановление Правительства Российской Федерации «О лицензировании отдельных видов деятельности» от 16.09.98г;

Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г;

ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении».

Руководящий документ «Положение по аттестации объектов информатизации по требованиям безопасности информации» (Утверждено Председателем Гостехкомиссии России 25.11.1994 г.);

Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования к защите информации» (Гостехкомиссия России, 1997);

«Положение о сертификации средств защиты информации по требованиям безопасности информации» (Постановление Правительства РФ 608, 1995 г.);

Руководящий документ «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1992 г.);

Руководящий документ «Концепция защиты средств вычислительной техники от НСД к информации» (Гостехкомиссия России, 1992 г.);

Руководящий документ «Защита от НСД к информации. Термины и определения» (Гостехкомиссия России, 1992 г.);

Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ» (Гостехкомиссия России, 1992 г.);

Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1997 г.);

Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» (Гостехкомиссия России, 1999 г.);

Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (Гостехкомиссия России, 2001г.).

РД Гостехкомиссии России составляют основу нормативной базы в области защиты от НСД к информации в нашей стране. Наиболее значимые из них, определяющие критерии для оценки защищенности АС (СВТ).

Критерии для оценки механизмов защиты программно-технического уровня, используемые при анализе защищенности АС и СВТ, выражены в РД Гостехкомиссии РФ:

«АС. Защита от НСД к информации. Классификация АС и требования по защите информации» и «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. (Основным источником при разработке этого документа послужила американская «Оранжевая книга»). Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий - первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

Первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;

Вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

Третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

Четвертая группа характеризуется верифицированной защитой содержит только первый класс.

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации».

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

наличие в АС информации различного уровня конфиденциальности;

уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

РД «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации».

При анализе системы защиты внешнего периметра корпоративной сети в качестве основных критериев целесообразно использовать РД «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации». Данный документ определяет показатели защищенности МЭ. Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ. Всего выделяется пять показателей защищенности:

Управление доступом;

Идентификация и аутентификация;

Регистрация событий и оповещение;

Контроль целостности;

Восстановление работоспособности.

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

Простейшие фильтрующие маршрутизаторы – 5 класс;

Пакетные фильтры сетевого уровня – 4 класс;

Простейшие МЭ прикладного уровня – 3 класс;

МЭ базового уровня – 2 класс;

Продвинутые МЭ – 1 класс.

МЭ первого класса защищенности могут использоваться в АС класса 1А, классах обрабатывающих информацию «особой важности». Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки «совершенно секретной» информации и т.п. [3].

7.1.2. Стандарты аудиторской деятельности

Ассоциация аудита и контроля информационных систем

Ассоциация аудита и контроля информационных систем – ISACA. Подход к проведению аудита ИС, как отдельной самостоятельной услуги, с течением времени упорядочился и стандартизировался. Крупные и средние аудиторские компании образовали ассоциации: союзы профессионалов в области аудита ИС, которые занимаются созданием и сопровождением стандартов аудиторской деятельности в сфере ИТ. Как правило, это закрытые стандарты.

Ассоциация ISACA занимается открытой стандартизацией аудита ИС.

Ассоциация ISACA основана в 1969 году и в настоящее время объединяет около 20 тысяч членов из более чем 100 стран, в том числе и России. Ассоциация координирует деятельность более чем 12000 аудиторов информационных систем.

Основная декларируемая цель ассоциации: это исследование, разработка, публикация и продвижение стандартизованного набора документов по управлению информационной технологией для ежедневного использования администраторами и аудиторами информационных систем.

В помощь профессиональным аудиторам, администраторам и заинтересованным пользователям ассоциацией ISACA и привлеченными специалистами из ведущих мировых консалтинговых компаний был разработан стандарт CoBiT.

CoBiT

CoBiT (Контрольные объекты информационной технологии) – открытый стандарт, первое издание, которое в 1996 году было продано в 98 странах по всему миру и облегчило работу профессиональных аудиторов в сфере информационных технологий. Стандарт связывает информационные технологии и действия аудиторов, объединяет и согласовывает многие другие стандарты в единый ресурс, позволяющий авторитетно, на современном уровне получить представление и управлять целями и задачами, решаемыми ИС. CoBiT учитывает все особенности информационных систем любого масштаба и сложности.

Основополагающее правило, положенное в основу CoBiT: ресурсы ИС должны управляться набором естественно сгруппированных процессов для обеспечения организации необходимой и надежной информацией (рисунок 7.1).

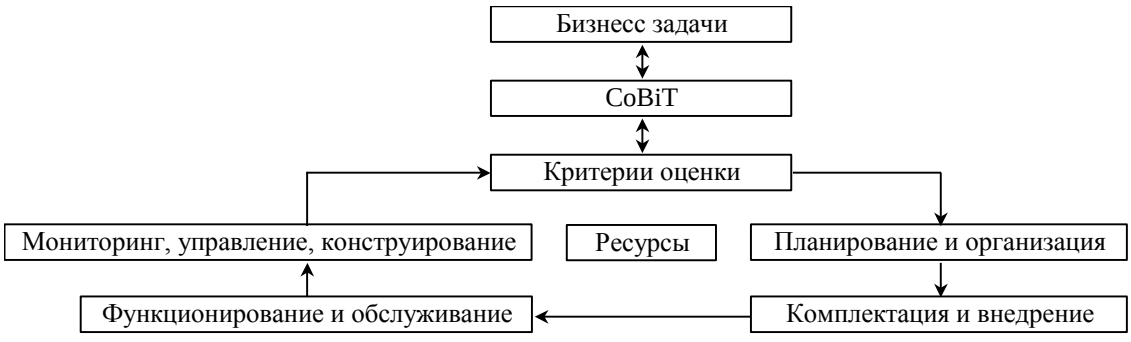


Рис. 7.1. Структура стандарта CoBiT

Каждый из приведенных элементов на блок схеме комплексный и включает в себя следующие компоненты.

Ресурсы: людские ресурсы, приложения, технологии, оборудование, данные. А теперь немного разъяснений по поводу того, какие ресурсы и критерии их оценки используются в стандарте CoBiT:

Трудовые ресурсы – под трудовыми ресурсами понимаются не только сотрудники организации, но также руководство организации и контрактный персонал. Рассматриваются навыки штата, понимание задач и производительность работы.

Приложения – прикладное программное обеспечение, используемое в работе организации.

Технологии – операционные системы, базы данных, системы управления и т.д.

Оборудование – все аппаратные средства ИС организации, с учетом их обслуживания.

Данные – данные в самом широком смысле — внешние и внутренние, структурированные и неструктурированные, графические, звуковые, мульти-медиа и т.д.

Критерии оценки: эффективность, технический уровень, безопасность, целостность, пригодность, согласованность, надежность.

Все эти ресурсы оцениваются CoBiT на каждом из этапов построения или аудита ИС по следующим критериям:

Эффективность – критерий, определяющий уместность и соответствие информации задачам бизнеса.

Технический уровень – критерий соответствия стандартам и инструкциям.

Безопасность – защита информации.

Целостность – точность и законченность информации.

Пригодность – доступность информации требуемым бизнес-процессам в настоящем и будущем. А также защита необходимых и сопутствующих ресурсов.

Согласованность – исполнение законов, инструкций и договоренностей, влияющих на бизнес-процесс, то есть внешние требования к бизнесу.

Надежность – соответствие информации, предоставляемой руководству организации, осуществление соответствующего управления финансированием и согласованность должностных обязанностей.

Планирование и организация:

P01 Стратегический план развития,
P02 Архитектура ИС,
P03 Технологическое направление,
P04 Внутренняя организационная структура и взаимоотношения,
P05 Управление инвестициями,
P06 Цели и задачи руководства,
P07 Пользователи и обслуживающий персонал,
P08 Законодательные и нормативные акты,
P09 Учет и анализ рисков,
P010 Управление проектами,
P011 Управление качеством.

Комплектация и внедрение:

A1 Технологическое решение,
A2 Прикладное ПО,
A3 Инфраструктура,
A4 Процедуры,
A5 Установка и аккредитация ИС,
A6 Оценка эффективности.

Функционирование и обслуживание:

DS1 Уровни обслуживания,
DS2 Услуги сторонних организаций,

DS3 Производительность и масштабируемость,
DS4 Непрерывность обслуживания,
DS5 Безопасность информации в ИС,
DS6 Определение и учет затрат,
DS7 Обучение пользователей,
DS8 Помощь и консультации обслуживающему персоналу,
DS9 Конфигурация элементов ИС,
DS10 Разрешение проблем и инцидентов,
DS11 Работа, передача, хранение и защита данных,
DS12 Безопасность работы,
DS13 Проведение и документирование работ.
Мониторинг, управление, контроль:
M1 Мониторинг происходящих процессов,
M2 Адекватность управления,
M3 Контроль независимого обслуживания,
M4 Проведение независимого аудита.

CoBiT базируется на стандартах аудита ISA и ISACF, но включает и другие международные стандарты, в том числе принимает во внимание утвержденные ранее стандарты и нормативные документы:

технические стандарты;
кодексы;
критерии ИС и описание процессов;
профессиональные стандарты;
требования и рекомендации;
требования к банковским услугам, системам электронной торговли и производству.

Стандарт разработан и проанализирован сотрудниками соответствующих подразделений ведущих консалтинговых компаний и используется в их работе наряду с собственными разработками.

Применение стандарта CoBiT возможно как для проведения аудита ИС организации, так и для изначального проектирования ИС. Обычный вариант прямой и обратной задач. Если в первом случае – это соответствие текущего состояния ИС лучшей практике аналогичных организаций и предприятий, то в другом – изначально верный проект и, как следствие, по окончании проектирования – ИС, стремящаяся к идеалу.

Несмотря на малый размер разработчики старались, чтобы стандарт был прагматичным и отвечал потребностям бизнеса, при этом сохраняя независимость от конкретных производителей, технологий и платформ.

На базовой блок-схеме CoBiT отражена последовательность, состав и взаимосвязь базовых групп. *Бизнес-процессы* (в верхней части схемы) предъявляют свои требования к ресурсам ИС, которые анализируются с использованием критериев оценки CoBiT на всех этапах построения и проведения аудита.

Четыре базовые группы (домена) содержат в себе тридцать четыре подгруппы, которые, в свою очередь состоят из трехсот двух объектов контроля. Объекты контроля предоставляют аудитору всю достоверную и актуальную информацию о текущем состоянии ИС.

Отличительные черты CoBiT:

Большая зона охвата (все задачи от стратегического планирования и основополагающих документов до анализа работы отдельных элементов ИС).

Перекрестный аудит (перекрывающиеся зоны проверки критически важных элементов).

Адаптируемый, наращиваемый стандарт.

Стандарт легко масштабируется и наращивается. CoBiT позволяет использовать любые разработки производителей аппаратно-программного обеспечения и анализировать полученные данные не изменяя общие подходы и собственную структуру.

Требования к представлению информации

Ассоциация ISACA разработала и приняла требования к представлению информации при проведении аудита. Применение стандарта CoBiT гарантирует соблюдение этих требований.

Основное требование: полезность информации. Чтобы информация была полезной, она должна обладать определенными характеристиками, среди которых:

Понятность. Информация должна быть понятной для пользователя, который обладает определенным уровнем знаний, что не означает, однако, исключения сложной информации, если она необходима.

Уместность. Информация является уместной или относящейся к делу, если она влияет на решения пользователей и помогает им оценивать прошлые, настоящие, будущие события или подтверждать и исправлять прошлые оценки. На уместность информации влияет ее содержание и существенность. Информация является существенной, если ее отсутствие или неправильная оценка могут повлиять на решение пользователя. Еще одна характеристика уместности: это своевременность информации, которая означает, что вся значимая информация своевременно, без задержки включена в отчет и такой отчет предоставлен вовремя. Неким аналогом принципа уместности в российской практике может служить требование полноты отражения операций за учетный период, хотя требование отражения всей информации не тождественно требованию отражения существенной информация.

Достоверность, надежность. Информация является достоверной, если она не содержит существенных ошибок или пристрастных оценок и правдиво отражает хозяйственную деятельность. Чтобы быть достоверной, информация должна удовлетворять следующим характеристикам:

правдивость;

нейтральность: информация не должна содержать однобоких оценок, то есть информация не должна предоставляться выборочно, с целью достижения определенного результата;

осмотрительность: готовность к учету потенциальных убытков, а не потенциальных прибылей и как следствие – создание резервов, такой подход уместен в состоянии неопределенности и не означает создание скрытых резервов или искажения информации;

достаточность информации: включает такую характеристику, как требование полноты информации, как с точки зрения ее существенности, так и затрат на ее подготовку.

Стандарты в области оценки информационной безопасности на базе «Общих критериев»

Проект «Общие критерии» стал основой для «Общих критериев оценки безопасности информационных технологий», который носит не только технический, но и экономико-политический характер. Его цель состоит, в частности, в том, чтобы упростить, удешевить и ускорить путь сертифицированных изделий информационных технологий на мировой рынок.

Эта цель близка и понятна российским специалистам. В 2002 году был официально издан ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий» с датой введения в действие первого января 2004 г. Таким образом, и Россия фактически живет по «Общим критериям» со всеми вытекающими из данного факта последствиями.

Согласно подходу, принятому в «Общих критериях», на основании предположений безопасности, при учете угроз и положений политики безопасности формулируются цели безопасности для объекта оценки. Для их достижения к объекту и его среде предъявляются требования безопасности.

«Общие критерии» в главной своей части являются каталогом (библиотекой) требований безопасности. Спектр стандартизованных требований чрезвычайно широк, что способствует универсальности “ОК”. Высокий уровень детализации делает их конкретными, допускающими однозначную проверку, способствует повторяемости результатов оценки. Требования параметризованы, что обеспечивает их гибкость.

«Общие критерии» содержат два основных вида требований безопасности:

функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности объекта оценки и реализующим их механизмам;

требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации объекта оценки.

Библиотека функциональных требований составляет вторую часть «Общих критериев», а каталог требований доверия – третью часть (первая содержит изложение основных концепций ОК).

Кроме того, выделяются общие требования к сервисам безопасности. К числу важнейших видов функциональных требований принадлежат: анализ аудита безопасности (FAU_SAA).

Из существенных для активного аудита компонентов класса FAU «Аудит безопасности» в «Общих критериях» отсутствуют анализ на соответствие политике безопасности (пороговый, статистический и сигнатурный анализы в семействе FAU_SAA предусмотрены), хранилища для описаний контролируемых объектов и для анализируемой информации, а также все интерфейсные компоненты.

В семейство FAU_GEN (генерация данных аудита безопасности) предлагается включить два новых компонента:

FAU_GEN.3 – ассоциирование объекта, операция с которым вызвала событие, с включением в регистрационные записи имени (идентификатора) этого объекта. На минимальном уровне должны протоколироваться открытие/закрытие объекта (установление/разрыв соединения и т.п.), на базовом - все промежуточные операции. На детальном уровне в регистрационные записи должны входить все операнды операции с объектом. Компонент FAU_GEN.3 добавлен по двум причинам. Во-первых, должна соблюдаться симметрия между субъектами и объектами. Во-вторых, статистические профили целесообразно строить не для субъектов, а для объектов, но для этого нужно располагать соответствующей информацией.

FAU_GEN.4 – предназначен для обеспечения неотказуемости сервиса, пользующегося услугами семейства FAU_GEN, от регистрации события.

Стандартный компонент FAU_SAR.3 дает возможность осуществлять поиск и сортировку регистрационной информации, задавая в качестве критериев логические выражения.

Подобные выражения полезны также для задания фильтров, управляющих работой сенсоров.

Автоматический анализ регистрационной информации с целью выявления подозрительной активности представлен в «Общих критериях» четырьмя компонентами семейства FAU_SAA.

FAU_SAA.1 ориентирован на обнаружение превышения порогов, заданных фиксированным набором правил.

FAU_SAA.2 служит для выявления нетипичной активности путем анализа профилей поведения. В «Общих критериях» предлагаются профили для субъектов, хотя профили объектов могут оказаться предпочтительными. «Общие критерии» допускают анализ, как в

реальном времени, так и постфактум. Поддержку анализа в реальном времени следует рассматривать как важнейшую отличительную особенность средств активного аудита.

FAU_SAA.3 направлен на выявление простых атак путем проведения сигнатурного анализа.

FAU_SAA.4 позволяет выявлять сложные, многоэтапные атаки, осуществляемые группой злоумышленников. Предусматривается возможность настройки всех четырех компонентов путем добавления, модификации или удаления правил, отслеживаемых субъектов и сигнатур.

Вводится еще один компонент, FAU_SAA.5, позволяющий выявлять нарушения политики безопасности. Задавать политики предлагается с помощью предикатов первого порядка.

В плане автоматического реагирования на подозрительную активность «Общие критерии» по сути ограничились констатацией подобной возможности. Решающий элемент, который, получив рекомендации от компонентов анализа, определяет, действительно ли имеет место подозрительная активность, и, при необходимости, надлежащим образом реагирует (выбирая форму реакции в зависимости от серьезности выявленных нарушений).

Это значит, что решатель (решающий элемент) должен уметь:

ранжировать подозрительную активность;

реагировать в соответствии с рангом нарушения.

Оба аспекта должны управляться администратором безопасности.

В качестве отдельной возможности, присущей системам высокого класса, фигурирует проведение корреляционного анализа информации.

Описание контролируемых объектов и хранение соответствующей информации - важнейшая составная часть средств активного аудита, придающая им свойства расширяемости и настраиваемости. К этому компоненту предъявляются в первую очередь технологические требования.

Мониторы, как организующие оболочки для менеджеров средств активного аудита, должны обладать двумя группами свойств:

обеспечивать защиту процессов, составляющих менеджер, от злоумышленных воздействий;

обеспечивать высокую доступность этих процессов.

Первая группа обслуживается семейством FPT_SEP (разделение доменов).

Вторая группа свойств может обеспечиваться такими техническими решениями, как программное обеспечение промежуточного слоя, кластерные конфигурации и т.д.

В плане безопасности целесообразно следовать требованиям FPT_FLS.1 (невозможность перехода в небезопасное состояние в случае сбоя или отказа), а также FPT_RCV.2, FPT_RCV.3, FPT_RCV.4 (надежное восстановление в автоматическом режиме, без потери данных, с точностью до функции безопасности).

Безопасность интерфейсов монитора (с другими мониторами, сенсорами, администратором безопасности) может обеспечиваться компонентами FPT_ITI.1, FPT_ITI.2 (обнаружение и исправление модификации экспортируемых данных), FPT_ITC.1 (конфиденциальность экспортируемых данных), FPT_ITA.1 (доступность экспортируемых данных).

На рабочем месте администратора безопасности должны быть обеспечены стандартные для средств управления возможности: графический интерфейс, возможность настройки способа визуализации и уровня детализации, отбора отображаемых событий. Специфичной для средств активного аудита является возможность получения объяснений от анализаторов и решателей по поводу обнаруженной подозрительной активности. Такие объяснения помогают выбрать адекватный способ реагирования.

Функциональный пакет (ФП) – это неоднократно используемая совокупность функциональных компонентов, объединенных для достижения определенных целей безопасности.

Профили защиты (ПЗ), соответствующие классам защищенности, строятся на основе базового ПЗ и соответствующих комбинаций ФП. Можно зафиксировать профили для следующих разновидностей средств активного аудита:

класс 5 - защита одного информационного сервиса с отслеживанием фиксированного набора характеристик и пороговым анализом (базовый ПЗ);

класс 4 - защита однохостовой конфигурации с произвольным набором информационных сервисов, отслеживанием сетевого трафика, системных и прикладных событий, пороговым и простым сигнатурным анализом в реальном масштабе времени;

класс 3 - защита сегмента локальной сети от многоэтапных атак при сохранении остальных предположений класса 4;

класс 2 - защита произвольной конфигурации с выявлением нетипичного поведения при сохранении остальных предположений класса 3;

класс 1 - наложение всех требований с возможностью обеспечения заданного соотношения между ошибками первого и второго рода.

7.2. Методы и средства аудита безопасности информационных систем

7.2.1. Основные понятия и определения

Активный аудит и его место среди других сервисов безопасности

Формула «защищать, обнаруживать, реагировать» является классической. Только эшелонированная, активная оборона, содержащая разнообразные элементы, дает шанс на успешное отражение угроз.

Назначение активного аудита – обнаруживать и реагировать. Обнаружению подлежит подозрительная активность компонентов ИС – от пользователей (внутренних и внешних) до программных систем и аппаратных устройств.

Подозрительную активность можно подразделить на:

злоумышленную,

аномальную (нетипичную).

Злоумышленная активность - это либо атаки, преследующие цель несанкционированного получения привилегий, либо действия, выполняемые в рамках имеющихся привилегий (возможно, полученных незаконно), но нарушающие политику безопасности. Последнее назовем – злоупотреблением полномочиями.

Нетипичная активность может впрямую не нарушать политику безопасности, но, как правило, она является следствием либо некорректной (или сознательно измененной) работы аппаратуры или программ, либо действий злоумышленников, маскирующихся под легальных пользователей.

Активный аудит дополняет такие традиционные защитные механизмы, как идентификация/аутентификация и разграничение доступа. Подобное дополнение необходимо по двум причинам. Во-первых, существующие средства разграничения доступа не способны реализовать все требования политики безопасности, если последние имеют более сложный вид, чем разрешение/запрет атомарных операций с ресурсами. Развитая политика безопасности может накладывать ограничения на суммарный объем прочитанной информации, запрещать доступ к ресурсу B, если ранее имел место доступ к ресурсу A, и т.п. Во-вторых, в самих защитных средствах есть ошибки и слабости, поэтому, помимо строительства заборов, приходится заботиться об отлавливании тех, кто смог через эти заборы перелезть.

Развитые системы активного аудита несут двойную нагрузку, образуя как первый, так и последний защитные рубежи (см. рисунок 7.2.). Первый рубеж предназначен для обнаружения атак и их оперативного пресечения. На последнем рубеже выявляются симптомы происходящих в данный момент или ранее случившихся нарушений политики безопасности, принимаются меры по пресечению нарушений и минимизации ущерба.

Рис. 7.2. Защитные рубежи, контролируемые системами активного аудита

И на первом, и на последнем рубеже, помимо активного аудита, присутствуют другие сервисы безопасности. К первому рубежу можно отнести сканеры безопасности, помогающие выявлять и устранять слабые места в защите. На последнем рубеже для обнаружения симптомов нарушений могут использоваться средства контроля целостности. Иногда их включают в репертуар систем активного аудита; мы, однако, не будем этого делать, считая контроль целостности отдельным сервисом.

Между сервисами безопасности существуют и другие связи. Так, активный аудит может опираться на традиционные механизмы протоколирования. В свою очередь, после выявления нарушения зачастую требуется просмотр ранее накопленной регистрационной информации, оценить ущерб, понять, почему нарушение стало возможным, спланировать меры, исключающие повторение инцидента. Параллельно производится надежное восстановление первоначальной конфигурации, то есть не измененной нарушителем.

Виды аудита

Классифицировать виды аудита можно по средствам, а именно:
активный аудит,
авторизованный аудит.

Активный аудит – это проверка непосредственно компьютерной информационной сети по средствам программных продуктов. Активный аудит позволяет реализовать постоянную проверку внутренней сети предприятия.

Авторизованный аудит – это проверка защищенности информационных активов предприятия на всех уровнях защиты (законодательном, административном, процедурном и программно-техническом). Подобную проверку осуществляют специально аккредитованные аудиторские службы.

Влияние аудита безопасности на развитие компании

Большинство лиц, ответственных за обеспечение информационной безопасности, задавалось вопросом: «Как оцепить уровень безопасности корпоративной информационной системы нашего предприятия для управления им в целом и определения перспектив его развития?».

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому вопрос «как оценить уровень безопасности корпоративной информационной системы» – обязательно влечет за собой следующие: в соответствии с какими критериями производить оценку эффективности защиты, как оценивать и переоценивать информационные риски предприятия? Вследствие этого, в дополнение к требованиям, рекомендациям и руководящим документам Гостехкомисии России и ФАПСИ приходится адаптировать к нашим условиям и применять методики международных стандартов (ISO 17799, 9001, 15408, BSI и пр.), а также использовать методы количественного анализа рисков в совокупности с оценками экономической эффективности инвестиций в обеспечение безопасности и защиты информации.

Такие методики работы по анализу рисков информационной безопасности, проектированию и сопровождению систем безопасности должны позволить:

произвести количественную оценку текущего уровня безопасности, задать допустимые уровни рисков, разработать план мероприятий по обеспечению требуемого уровня безопасности на организационно-управленческом, технологическом и техническом уровнях с использованием современных методик и средств;

рассчитать и экономически обосновать перед руководством или акционерами размер необходимых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;

выявить и провести первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;

определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности предприятия, создать необходимый пакет организационно-распорядительной документации;

разработать и согласовать со службами организации, надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;

обеспечить поддержание внедренного комплекса защиты в соответствии с из меняющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Новые возможности развития компании

Выполнение приведенных выше мероприятий открывает перед должностными лицами разного уровня новые широкие возможности:

руководителям организаций и предприятий позволяет обеспечить формирование единых *политики и концепции безопасности* предприятия; рассчитать, согласовать и

обосновать необходимые затраты в защиту предприятия; объективно и независимо оценить текущей уровень информационной безопасности предприятия; обеспечить требуемый уровень безопасности и в целом повысить экономическую эффективность предприятия; эффективно создавать и использовать *профили защиты* конкретного предприятия на основе неоднократно апробированных и адаптированных качественных и количественных методик опенки информационной безопасности предприятий;

начальникам служб автоматизации и информационной безопасности предприятия – получить оперативную и объективную *качественную и количественную* оценку состояния информационной безопасности предприятия на всех основных уровнях рассмотрения вопросов безопасности: *организационно-управленческом, технологическом и техническом;* выработать и обосновать необходимые меры организационного характера (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции действия в нештатных ситуациях); помогают составить экономическое обоснование необходимых инвестиций в защиту информации, обоснованно выбрать те или иные аппаратно-программные средства защиты информации в рамках единой *концепции безопасности* в соответствии с требованиями распоряжений и руководящих документов Гостехкомиссии России, ФАПСИ, а также международных стандартов ISO 17799, 9001, 15408, BSI; адаптировать и использовать в своей работе предложенные количественные показатели опенки информационной безопасности, методики оценки и управления безопасностью с привязкой к экономической составляющей эффективности предприятия;

системным, сетевым администраторам и администраторам безопасности предприятия - объективно оценить безопасность всех основных компонентов и сервисов корпоративной информационной системы предприятия, техническое состояние аппаратно-программных средств защиты информации (межсетевых экранов, маршрутизаторов, хостов, серверов, корпоративных БД и приложений); успешно применять на практике рекомендации, полученные в ходе выполнения аналитического исследования, для нейтрализации и локализации выявленных уязвимостей аппаратно-программного уровня;

сотрудникам и работникам предприятий и организаций - определить основные функциональные отношения и, что особенно важно, *зоны ответственности,* в том числе финансовой, за надлежащее использование информационных ресурсов и состояние *политики безопасности* предприятия.

7.2.2. Основные этапы проведения аудита

Комплексный аудит информационной безопасности включает следующие виды работ:

обследование объекта - построение информационной модели АС заказчика;

инвентаризация ресурсов – ранжирование ресурсов компании по степени важности;

построение частной модели угроз – классификация угроз по степени опасности и вероятности;

построение модели нарушителя;

оценка потенциального ущерба от нарушения безопасности – оценка рисков с применением методики трехфакторного анализа;

оценка существующей системы безопасности на соответствие требованиям стандартов безопасности: ведомственным, государственным, международным;

выявление уязвимых мест и каналов утечки информации;

разработка и оценка предложений по применению контрмер;

проектирование комплекса средств защиты;

разработка организационных мероприятий - пакет организационно-распорядительной документации;

оценка остаточных рисков.

Практические шаги авторизованного аудита безопасности

Как на практике реализовать перечисленные возможности? По мнению специалистов, это становится возможным в ходе следующих практических шагов аудита безопасности.

1. Комплексный анализ ИС предприятия и подсистемы информационной безопасности на методологическом, организационно-управленческом, технологическом и техническом уровнях. Анализ рисков.

1.1. Исследование и оценка состояния информационной безопасности КИС и подсистемы информационной безопасности предприятия.

Комплексная оценка соответствия типовых требований РД Гостехкомиссии РФ системе информационной безопасности предприятия.

Комплексная оценка соответствия типовых требований международных стандартов ISO системе информационной безопасности предприятия.

Комплексная оценка соответствия специальных требований заказчика системе информационной безопасности предприятия.

1.2. Работы на основе анализа рисков.

Анализ рисков. Уровень управления рисками на основе качественных оценок рисков.

Анализ рисков. Уровень управления рисками на основе количественных оценок рисков.

1.3. Инструментальные исследования.

1.3.1. Инструментальное исследование элементов инфраструктуры компьютерной сети и корпоративной информационной системы на наличие уязвимостей.

1.3.2. Инструментальное исследование защищенности точек доступа предприятия в Internet.

1.4. Анализ документооборота предприятия.

2. Разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, общетехническому и программно-аппаратному обеспечению режима информационной безопасности предприятия.

2.1. Разработка концепции обеспечения информационной безопасности предприятия.

2.2. Разработка корпоративной политики обеспечения информационной безопасности предприятия на организационно-управленческом, правовом, технологическом и техническом уровнях.

2.3. Разработка плана защиты предприятия заказчика.

2.4. Дополнительные работы по анализу и созданию методологического, организационно-управленческого, технологического, инфраструктурного и технического обеспечения режима информационной безопасности предприятия заказчика.

3. Организационно-технологический анализ ИС предприятия.

3.1. Оценка организационно-управленческого уровня безопасности.

Оценка соответствия типовым требованиям руководящих документов РФ к системе информационной безопасности предприятия в области организационно-технологических норм.

Анализ документооборота предприятия категории «конфиденциально» на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям предприятия по обеспечению конфиденциальности информации.

Дополнительные работы по исследованию и оценке информационной безопасности объекта.

3.2. Разработка рекомендаций по организационно-управленческому, технологическому, общетехническому обеспечению режима информационной безопасности предприятия.

Разработка элементов концепции обеспечения информационной безопасности предприятия.

Разработка элементов корпоративной политики обеспечения информационной безопасности предприятия на организационно-управленческом, правовом и технологическом уровнях.

4. Экспертиза решений и проектов.

Экспертиза решений и проектов автоматизации на соответствие требованиям по обеспечению информационной безопасности экспертно-документальным методом.

Экспертиза проектов подсистем информационной безопасности на соответствие требованиям по безопасности экспертно-документальным методом.

5. Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации.

Анализ документооборота предприятия категории “конфиденциально” на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям предприятия по обеспечению конфиденциальности информации.

Поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровне.

6. Работы, поддерживающие практическую реализацию плана защиты.

Разработка технического проекта модернизации средств защиты КИС, установленных у заказчика по результатам проведенного комплексного аналитического исследования корпоративной сети.

Разработка системы поддержки принятия решений на предприятии заказчика по обеспечению информационной безопасности предприятия на основе CASE-систем и др.

Подготовка предприятия к аттестации.

6.3.1. Подготовка “под ключ” предприятия к аттестации объектов информатизации заказчика на соответствие требованиям РД РФ.

6.3.2. Подготовка предприятия к аттестации КИС на соответствие требованиям по безопасности международных стандартов ISO 15408, ISO 17799, стандарта ISO 9001 при обеспечении требований информационной безопасности предприятия.

6.4. Разработка организационно-распорядительной и технологической документации.

6.4.1. Разработка расширенного перечня сведений ограниченного распространения как части политики безопасности.

6.4.2. Разработка пакета организационно-распорядительной документации (ОРД) в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровне.

6.4.3. Поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной, политики ИБ предприятия на организационно-управленческом и правовом уровнях.

7. Повышение квалификации и переподготовка специалистов.

Тренинги в области организационно-правовой составляющей защиты информации.

Обучение основам экономической безопасности.

Тренинги в области технологии защиты информации.

Тренинги по применению продуктов (технических средств) защиты информации.

Обучение действиям при попытке взлома информационных систем.

Обучение и тренинги по восстановлению работоспособности системы после нарушения штатного режима ее функционирования, а также по восстановлению данных и программ из резервных копий.

Сопровождение системы информационной безопасности после проведенного комплексного анализа или анализа элементов системы ИБ предприятия.

Ежегодная переоценка состояния ИБ.

Здесь под термином *аудит* информационной безопасности корпоративной системы Internet/Intranet понимается *системный процесс* получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности на всех основных уровнях обеспечения безопасности: методологическом, организационно-управленческом, технологическом и техническом. Таких оценок, которые позволяют выработать практические рекомендации по управлению и обеспечению информационной безопасности компании, адекватные поставленным целям и задачам развития бизнеса.

В целом независимо от своей разновидности, состава и объема аудит безопасности корпоративной системы Internet/Intranet должен позволить решить следующие актуальные задачи каждой проверяемой компании:

обеспечить (при необходимости повысить) информационную безопасность предприятия;

снизить потенциальные потери предприятия путем повышения устойчивости функционирования корпоративной сети;

защитить конфиденциальную информацию, передаваемую по открытым каналам связи;

защитить информацию от умышленного искажения (разрушения), несанкционированного копирования, доступа или использования;

обеспечить контроль действий пользователей в корпоративной сети предприятия;

своевременно оценить и переоценить информационные риски бизнес деятельности компании;

выработать оптимальные планы развития и управления предприятием.

Планирование авторизованного аудита информационной безопасности компании

В соответствии с рекомендациями международных стандартов информационной безопасности процедура проведения аудита безопасности компании должна планироваться заранее. Для этого необходимо составить *план проведения аудита,* который должен отражать все мероприятия и процедуры, связанные с первоначальными и контрольными проверками продолжительностью более одного дня. Кроме того необходимо ознакомиться с соответствующей законодательной и нормативной базой для выявления требований по информационной безопасности, которые могут быть использованы для обеспечения информационной безопасности компании.

Для проведения аудита информационной безопасности компании необходимо подготовить все необходимые сведения о собственной структуре, бизнес деятельности, текущих проектах, состоянии информационной инфраструктуры и т. п. Кроме того, потребуется:

документально оформленные концепция и политика безопасности компании,

список используемого в компании системного и прикладного программного обеспечения,

описание технологии обработки данных,

состав и структура подсистемы защиты информации,

общая карта компьютерной сети компании.

План проведения аудита должен определять проверяемые области деятельности компании и время их проверки с указанием, какие именно требования международных стандартов, например ISO 17799, и руководящих документов Гостехкомиссии РФ будут проверяться. Т.е. план подготовки и проведения аудита должен определять потребности компании в оценке и объективном анализе состояния информационной безопасности, потребности в соответствующих аппаратно-программных средствах защиты информации, потребности в обучении и переподготовке службы информационной безопасности, а также освещать другие вопросы, ответы на которые невозможно дать без проведения аудита. В дальнейшем план проведения аудита с внесенными в него изменениями по ходу проверок прилагается к отчету о проведении аудита. Кроме того, необходимо помнить о согласовании плана проведения аудита с Концепцией и Политикой информационной безопасности компании.

Рекомендуется выделять четыре возможных этапа планирования аудита:

Подготовка аудита безопасности;

Анализ требований и исходных данных;

Расчет трудоемкости и стоимости выполняемых работ;

Документирование процедуры проведения аудита.

Подготовительный этап

На *подготовительном этапе* исполнитель определяет общий порядок работ, устанавливающий последовательность выполнения и возможные затраты ресурсов, и согласовывает его с заказчиком. На этом этапе рассматриваются:

Назначение и цели предстоящего аудита, порядок их достижения.

Принципы установки рамок проведения аудита.

Функции, структура и состав корпоративной системы Internet/Intranet, узкие места и потенциальные уязвимости в системе управления информационной безопасностью.

Методики оценки квалификации специалистов и сотрудников службы информационной безопасности.

Способы категорирования обрабатываемой в корпоративной информационной системе информации, например на общедоступную, конфиденциальную и строго конфиденциальную;

Методы и инструментарии оценки временных затрат и затрат ресурсов компании на аудит информационной безопасности. Возможность использования результатов ранее проведенного аудита, в том числе анализа информационных рисков и анализа соответствия требованиям международных стандартов и руководящих документов Гостехкомиссии РФ;

Состав группы экспертов в области безопасности корпоративных систем Internet/Intranet и распределение обязанностей между ними;

Параметры корпоративной информационной сети компании и среды ее функционирования, оказывающие существенное влияние на качество аудита безопасности;

Совокупность учитываемых при проведении аудита безопасности требований международных, государственных, межведомственных и внутренних стандартов;

Внутренняя отчетная документация, оформление и при необходимости корректировка концепции и политики информационной безопасности компании;

Перспективы и тенденции развития корпоративной системы защиты информации компании, вопросы выработки стратегии и тактики ее развития.

Согласованный с заказчиком общий порядок проведения аудита безопасности компании может быть отражен в соответствующем техническом задании.

Этап анализа требований и исходных данных

Этап *анализа требований и исходных данных* составляет главную часть планирования аудита. В процессе анализа рассматриваются:

Требования информационной безопасности. Цель аудита – объективно и оперативно оценить и проверить соответствие исследуемой корпоративной системы защиты компании предъявляемым к ней требованиям информационной безопасности. Поэтому для такой оценки необходимо сначала рассмотреть требования информационной безопасности. Основными требованиями информационной безопасности для отечественных предприятий и компаний являются требования руководящих документов Гостехкомиссии РФ, законов Российской Федерации, внутриведомственных, межведомственных, национальных и международных стандартов. Кроме этого, для каждой корпоративной информационной системы необходимо учитывать специальные требования внутреннего использования, согласованные с концепцией и политикой безопасности компании. Такие внутренние требования рекомендуется формулировать по результатам анализа информационных рисков компании, учитывающих специфику конкретной компании;

Исходные данные для проведения аудита. В руководящем документе Гостехкомиссии «Положение по аттестации объектов информатизации по требованиям безопасности информации» приводится стандартный перечень исходных данных, необходимых для разработки программы и методики аттестационных испытаний. Помимо стандартных исходных данных могут использоваться и дополнительные исходные данные, специфичные для каждой конкретной компании, например статистика нарушений политики безопасности компании, статистика внешних и внутренних атак, уязвимости наиболее критичных корпоративных информационных ресурсов и т. д. Также нужно учитывать, что, как правило, руководство компании имеет собственные взгляды на информацию, предоставляемую в качестве исходных данных для аудита безопасности. Поэтому между заказчиком и исполнителем работ по аудиту информационной безопасности рекомендуется заключить специальное соглашение о конфиденциальности или соответствующий протокол о намерениях;

Рамки проведения аудита. При определении рамок проведения аудита необходимо в равной степени учитывать организационный, технологический, и программно-технический уровни обеспечения информационной безопасности. В противном случае результаты аудита не будут объективно отражать реальный уровень информационной безопасности компании. Например, дорогостоящие аппаратно-программные средства защиты информации могут оказаться бесполезными, если неправильно определены и реализованы меры и мероприятия на организационном и технологическом уровнях. При определении рамок аудита необходимо зафиксировать штатные условия функционирования корпоративной информационной системы безопасности компании. Такая фиксация может быть отражена в «Аттестате соответствия» или «Паспорте компании» и является необходимым условием для обеспечения требуемого уровня информационной безопасности компании и разработки планов действия в случае возникновения нештатных условий функционирования корпоративной системы Internet/Intranet;

Области детального изучения. При проведении аудита основное внимание должно уделяться компонентам и подсистемам, осуществляющим обработку конфиденциальной информации компании. При этом необходимо уметь рассчитать возможный ущерб, который может быть нанесен компании в случае разглашения конфиденциальной информации и нарушения Политики безопасности. Это должно быть отражено в соответствующих документах компании, регламентирующих ее политику информационной безопасности. Для определения возможного ущерба могут использоваться разнообразные формальные методы, например методы экспертных оценок. В качестве исходных данных для принятия решения об областях детального изучения могут служить

результаты ранее проведенного, текущего комплексного аудита безопасности компании, результаты анализа информационных рисков компании и другие данные. Кроме того при необходимости уязвимые места дополнительно могут быть исследованы специальными инструментальными проверками с помощью так называемых сканеров и систем проверки уровня защищенности;

Требуемый уровень детализации и полноты. В большинстве случаев для получения адекватных результатов достаточно провести базовый анализ корпоративной системы защиты информации, позволяющий определить общий уровень информационной безопасности компании и проверить его на соответствие некоторым требованиям безопасности. В некоторых случаях дополнительно требуется провести детальный анализ, цель которого — количественно оценить уровень информационной безопасности компании на основе специальных количественных метрик и мер информационной безопасности. Для этого сначала
определяются все необходимые количественные показатели, а затем производится оценка уровня информационной безопасности компании. Существенно, что при этом становится возможным сравнивать уровень безопасности компании с некоторым эталоном, определять тенденции и перспективы развития системы корпоративной безопасности, необходимые инвестиции и т. д.

Этап расчета трудоемкости и стоимости

На этапе *расчета трудоемкости и стоимости* проводимых работ по данным проведенного анализа оцениваются временные, финансовые, технические, информационные и прочие ресурсы, необходимые для аудита информационной безопасности. Выделение ресурсов рекомендуется производить с учетом возможных нештатных ситуаций, способных увеличить трудоемкость аудита безопасности.

Этап формализации и документирования

Завершается планирование аудита *формализацией и документированием* выполнения аудита, что прежде всего подразумевает подготовку и согласование плана проведения аудита. План проведения аудита в общем случае включает в себя следующие разделы:

Краткая характеристика работ. Включает все необходимые сведения о порядке проведения работ;

Введение. Указывается актуальность проведения аудита безопасности, особенности и требования к порядку проведения аудита, характеристика исследуемого объекта, рамки проведения аудита, общий порядок работ, требования по фиксации результатов аудита. Дополнительно приводятся сведения о категорировании корпоративной информации, например конфиденциальной и строго конфиденциальной. Также перечисляются основные решаемые задачи, ограничения, выполняемые функции и критерии оценивания уровня информационной безопасности компании, требования нормативных документов Российской Федерации, международных стандартов и внутренних требований компании;

Распределение обязанностей. Определяется штат и функциональные обязанности группы специалистов, которые будут проводить аудит безопасности;

Требования информационной безопасности. Фиксируется обоснованный выбор требований информационной безопасности, определяются критерии и показатели оценки информационной безопасности компании, выбираются количественные метрики и меры безопасности. Помимо нормативной и законодательной базы Российской Федерации дополнительно рекомендуется использовать требования международных и внутренних стандартов компании, актуальные для каждой отдельно взятой. Оценку инвестиций в

модернизацию корпоративной системы защиты информации рекомендуется проводить на основе результатов анализа информационных рисков компании;

Формализация оценок уровня безопасности компании. Определяются качественные и количественные параметры для получения объективных оценок уровня информационной безопасности компании. Перечисляются задачи, выполняемые при проведении базового и детального анализа информационных рисков. Состав задач зависит от того, на каком этапе жизненного цикла находится исследуемая безопасность корпоративной системы Internet/Intranet: этапе проектирования, эксплуатации или др. В этом разделе отражаются критичные информационные ресурсы компании, оценка экономической эффективности ее деятельности, используемые модели, методы средства проведения аудита безопасности, исходные данные;

План-график работ. Определяются сроки, календарный план выполняемых работ, время их окончания, формы отчетных документов, требования по приему-сдаче работы и прочее;

Поддержка и сопровождение. Перечисляются требования к административной, технологической и технической поддержке аудита информационной безопасности;

Отчетные документы. Основными отчетными документами являются отчет по результатам аудита безопасности, концепция и политика информационной безопасности, план защиты компании;

Приложения. В приложениях приводятся протоколы проверок, а также информация по методикам и инструментарии проведения аудита, выявленные замечания, рекомендации и прочее.

7.2.3. Методика анализа защищенности

В настоящее время не существует каких-либо стандартизированных методик анализа защищенности АС, поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако типовую методику анализа защищенности корпоративной сети предложить все-таки возможно. И хотя данная методика не претендует на всеобщность, ее эффективность многократно проверена на практике.

Типовая методика анализа защищенности корпоративной сети включает использование следующих методов:

Изучение исходных данных по АС;

Оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;

Анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;

Ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры;

Сканирование внешних сетевых адресов ЛВС из сети Интернет;

Сканирование ресурсов ЛВС изнутри;

Анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

Исходные данные по обследуемой АС

В соответствии с требованиями РД Гостехкомиссии при проведении работ по аттестации безопасности АС, включающих в себя предварительное обследование и анализ

защищенности объекта информатизации, заказчиком работ должны быть предоставлены следующие исходные данные:

Полное и точное наименование объекта информатизации и его назначение.

Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) информации и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия).

Организационная структура объекта информатизации.

Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация.

Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.

Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.

Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.

Наличие и характер взаимодействия с другими объектами информатизации.

Состав и структура системы защиты информации на аттестуемом объекте информатизации.

Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.

Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.

Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).

Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).

Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

Опыт показывает, что перечисленных исходных данных явно недостаточно для выполнения работ по анализу защищенности АС, и приведенный в РД Гостехкомиссии список нуждается в расширении и конкретизации. Пункт 14 приведенного списка предполагает предоставление других исходных данных по объекту информатизации, влияющих на безопасность информации. Как раз эти «дополнительные» данные и являются наиболее значимыми для оценки текущего положения дел с обеспечением безопасности АС. Их список включает следующие виды документов:

Дополнительная документация:

Нормативно-распорядительная документация по проведению регламентных работ.

Нормативно-распорядительная документация по обеспечению политики безопасности.

Должностные инструкции для администраторов, инженеров технической поддержки, службы безопасности.

Процедуры и планы предотвращения и реагирования на попытки НСД к информационным ресурсам.

Схема топологии корпоративной сети с указанием IP-адресов и структурная схема.

Данные по структуре информационных ресурсов с указанием степени критичности или конфиденциальности каждого ресурса.

Размещение информационных ресурсов в корпоративной сети.

Схема организационной структуры пользователей.

Схема организационной структуры обслуживающих подразделений.

Схемы размещения линий передачи данных.

Схемы и характеристики систем электропитания и заземления объектов АС.

Данные по используемым системам сетевого управления и мониторинга.

Проектная документация:

Функциональные схемы.

Описание автоматизированных функций.

Описание основных технических решений.

Эксплуатационная документация: Руководства пользователей и администраторов используемых программных и технических средств защиты информации (СЗИ) (в случае необходимости).

При анализе конфигурации средств защиты внешнего периметра ЛВС и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты, определяемые их конфигурацией:

Настройка правил разграничения доступа (правил фильтрации сетевых пакетов) на МЭ и маршрутизаторах;

Используемые схемы и настройка параметров аутентификации;

Настройка параметров системы регистрации событий;

Использование механизмов, обеспечивающих сокрытие топологии защищаемой сети, включающих в себя трансляцию сетевых адресов (NAT), маскарадинг и использование системы split DNS;

Настройка механизмов оповещения об атаках и реагирования;

Наличие и работоспособность средств контроля целостности;

Версии используемого ПО и наличие установленных пакетов программных коррекций.

Методы анализа защищенности информационной системы

Выявление злоумышленной активности

Под злоумышленной активностью мы понимаем как атаки (очевидно, противоречащие любой политике безопасности), так и действия, нарушающие политику безопасности конкретной организации путем злоупотребления имеющимися полномочиями. Разделение двух видов злоумышленной активности представляется нам целесообразным по той причине, что настройка на выявление атак может быть выполнена поставщиком системы активного аудита (атаки носят универсальный характер), в то время как политика безопасности (если, конечно, она есть) у каждой организации своя и настраиваться на нее заказчикам придется самим.

Для выявления злоумышленной активности пытались и пытаются использовать несколько универсальных технологий: экспертные системы, нейронные сети, сопоставление с образцом, конечные автоматы и т.п. Одной из первых и до сих пор самой употребительной остается технология обнаружения сигнатур злоумышленных действий. Идея состоит в том, чтобы каким-либо образом задать характеристики злоумышленного поведения (это и называется сигнатурами), а затем отслеживать поток событий в поисках соответствия с предопределенными образцами. В более серьезных разработках уже свыше десяти лет используются экспертные системы, опирающиеся на наборы правил, задающие более мощные языки.

Самой сложной проблемой для сигнатурного подхода является обнаружение ранее неизвестных атак, ведь новые угрозы появляются практически каждый день. Бороться с ними можно двумя способами.

Во-первых, можно регулярно обновлять набор сигнатур. Здесь, помимо полноты, критически важной является частота обновлений. Сигнатуры новых атак должны предоставляться заказчикам на порядок быстрее, чем заплаты от производителей скомпрометированных аппаратных или программных продуктов. На практике это означает обновление в течение суток, но никак не раз в месяц. В противном случае системы активного аудита начинают напоминать фиговый листок, а не средство защиты от реальных угроз.

Во-вторых, можно сочетать сигнатурный подход с методами выявления аномальной активности (см. ниже). Атака или злоупотребление полномочиями - это почти всегда аномалия. Задача такова – не пропустить ее и не поднимать слишком часто ложных тревог.

Выявление аномальной активности

Для выявления аномальной активности предложено довольно много методов: нейронные сети, экспертные системы, статистический подход.

Статистический подход можно подразделить на кластерный и факторный анализ, а также дискриминантный (классификационный) анализ. Не вдаваясь в детали, укажем, что буквальное применение этих методов не дает хороших результатов; необходимо учитывать специфику предметной области - активного аудита.

Статистический анализ (с учетом сделанных оговорок) представляется наиболее перспективным, отчасти “от противного”, в силу недостатков, присущих другим подходам.

У нейронных сетей две основные проблемы:

непонятность результатов: нейронная сеть принимает решение, но не объясняет, почему оно было принято;

нехватка адекватного обучающего материала: невозможно создать базу всех типов аномалий.

Основной недостаток экспертных систем – неумение выявлять (и, следовательно, отражать) неизвестные атаки.

У статистического подхода также есть проблемы:

относительно высокая вероятность ложных тревог (не типичность поведения не всегда означает злой умысел);

плохая работа в случаях, когда действия пользователей не имеют определенного шаблона, когда с самого начала пользователи совершают злоумышленные действия (злоумышленные действия типичны), наконец, когда пользователь постепенно изменяет шаблон своего поведения в сторону злоумышленных действий.

Тем не менее, с этими проблемами можно бороться.

Выявление аномальной активности статистическими методами основывается на сравнении краткосрочного поведения с долгосрочным. Для этого измеряются значения некоторых параметров работы субъектов (пользователей, приложений, аппаратуры). Параметры могут отличаться по своей природе; можно выделить следующие группы:

категориальные (измененные файлы, выполненные команды, номер порта и т.п.);

числовые (процессорное время, объем памяти, количество просмотренных файлов, число переданных байт и т.п.);

величины интенсивности (число событий в единицу времени);

распределение событий (таких как доступ к файлам, вывод на печать и т.п.).

Алгоритмы анализа могут работать с разнородными значениями, а могут преобразовать все параметры к одному типу (например, разбив область значения на конечное число подобластей и рассматривая все параметры как категориальные). Выбор измеряемых характеристик работы - очень важный момент. С одной стороны, недостаточное число

фиксируемых параметров может привести к неполноте описания поведения субъекта и к большому числу пропуска атак; с другой стороны, слишком большое число отслеживаемых характеристик потребует слишком большого объема памяти и замедлит работу алгоритма анализа.

Измерения параметров накапливаются и преобразуются в профили - описания работы субъектов. Суть преобразования множества результатов измерения в профили - сжатие информации. В результате от каждого параметра должно остаться лишь несколько значений статистических функций, содержащих необходимые для анализирующего алгоритма данные. Для того чтобы профили адекватно описывали поведение субъекта, необходимо отбрасывать старые значения параметров при пересчете значений статистических функций. Для этого, как правило, используется один из двух методов:

Метод скользящих окон – результаты измерений за некоторый промежуток времени (для долгосрочных профилей - несколько недель, для краткосрочных - несколько часов) сохраняются; при добавлении новых результатов старые отбрасываются. Основным недостатком метода скользящих окон является большой объем хранимой информации.

Метод взвешенных сумм – при вычислении значений статистических функций более старые данные входят с меньшими весами (как правило, новые значения функций вычисляются по рекуррентной формуле, и необходимость хранения большого количества информации отпадает). Основным недостатком метода является более низкое качество описания поведения субъекта, чем в методе скользящих окон.

Итак, долгосрочные профили содержат в себе информацию о поведении субъектов за последние несколько недель; обычно они пересчитываются раз в сутки, когда загрузка системы минимальна. Краткосрочные профили содержат информацию о поведении за последние несколько часов или даже минут; они пересчитываются при поступлении новых результатов измерений.

Сравнение краткосрочных и долгосрочных профилей может производиться разными способами. Можно просто проверять, все ли краткосрочные значения попадают в доверительные интервалы, построенные по долгосрочному профилю. Однако в этом случае аномалии, распределенные по нескольким параметрам, могут остаться незамеченными. Поэтому предпочтительнее анализировать профили в совокупности. Далее, измеряемые характеристики, как правило, не являются независимыми, поэтому было бы желательным, чтобы влияние параметров на решение о типичности поведения было пропорционально степени их независимости.

Полезной числовой характеристикой является количество зафиксированных ошибок. При этом обнаруживается не только злоумышленное поведение, но и сбои и отказы аппаратуры и программ, что также можно считать нарушением информационной безопасности. Разумеется, целесообразно измерять и объем сетевого трафика. Аномальными являются отклонения в обе стороны (слишком большой трафик - сервис используют в злоумышленных целях, слишком маленький - нарушена доступность сервиса).

Применительно к сетевому трафику и некоторым другим событиям полезным классом величин оказывается интенсивность.

Для успеха статистического подхода важен правильный выбор субъектов, поведение которых анализируется. Например, целесообразно анализировать поведения сервисов или их компонентов (например, доступ анонимных пользователей к FTP-сервису). По сравнению с отдельными пользователями, поведение сервисов отличается большей стабильностью, да и для информационной безопасности организации важны именно сервисы. Совсем нет смысла анализировать сетевой трафик “вообще”, его также нужно структурировать по типам поддерживаемых сервисов (плюс служебные моменты сетевого и транспортного уровней, такие как установление соединений).

Реагирование на подозрительные действия

После того, как обнаружена сигнатура злоумышленного действия или нетипичная активность, необходимо выбрать достойный ответ. По многим соображениям удобно, чтобы компонент реагирования содержал собственную логику, фильтруя сигналы тревоги и сопоставляя сообщения, поступающие от подсистем анализа. Для активного аудита одинаково опасны:

пропуск атак - это значит, что не обеспечивается должной защиты,

большое количество ложных тревог – это значит, что активный аудит быстро отключат.

При выборе реакции особенно важно определить первопричину проблем. Для сетевых систем это особенно сложно в силу возможности подделки адресов в пакетах. Данный пример показывает, что сильнодействующие средства, пытающиеся воздействовать на злоумышленника, сами могут стать косвенным способом проведения атак.

Предпочтительны более спокойные, но также достаточно эффективные меры, такие как блокирование злоумышленного сетевого трафика средствами межсетевого экранирования (ряд систем активного аудита умеют управлять конфигурацией экранов) или принудительное завершение сеанса работы пользователя. Конечно, и здесь остается опасность наказать невиновного, так что политика безопасности каждой организации должна определять, что важнее - не пропустить нарушение или не обидеть лояльного пользователя.

С точки зрения быстрого реагирования, традиционные меры, связанные с информированием администратора, не особенно эффективны. Они хороши в долгосрочном плане, для глобального анализа защищенности командой профессионалов. Здесь активный аудит смыкается с пассивным, обеспечивая сжатие регистрационной информации и представление ее в виде, удобном для человека.

Разумная реакция на подозрительные действия может включать увеличение степени детализации протоколов и активизацию средств контроля целостности. В принципе, это пассивные меры, но они помогут понять причины и ход развития нарушения, так что человеку будет проще выбрать «меру пресечения».

Методы тестирования системы защиты

Тестирование системы защиты АС проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите. Традиционно используются два основных метода тестирования:

тестирование по методу «черного ящика»;

тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования в данном случае являются сетевые сканеры, располагающие базами данных известных уязвимостей.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рисками. Выводы о наличие уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике. Основным инструментом

анализа в данном случае являются программные агенты средств анализа защищенности системного уровня, рассматриваемые ниже.

7.2.4. Средства анализа защищенности

Арсенал программных средств, используемых для анализа защищенности АС достаточно широк. Причем во многих случаях свободно распространяемые программные продукты ничем не уступают коммерческим. Достаточно сравнить некоммерческий сканер NESSUS с его коммерческими аналогами.

Одним из методов автоматизации процессов анализа и контроля защищенности распределенных компьютерных систем является использование технологии интеллектуальных программных агентов. Система защиты строится на архитектуре консоль/менеджер/агент. На каждую из контролируемых систем устанавливается программный агент, который и выполняет соответствующие настройки ПО и проверяет их правильность, контролирует целостность файлов, своевременность установки пакетов программных коррекций, а также выполняет другие полезные задачи по контролю защищенности АС. Управление агентами осуществляется по сети программой менеджером.

Менеджеры являются центральными компонентами подобных систем. Они посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все данные, полученные от агентов в центральной базе данных. Администратор управляет менеджерами при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т. п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу. Такой подход был использован при построении комплексной системы управления безопасностью организации Symantec ESM.

Другим широко используемым методом анализа защищенности является активное тестирование механизмов защиты путем эмуляции действий злоумышленника по осуществлению попыток сетевого вторжения в АС. Для этих целей применяются сетевые сканеры, эмулирующие действия потенциальных нарушителей. В основе работы сетевых сканеров лежит база данных, содержащая описание известных уязвимостей ОС, МЭ, маршрутизаторов и сетевых сервисов, а также алгоритмов осуществления попыток вторжения (сценариев атак). Рассматриваемые ниже сетевые сканеры Nessus и Symantec NetRecon являются достойными представителями данного класса программных средств анализа защищенности.

Таким образом, программные средства анализа защищенности условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средствами анализа защищенности сетевого уровня. Второй класс, к которому относятся все остальные рассмотренные здесь средства, иногда называют средствами анализа защищенности системного уровня. Данные классы средств имеют свои достоинства и недостатки, а на практике взаимно дополняют друг друга.

Для функционирования сетевого сканера необходим только один компьютер, имеющий сетевой доступ к анализируемым системам, поэтому в отличие от продуктов, построенных на технологии программных агентов, нет необходимости устанавливать в каждой анализируемой системе своего агента (своего для каждой ОС).

К недостаткам сетевых сканеров можно отнести большие временные затраты, необходимые для сканирования всех сетевых компьютеров из одной системы, и создание большой нагрузки на сеть. Кроме того, в общем случае трудно отличить сеанс сканирования от действительных попыток осуществления атак. Сетевыми сканерами также с успехом пользуются злоумышленники.

Системы анализа защищенности, построенные на интеллектуальных программных агентах, являются потенциально более мощным средством, чем сетевые сканеры. Однако, несмотря на все свои достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому эти средства лучше применять совместно. Кроме того, сканеры являются более простым, доступным, дешевым и, во многих случаях, более эффективным средством анализа защищенности.

Средства анализа параметров защиты (Security Benchmarks)

Уровень защищенности компьютерных систем от угроз безопасности определяется многими факторами. При этом одним из определяющих факторов является адекватность конфигурации системного и прикладного ПО, средств защиты информации и активного сетевого оборудования существующим рискам. Перечисленные компоненты АС имеют сотни параметров, значения которых оказывают влияние на защищенности системы, что делает их ручной анализ трудновыполнимой задачей. Поэтому в современных АС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации зачастую используются специализированные программные средства.

Анализ параметров защиты осуществляется по шаблонам, содержащим списки параметров и их значений, которые должны быть установлены для обеспечения необходимого уровня защищенности. Различные шаблоны определяют конфигурации для различных программно-технических средств.

Относительно коммерческих корпоративных сетей, подключенных к сети Интернет, можно говорить о некотором базовом уровне защищенности, который в большинстве случаев можно признать достаточным. Разработка спецификаций (шаблонов) для конфигурации наиболее распространенных системных программных средств, позволяющих обеспечить базовый уровень защищенности, в настоящее время осуществляется представителями международного сообщества в лице организаций и частных лиц, профессионально занимающихся вопросами информационной безопасности и аудита АС, под эгидой международной организации Центр Безопасности Интернет (Center of Internet Security). На данный момент закончены, либо находятся в разработке следующие спецификации (Security Benchmarks):

Solaris (Level-1)
Windows 2000 (Level-1)
CISCO IOS Router (Level-1/Level-2)
Linux (Level-1)
HP-UX (Level-1)
AIX (Level-1)
Check Point FW-1/VPN-1 (Level-2)
Apache Web Server (Level-2)
Windows NT (Level-1)
Windows 2000 Bastion Host (Level-2)
Windows 2000 Workstation (Level-2)
Windows IIS5 Web Server (Level-2)

В приведенном списке спецификации первого уровня (Level-1) определяют базовый (минимальный) уровень защиты, который требуется обеспечить для большинства систем, имеющих подключения к Интернет. Спецификации второго уровня (Level-2) определяют продвинутый уровень защиты, необходимый для систем, в которых предъявляются повышенные требования по безопасности.

Перечисленные спецификации являются результатом обобщения мирового опыта обеспечения информационной безопасности.

Для анализа конфигурации компонентов АС на соответствие этим спецификациям используются специализированные тестовые программные средства (CIS-certified scoring tools).

В качестве примера рассмотрим спецификацию базового уровня защиты для ОС MS Windows 2000 и соответствующий программный инструментарий для анализа конфигурации ОС.

Сетевые сканеры

Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности АС.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и непотерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

Идентификацию доступных сетевых ресурсов;

Идентификацию доступных сетевых сервисов;

Идентификацию имеющихся уязвимостей сетевых сервисов;

Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

В настоящее время существует большое количество как коммерческих, так и свободно распространяемых сканеров, как универсальных, так и специализированных, предназначенных для выявления только определенного класса уязвимостей. Многие из них можно найти в сети Интернет. Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 1000.

Одним из наиболее продвинутых коммерческих продуктов этого класса является сетевой сканер NetRecon компании Symantec, база данных которого содержит около 800 уязвимостей UNIX, Windows и NetWare систем и постоянно обновляется через Web. Рассмотрение его свойств позволит составить представление о всех продуктах этого класса.

Сетевой сканер NetRecon

Сетевой сканер NetRecon является инструментом администратора безопасности, предназначенным для исследования структуры сетей и сетевых сервисов и анализа защищенности сетевых сред. NetRecon позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентах. Например, NetRecon позволяет находить уязвимости в таких сетевых сервисах, как ftp, telnet, DNS, электронная почта, Web-сервер и др. При этом проверяются версии и конфигурации сервисов, их защищенность от сетевых угроз и устойчивость к попыткам проникновения. Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, которые реализуют алгоритмы, эмулирующие действия злоумышленника по осуществлению сетевых атак.

Программа работает в среде ОС Windows NT и имеет удобный графический интерфейс, позволяющий определять параметры сканирования, наблюдать за ходом сканирования, генерировать и просматривать отчеты о результатах сканирования. Результаты отображаются в графической и в табличной форме в реальном масштабе времени.

Создаваемые NetRecon отчеты содержат подробную информацию о найденных уязвимостях, включая слабость паролей пользователей, подверженность определенных сервисов угрозам отказа в обслуживании, уязвимые для сетевых атак конфигурации ОС и многие другие. Наряду с сообщениями о найденных уязвимостях и их описаниями, приводятся рекомендации по их устранению. Отчет о результатах сканирования позволяет наметить план мероприятий по устранению выявленных недостатков.

NetRecon самостоятельно определяет конфигурацию сети и позволяет выбрать сетевые ресурсы для сканирования. Может осуществляться параллельное сканирование всех сетевых ресурсов, сканирование по диапазону сетевых адресов, сканирование отдельных систем или подсетей. Сеанс сканирования может включать в себя все виды проверок либо отдельные проверки по выбору пользователя. Глубина сканирования определяется продолжительностью сеанса сканирования, которая задается пользователем. Например, проверки, связанные с подбором пользовательских паролей по словарю, сопряжены с существенными временными затратами и не могут быть завершены в течение короткого сеанса сканирования.

NetRecon дает возможность пользователю отслеживать путь поиска уязвимости, представляющий собой последовательность проверок, производимых NetRecon, которая привела к выявлению данной уязвимости. Путь поиска уязвимости позволяет проследить действия возможного нарушителя, осуществляющего атаку на сетевые ресурсы.

Используемая NetRecon база данных содержит описание известных уязвимостей и сценариев атак. Она регулярно пополняется новыми данными. Обновление этой базы данных производится через Web-узел компании Symantec автоматически, при помощи механизма LiveUpdate.

Сетевой сканер NESSUS

Сетевой сканер Nessus может рассматриваться в качестве достойной альтернативы коммерческим сканерам. Nessus является свободно распространяемым и постоянно обновляемым программным продуктом. Удобный графический интерфейс позволяет определять параметры сеанса сканирования, наблюдать за ходом сканирования, создавать и просматривать отчеты.

По своим функциональным возможностям сканер защищенности Nessus находится в одном ряду, а по некоторым параметрам и превосходит такие широко известные коммерческие сканеры, как NetRecon компании Symantec, Internet Scanner компании ISS.

Версия 0.99 серверной части сканера Nessus была сертифицирована в Гостехкомиссии России (Сертификат N 361 от 18 сентября 2000 г.).

Nessus предоставляет очень широкие возможности по поиску уязвимостей корпоративных сетей и исследованию структуры сетевых сервисов. Помимо использования стандартных способов сканирования TCP и UDP портов, Nessus позволяет осуществлять поиск уязвимостей в реализациях протоколов управления сетью ICMP и SNMP.

Высокая скорость сканирования достигается за счет использования при реализации сканера Nessus многопотоковой архитектуры программирования, позволяющей осуществлять одновременное параллельное сканирование сетевых хостов. Для сканирования каждого хоста сервером nessusd создается отдельный поток выполнения.

При реализации Nessus использована нетипичная для сетевых сканеров клиент/серверная архитектура. Взаимодействие между клиентом и сервером осуществляется по защищенному клиент-серверному протоколу, предусматривающему использование надежной схемы аутентификации и шифрование передаваемых данных.

Все сценарии сканирования разделены на группы по типам реализуемых ими сетевых атак, обнаруживаемых уязвимостей, а также по видам тестируемых сетевых сервисов. Так, имеются специальные группы сценариев:

Backdoors для обнаружения "троянских" программ:

Gain Shell Remotely - для реализации атак на получение пользовательских полномочий на удаленной UNIX системе;

Firewalls - для тестирования МЭ;

FTP - для тестирования FTP-серверов;

Windows - для поиска уязвимостей Windows-систем и т.п.

Особую группу сценариев сканирования Denail of Service составляют атаки на отказ в обслуживании (DoS). Единственный способ убедиться в том, что сканируемая система подвержена той или иной DoS - это выполнить эту атаку и посмотреть на реакцию системы. Эта группа сценариев, однако, является потенциально опасной, т.к. их запуск может привести к непредсказуемым последствиям для сканируемой сети, включая сбои в работе серверов и рабочих станций, потерю данных и "полный паралич" корпоративной сети. Поэтому большинство DoS в данной группе по умолчанию отключено.

7.2.5. Архитектура систем аудита

У систем активного аудита целесообразно различать локальную и глобальную архитектуру.

Локальная архитектура

В рамках локальной архитектуры реализуются элементарные составляющие, которые затем могут быть объединены для обслуживания корпоративных систем.

Основные элементы локальной архитектуры и связи между ними показаны на рисунке 7.3. Первичный сбор данных осуществляют агенты, называемые также *сенсорами.* Регистрационная информация может извлекаться из системных или прикладных журналов (технически несложно получать ее и напрямую от ядра ОС), либо добываться из сети с помощью соответствующих механизмов активного сетевого оборудования или путем перехвата пакетов посредством установленной в режим мониторинга сетевой карты.

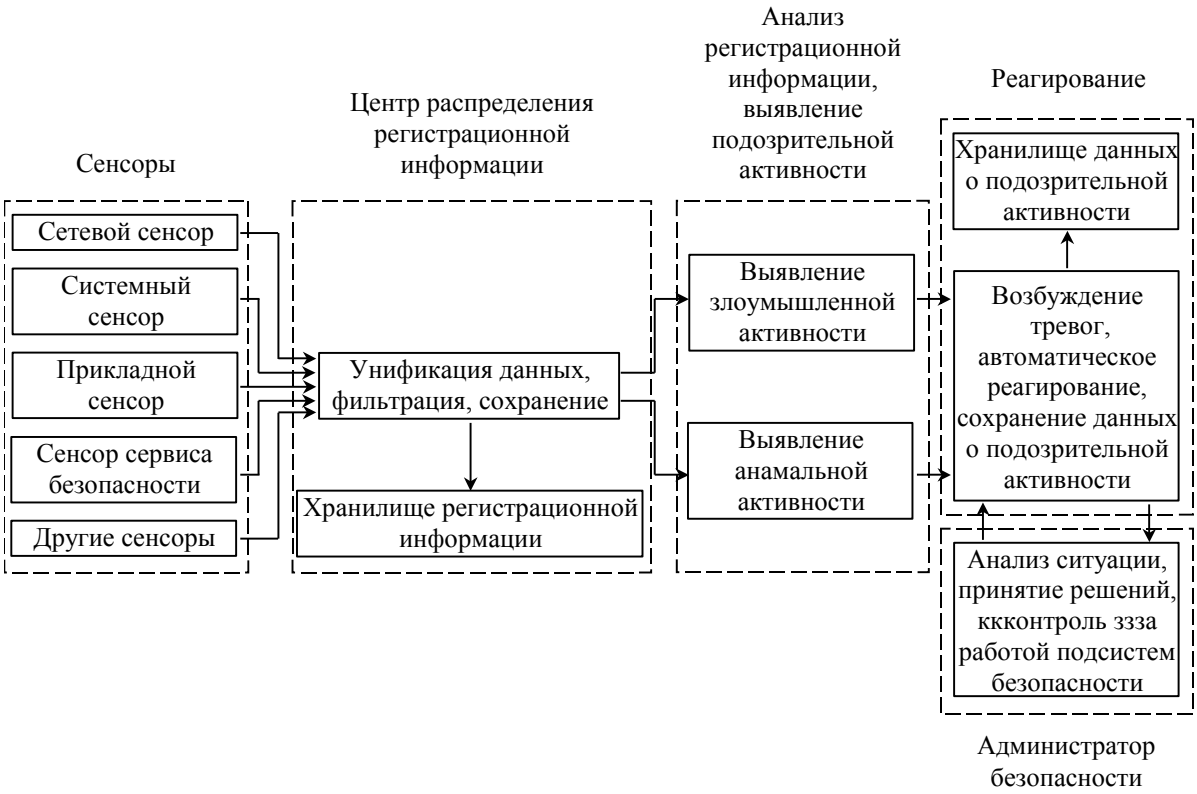


Рис. 7.3. Основные элементы локальной архитектуры систем активного аудита.

На уровне агентов (сенсоров) может выполняться фильтрация данных с целью уменьшения их объема. Это требует от агентов некоторого интеллекта, но зато разгружает остальные компоненты системы.

Агенты передают информацию в центр распределения, который приводит ее к единому (стандартному для конкретной системы активного аудита) формату, возможно, осуществляет дальнейшую фильтрацию (редукцию), сохраняет в базе данных и направляет для анализа статистическому и экспертному компонентам. Один центр распределения может обслуживать несколько сенсоров.

Содержательный активный аудит начинается со статистического и экспертного компонентов (например, потому, что для однохостовых систем регистрационную информацию не надо каким-то особым образом извлекать и передавать). Мы детально рассмотрим их в двух следующих разделах.

Если в процессе статистического или экспертного анализа выявляется подозрительная активность, соответствующее сообщение направляется решателю, который определяет, является ли тревога оправданной, и выбирает способ реагирования.

Обычно, когда пишут о способах реагирования, перечисляют отправку сообщения на пейджер администратора, посылку электронного письма ему же и т.п., то есть имеют в виду “ручное” принятие мер после получения сигнала о подозрительной активности. К сожалению, многие современные атаки длятся секунды или даже доли секунды, поэтому включение в процесс реагирования человека вносит недопустимо большую задержку. Ответные меры должны быть в максимально возможной степени автоматизированы, иначе активность аудита во многом теряет смысл.

Автоматизация нужна еще и по той простой причине, что далеко не во всех организациях системные администраторы обладают достаточной квалификацией для адекватного реагирования на инциденты. Хорошая система активного аудита должна уметь внятно объяснить, почему она подняла тревогу, насколько серьезна ситуация и каковы

рекомендуемые способы действия. Если выбор должен оставаться за человеком, то пусть он сводится к нескольким элементам меню, а не к решению концептуальных проблем.

Глобальная архитектура

Глобальная архитектура подразумевает организацию одно- и разно-ранговых связей между локальными системами активного аудита (см. рисунок 7.4). На одном уровне иерархии располагаются компоненты, анализирующие подозрительную активность с разных точек зрения. Например, на хосте могут располагаться подсистемы анализа поведения пользователей и приложений. Их может дополнять подсистема анализа сетевой активности. Когда один компонент обнаруживает что-то подозрительное, то во многих случаях целесообразно сообщить об этом соседям либо для принятия мер, либо для усиления внимания к определенным аспектам поведения системы.

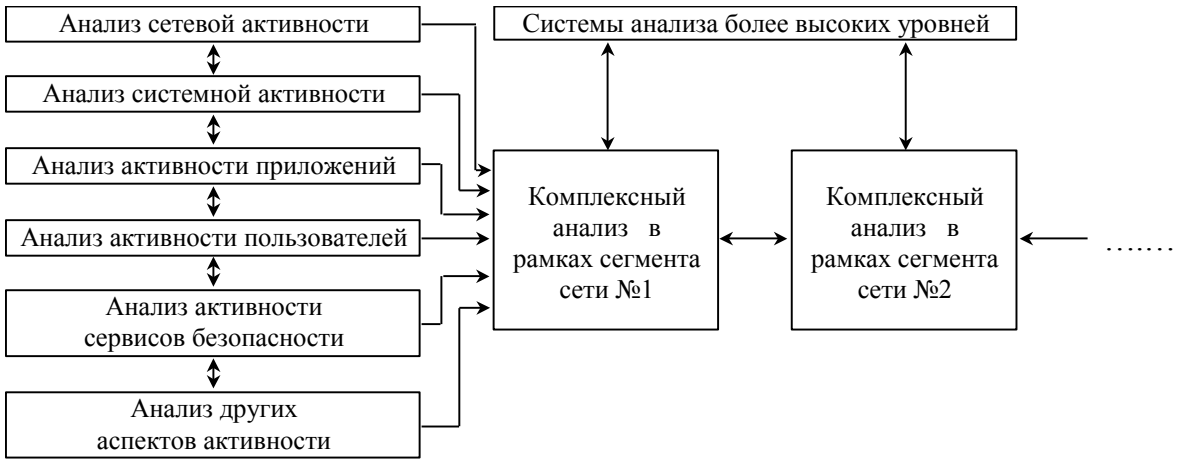


Рис. 7.4. Глобальная архитектура системы активного аудита.

Разно-ранговые связи используются для обобщения результатов анализа и получения целостной картины происходящего. Иногда у локального компонента недостаточно оснований для возбуждения тревоги, но «по совокупности» подозрительные ситуации могут быть объединены и совместно проанализированы, после чего порог подозрительности окажется превышенным. Целостная картина, возможно, позволит выявить скоординированные атаки на разные участки информационной системы и оценить ущерб в масштабе организации.

Очевидно, формирование иерархии компонентов активного аудита необходимо и для решения проблем масштабируемости, но этот аспект является стандартным для систем управления и мы не будем на нем останавливаться.

К числу важнейших архитектурных относится вопрос о том, какую информацию и в каких масштабах собирать и анализировать. Первые системы активного аудита были однохостовыми. Затем появились многохостовые конфигурации. Прорыву в области коммерческих продуктов мы обязаны сетевым системам, анализировавшим исключительно сетевые пакеты.

В настоящее время можно наблюдать конвергенцию архитектур, в результате чего рождаются комплексные системы, отслеживающие и анализирующие как компьютерную, так и сетевую регистрационную информацию.

Традиционным является вопрос: где размещать сенсоры систем активного аудита?

Столь же традиционный ответ гласит: «везде, где можно». Только анализ всех доступных источников информации позволит с достоверностью обнаруживать атаки и злоупотребления полномочиями и докапываться до их первопричин. Если вернуться к

трактовке информационной системы в виде совокупности сервисов, то средства обнаружения атак должны располагаться перед защищаемыми ресурсами (имея в виду направление движения запросов к сервисам), а средства выявления злоупотреблений полномочиями - на самих сервисах. Обнаружение аномальной активности полезно во всех упомянутых точках. Только при таком размещении сенсоров будет выполнен важнейший принцип невозможности обхода защитных средств. Кроме того, будет минимизировано число сенсоров, что в условиях сегментации сетей и применения коммутационных технологий также оказывается проблемой.

Для того, чтобы система активного аудита, особенно распределенная, была практически полезной, необходимо обеспечить целостность анализируемой и передаваемой информации, а также целостность самой программной системы и ее живучесть в условиях отказа или компрометации отдельных компонентов (зачастую атака направляется сначала на средства безопасности, а уже потом - на прикладные компоненты). Ясно, что это проблема всех распределенных систем, и для ее решения служат сервисы взаимной аутентификации и контроля целостности (в том числе проверка подлинности источника данных).

7.2.6. Требования к системам активного аудита

В этом пункте рассмотрим требования к системам активного аудита, существенные с точки зрения заказчиков. На первое место следует поставить требование полноты. Это весьма емкое понятие, включающее в себя следующие аспекты:

Полнота отслеживания информационных потоков к сервисам. Активный аудит должен охватывать все потоки всех сервисов. Это означает, что система активного аудита должна содержать сетевые и системные сенсоры, анализировать информацию на всех уровнях - от сетевого до прикладного. Очевидно, из рассматриваемого аспекта полноты вытекает требование расширяемости, поскольку ни один программный продукт не может быть изначально настроен на все сервисы.

Полнота спектра выявляемых атак и злоупотреблений полномочиями. Данное требование означает не только то, что у системы должен быть достаточно мощный язык описания подозрительной активности (как атак, так и злоупотреблений полномочиями). Этот язык должен быть прост, чтобы заказчики могли производить настройку системы в соответствии со своей политикой безопасности. Поставщик системы активного аудита должен в кратчайшие сроки (порядка суток) передавать заказчику сигнатуры новых атак. Система должна уметь выявлять аномальную активность, чтобы справляться с заранее неизвестными способами нарушений.

Достаточная производительность. Система активного аудита должна справляться с пиковыми нагрузками защищаемых сервисов.

Пропуск даже одного сетевого пакета может дать злоумышленнику шанс на успешную атаку. Если известно, что система активного аудита обладает недостаточной производительностью, она может стать объектом атаки на доступность, на фоне которой будут развиваться другие виды нападения. Для локальных сетей стандартными стали скорости 100 Мбит/с. Это требует от системы активного аудита очень высокого качества реализации, мощной аппаратной поддержки. Если учесть, что защищаемые сервисы находятся в постоянном развитии, то станет понятно, что требование производительности одновременно является и требованием масштабируемости.

Помимо полноты, системы активного аудита должны удовлетворять следующим требованиям:

Минимум ложных тревог. В абсолютном выражении допустимо не более одной ложной тревоги в час (лучше, если их будет еще на порядок меньше). При интенсивных потоках данных между сервисами и их клиентами подобное требование оказывается весьма жестким. Пусть, например, в секунду по контролируемому каналу проходит 1000 пакетов. За час пакетов будет 3 600 000. Можно предположить, что почти все они не являются

злоумышленными. И только один раз система активного аудита имеет право принять «своего» за «чужого», то есть вероятность ложной тревоги должна составлять в данном случае не более $3 \cdot 10^{-7}$.

Умение объяснять причину тревоги. Выполнение этого требования во-первых, помогает отличить обоснованную тревогу от ложной, во-вторых, помогает определить первопричину инцидента, что важно для оценки его последствий и недопущения повторных нарушений. Даже если реагирование на нарушение производится в автоматическом режиме, должна оставаться возможность последующего разбора ситуации специалистами.

Интеграция с системой управления и другими сервисами безопасности. Интеграция с системой управления имеет две стороны. Во-первых, сами средства активного аудита должны управляться (устанавливаться, конфигурироваться, контролироваться) наравне с другими инфраструктурными сервисами. Во-вторых, активный аудит может (и должен) поставлять данные в общую базу данных управления. Интеграция с сервисами безопасности необходима как для лучшего анализа ситуации (например, с привлечением средств контроля целостности), так и для оперативного реагирования на нарушения (средствами приложений, операционных систем или межсетевых экранов).

Наличие технической возможности удаленного мониторинга информационной системы. Это спорное требование, поскольку не все организации захотят оказаться под чьим-то «колпаком». Тем не менее, с технической точки зрения подобная мера вполне оправдана, поскольку большинство организаций не располагает квалифицированными специалистами по информационной безопасности. Удаленный мониторинг может быть использован и для бесспорных целей, таких как контроль из штаб-квартиры за работой удаленных отделений.

Сформулированные требования можно считать максималистскими. По-видимому, ни одна современная коммерческая система, ни один поставщик не удовлетворяют им в полной мере, однако, без их выполнения активный аудит превращается из серьезного оборонительного оружия в сигнализацию для отпугивания детей младшего школьного возраста. Захотят ли заказчики платить деньги за подобные игрушки? Нет, конечно, если только они достаточно разбираются в предмете.

Системы активного аудита принадлежат к области высоких технологий. У них развитая математическая база, продвинутая архитектура, они вобрали в себя знания по информационной безопасности. Мало кто из распространителей понимает, как работает то, что они продают; им остается пересказывать рекламные буклеты производителей, где, конечно, все выглядит замечательно. Заказчики тоже не обязаны вдаваться в детали, но они должны знать, о чем спрашивать поставщиков. Не всегда те смогут ответить, но и молчание многое скажет заказчику.

7.2.7. Возможные критерии оценки систем активного аудита

Предлагаемые критерии имеют много общего с критериями оценки систем управления. Это не случайно, так как активный аудит и управление по сути своей близки.

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся нетипичным для данного пользователя (компонента) или (в соответствии с заранее определенными критериями) злоумышленным.

Рассматриваемые в данных критериях системы должны выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нетипичные или злоумышленные действия. Кроме того, они должны удовлетворять общим требованиям к сервисам информационной безопасности.

Основными показателями, характеризующими системы активного аудита, являются:

спектр контролируемых объектов;

спектр и степень детальности отслеживаемых характеристик;

расширяемость системы;

настраиваемость системы;
степень автоматизации функционирования системы;
возможность работы в рамках распределенных систем;
возможность работы в реальном масштабе времени;
технологичность системы.

Показатели, используемые для оценки систем активного аудита

Выделяются следующие показатели:
Отслеживание поведения пользователей и компонентов информационной системы.
Обеспечение конфиденциальности и целостности регистрационной информации.
Выявление злоумышленного поведения.
Выявление нетипичного поведения.
Администрирование.
Контроль целостности.
Масштабируемость.
Доступность.
Восстановление.
Документация.
Тестирование.

Отслеживание поведения пользователей и компонентов информационной системы

Возможность отслеживания базового набора характеристик поведения пользователей и компонентов информационной системы.

Возможность изменения (в том числе пополнения) набора отслеживаемых характеристик.

Возможность отслеживания характеристик в распределенных системах.

Возможность отслеживания поведения отдельных пользователей и компонентов информационной системы в реальном масштабе времени.

Возможность задания способа информирования администратора безопасности о выходе отслеживаемых характеристик за допустимые рамки.

Возможность задания способа автоматического реагирования на выход отслеживаемых характеристик за допустимые рамки.

Обеспечение конфиденциальности и целостности регистрационной информации

Защита регистрационной информации от несанкционированного доступа в рамках отдельных систем.

Контроль целостности (взаимной согласованности) регистрационной информации в рамках распределенных систем.

Защита регистрационной информации от несанкционированного доступа в рамках распределенных систем.

Возможность задания способа информирования администратора безопасности о нарушении целостности и/или конфиденциальности регистрационной информации.

Возможность задания способа автоматического реагирования на нарушение целостности и/или конфиденциальности регистрационной информации.

Выявление злоумышленного поведения

Возможность выявления базового набора злоумышленных действий.

Возможность пополнения базы правил, описывающих злоумышленные действия.

Возможность настройки базы правил на конкретные информационные сервисы.

Возможность выявления злоумышленных действий, распределенных во времени

Возможность выявления злоумышленных действий в распределенных системах

Возможность выявления злоумышленных действий в реальном масштабе времени

Возможность задания способа информирования администратора безопасности о выявленных злоумышленных действиях.

Возможность задания уровня детализации информации, подтверждающей наличие злоумышленных действий.

Возможность задания способа автоматического реагирования на выявленные злоумышленные действия.

Наличие средств автоматической проверки согласованности базы правил в рамках распределенной конфигурации.

Наличие средств анализа злоумышленных действий с выдачей рекомендаций по предотвращению подобных действий в будущем.

Наличие средств прогнозирования злоумышленных действий.

Выявление нетипичного поведения.

Наличие подсистемы статистического анализа для выявления нетипичного поведения.

Возможность выявления нетипичного поведения при использовании базового набора информационных сервисов.

Возможность пополнения и/или изменения набора контролируемых аспектов поведения.

Возможность настройки на конкретные информационные сервисы.

Наличие средств для изменения параметров статистического анализа с целью обеспечения заданного соотношения между ошибками первого рода (отсутствие реакции на нетипичное поведение) и ошибками второго рода (ложное срабатывание).

Возможность выявления нетипичного поведения в рамках распределенной системы.

Возможность выявления нетипичного поведения в реальном масштабе времени

Возможность задания способа информирования администратора безопасности о выявленном нетипичном поведении.

Возможность задания уровня детализации информации, подтверждающей наличие нетипичного поведения

Возможность задания способа автоматического реагирования на выявленное нетипичное поведение

Наличие средств автоматической проверки согласованности статистических параметров в рамках распределенной конфигурации

Наличие средств автоматической оценки соотношения между ошибками первого и второго рода при заданных статистических параметрах

Администрирование

Идентификация и аутентификация администраторов в рамках локальных систем

Идентификация и аутентификация администраторов в рамках распределенных систем

Регистрация административных действий в рамках локальных систем

Регистрация административных действий в рамках распределенных систем

Возможность централизованного выявления подозрительной активности в рамках распределенных систем

Возможность централизованного администрирования распределенных систем активного аудита

Контроль целостности

Наличие средств контроля целостности программной и информационной частей системы активного аудита (локальные, распределенные, использующие аттестованные алгоритмы)

Масштабируемость

Наличие средств масштабирования по числу отслеживаемых пользователей и компонентов информационной системы: возможность группирования пользователей (компонентов) с однородными характеристиками.

Наличие средств масштабирования по размеру обслуживаемой информационной системы, возможность варьирования между распределенной и централизованной обработкой регистрационной информации, возможность организации иерархии обрабатывающих центров.

Доступность

Наличие средств обеспечения высокой доступности: сбои и отказы отдельных подсистем или компонентов системы активного аудита не должны нарушать работоспособность других подсистем (компонентов).

Восстановление

Наличие средств восстановления после сбоев и отказов, в том числе отказов отдельных элементов распределенной системы.

Документация

Руководство администратора системы активного аудита (локальные, распределенные, с использованием аттестованных алгоритмов контроля целостности).

Руководство программиста (описание программных интерфейсов с системой сбора и анализа регистрационной информации).

Конструкторская (проектная) документация.

Тестовая документация.

Тестирование

Обеспечение возможности регламентного тестирования средств сбора регистрационной информации, подсистем выявления злоумышленного и нетипичного поведения, средств контроля целостности, средств администрирования, средств восстановления.

7.2.8. Результаты аудита

Результаты аудита ИС организации можно разделить на три основных группы:

1 Организационные: планирование, управление, документооборот функционирования ИС.

2 Технические: сбои, неисправности, оптимизация работы элементов ИС, непрерывное обслуживание, создание инфраструктуры и т.д.

3 Методологические: подходы к решению проблемных ситуаций, управлению и контролю, общая упорядоченность и структуризация.

Проведенный аудит позволит обоснованно создать следующие документы:

Долгосрочный план развития ИС.

Политика безопасности ИС организации.

Методология работы и доводки ИС организации.

План восстановления ИС в чрезвычайной ситуации.

Заключение

Прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий дает сильный толчок к развитию средств обеспечения безопасности, что требует во многом предусмотреть научную парадигму информационной безопасности. Теория информационной безопасности – одна из самых развивающихся естественных наук.

Основными положениями информационной безопасности являются:

Исследование и анализ причин нарушения безопасности информационных систем.

Разработка эффективных моделей безопасности, адекватных современной степени развития программных и аппаратных средств, а также возможностям злоумышленников и разрушающим программным средствам.

Создание методов и средств корректного внедрения моделей безопасности в существующие АС, с возможностью гибкого управления безопасностью в зависимости от выдвигаемых требований, допускаемого риска и расхода ресурсов.

Необходимость разработки средств анализа безопасности информационных систем с помощью осуществления тестовых воздействий.

Особую роль в развитии теории информационной безопасности как науки так и отрасли промышленности играют центры компьютерной безопасности. К ним относятся государственные, общественные и коммерческие организации, а также неформальные объединения, основное направление деятельности которых – координация усилий, направленных на актуализацию проблем защиты информации, проведение теоретических исследований и разработка конкретных практических решений в области безопасности, аналитическая деятельность и прогнозирование.

В Российской Федерации такими центрами являются Государственная техническая комиссия при президенте Российской Федерации, Институт криптографии, связи и информатики Академии федеральной службы безопасности, Академия криптографии Российской Федерации.

Литература

1. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001. - 352 с.
2. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000. – 192 с.
3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
4. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с.
5. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. - М.: Издательство Агенства "Яхтсмен", 1996.
6. Теория и практика обеспечения информационной безопасности. Под редакцией Зегжды П.Д. - М.: Издательство Агенства "Яхтсмен", 1996.
7. Баранов А.П., Зегжда Д.П., Ивашко А.М., Корт С.С. Теоретические основы информационной безопасности (дополнительные главы). Учебное пособие – ЦОП СпбГУ, Санкт-Петербург, 1998.
8. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC), DOD, 1985.
9. Сборник руководящих документов по защите информации от несанкционированного доступа. - М.: Гостехкомиссия, 1998.

10. Основы информационной безопасности / Галатенко В.А. Под редакцией члена-корреспондента РАН В.Б. Бетелина / - М.: ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», 2003. – 280 с.
11. Петренко С.А., Петренко А.А. Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 416 с.
12. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2001. – 264 с.