В. Ф. Шаньгин

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Рекомендовано Министерством образования Российской Федерации в качестве учебного пособия для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей 2200 «Информатика и вычислительная техника»

Москва
ИД «ФОРУМ» — ИНФРА-М
2008

УДК 002.56(075.32)
ББК 32.973я723
Ш20

Рецензенты:
доктор технических наук, профессор, зав. кафедрой «Информатика и программное обеспечение вычислительных систем» Московского государственного института электронной техники (Технического университета) *Л. Г. Гагарина*;
начальник ОМТС «Кедах Электроникс Инжиниринг» *С. А. Костина*

Шаньгин В. Ф.
Ш20 Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2008. — 416 с.: ил. — (Профессиональное образование).

ISBN 978-5-8199-0331-5 (ИД «ФОРУМ»)
ISBN 978-5-16-003132-3 (ИНФРА-М)

В учебном пособии формулируются основные понятия и определения информационной безопасности и анализируются угрозы информационной безопасности в компьютерных системах и сетях. Определяются базовые понятия политики безопасности. Рассматриваются основные криптографические методы и алгоритмы защиты компьютерной информации.

Обосновывается комплексный подход к обеспечению информационной безопасности корпоративных сетей. Описываются базовые технологии защиты межсетевого обмена данными. Рассматриваются методы и средства антивирусной защиты. Описывается организационно-правовое обеспечение информационной безопасности на основе стандартов и руководящих документов Государственной технической комиссии России.

Предназначено в качестве учебного пособия для студентов, обучающихся по соответствующим специальностям.

УДК 002.56(075.32)
ББК 32.973я723

ISBN 978-5-8199-0331-5 (ИД «ФОРУМ»)
ISBN 978-5-16-003132-3 (ИНФРА-М)

Предисловие

Быстрый рост глобальной сети Internet и стремительное развитие информационных технологий привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Новые технологические возможности облегчают распространение информации, повышают эффективность производственных процессов, способствуют расширению деловых отношений. Однако несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается. Поэтому проблемы обеспечения информационной безопасности привлекают пристальное внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей, включая компании, работающие в сфере электронного бизнеса.

Без знания и квалифицированного применения современных технологий, стандартов, протоколов и средств защиты информации невозможно достигнуть требуемого уровня информационной безопасности компьютерных систем и сетей.

Предлагаемая вниманию читателя книга посвящена систематическому изложению и анализу современных методов, средств и технологий защиты информации в компьютерных системах и сетях. Автор старался изложить материал максимально доступно без потери в качестве.

Основное содержание книги, состоящее из семнадцати глав, разбито на пять логически связанных частей.

Каждая из этих частей объединяет несколько глав, связанных общей темой.

Книга содержит также список основных сокращений.

Весь материал книги базируется только на открытых публикациях в Internet, отечественной и зарубежной печати. В основу книги положены материалы лекций, читаемых автором в Мос-

ковском институте электронной техники, результаты научных и проектных работ, связанных с созданием комплексных систем защиты информационных ресурсов организаций и предприятий с распределенными подразделениями и филиалами, а также использованы некоторые материалы публикаций преподавателей и сотрудников Института криптографии, связи и информатики Академии ФСБ России [55, 56, 63].

Автор заранее благодарен читателям, которые пришлют ему свои замечания и пожелания.

Введение

Интернет сегодня — это технология, кардинально меняющая весь уклад нашей жизни: темпы научно-технического прогресса, характер работы, способы общения. Эффективное применение информационных технологий является общепризнанным стратегическим фактором роста конкурентоспособности компании. Многие предприятия в мире переходят к использованию широких возможностей Интернета и электронного бизнеса, неотъемлемый элемент которого — электронные транзакции (по Интернету и другим публичным сетям).

Электронная коммерция, продажа информации в режиме on-line и многие другие услуги становятся основными видами деятельности для многих компаний, а их корпоративные информационные системы (КИС) — главным инструментом управления бизнесом и, фактически, важнейшим средством производства.

Важным фактором, влияющим на развитие КИС предприятия, является поддержание массовых и разнообразных связей предприятия через Интернет с одновременным обеспечением безопасности этих коммуникаций. Поэтому решение проблем информационной безопасности, связанных с широким распространением Internet, Intranet и Extranet — одна из самых актуальных задач, стоящих перед разработчиками и поставщиками информационных технологий.

Задача обеспечения информационной безопасности КИС традиционно решается построением *системы информационной безопасности* (СИБ), определяющим требованием к которой является сохранение вложенных в построение КИС инвестиций. Иначе говоря, СИБ должна функционировать абсолютно прозрачно для уже существующих в КИС приложений и быть полностью совместимой с используемыми в КИС сетевыми технологиями.

Создаваемая СИБ предприятия должна учитывать появление новых технологий и сервисов, а также удовлетворять общим требованиям, предъявляемым сегодня к любым элементам КИС, таким как:

- *применение открытых стандартов*;
- *использование интегрированных решений*;
- *обеспечение масштабирования в широких пределах.*

Переход на открытые стандарты составляет одну из главных тенденций развития средств информационной безопасности. Такие стандарты как IPSec и PKI обеспечивают защищенность внешних коммуникаций предприятий и совместимость с соответствующими продуктами предприятий-партнеров или удаленных клиентов. Цифровые сертификаты X.509 также являются на сегодня стандартной основой для аутентификации пользователей и устройств. Перспективные средства защиты безусловно должны поддерживать эти стандарты сегодня.

Под *интегрированными решениями* понимается как интеграция средств защиты с остальными элементами сети (ОС, маршрутизаторами, службами каталогов, серверами QoS-политики и т. п.), так и интеграция различных технологий безопасности между собой для обеспечения *комплексной защиты* информационных ресурсов предприятия, например интеграция межсетевого экрана с VPN-шлюзом и транслятором IP-адресов.

По мере роста и развития КИС система информационной безопасности должна иметь возможность легко масштабироваться без потери целостности и управляемости. *Масштабируемость средств защиты* позволяет подбирать оптимальное по стоимости и надежности решение с возможностью постепенного наращивания системы защиты. Масштабирование обеспечивает эффективную работу предприятия при наличии у него многочисленных филиалов, десятков предприятий-партнеров, сотен удаленных сотрудников и миллионов потенциальных клиентов.

Для того чтобы обеспечить надежную защиту ресурсов КИС, в СИБ должны быть реализованы самые прогрессивные и перспективные технологии информационной защиты. К ним относятся:

- *криптографическая защита данных* для обеспечения конфиденциальности, целостности и подлинности информации;
- *технологии аутентификации* для проверки подлинности пользователей и объектов сети;

- *технологии межсетевых экранов* для защиты корпоративной сети от внешних угроз при подключении к общедоступным сетям связи;
- *технологии виртуальных защищенных каналов и сетей VPN* для защиты информации, передаваемой по открытым каналам связи;
- *гарантированная идентификация пользователей* путем применения токенов (смарт-карт, touch-memory, ключей для USB-портов и т. п.) и других средств аутентификации;
- *управление доступом на уровне пользователей* и защита от несанкционированного доступа к информации;
- *поддержка инфраструктуры управления открытыми ключами PKI;*
- *технологии обнаружения вторжений* (*Intrusion Detection*) для активного исследования защищенности информационных ресурсов;
- *технологии защиты от вирусов* с использованием специализированных комплексов антивирусной профилактики и защиты;
- *централизованное управление СИБ* на базе единой политики безопасности предприятия;
- *комплексный подход к обеспечению информационной безопасности*, обеспечивающий рациональное сочетание технологий и средств информационной защиты.

Часть 1
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Применение информационных технологий (ИТ) требует повышенного внимания к вопросам информационной безопасности. Разрушение информационного ресурса, его временная недоступность или несанкционированное использование могут нанести компании значительный материальный ущерб. Без должной степени защиты информации внедрение ИТ может оказаться экономически невыгодным в результате значительных потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях.

Реализация решений, обеспечивающих безопасность информационных ресурсов, существенно повышает эффективность всего процесса информатизации в организации, обеспечивая целостность, подлинность и конфиденциальность дорогостоящей деловой информации, циркулирующей в локальных и глобальной информационных средах.

Глава 1
ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Новые ИТ активно внедряются во все сферы народного хозяйства. Появление локальных и глобальных сетей передачи данных предоставило пользователям компьютеров новые возможности для оперативного обмена информацией. Развитие Internet привело к использованию глобальных сетей передачи данных в повседневной жизни практически каждого человека. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им ИТ.

1.1. Основные понятия защиты информации и информационной безопасности

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития ИТ.

Рассмотрим основные понятия защиты информации и информационной безопасности компьютерных систем и сетей с учетом определений ГОСТ Р 50922—96 [14, 62].

Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации — это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации — степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки — деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

Защита информации от разглашения — деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от НСД — деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим НСД к защищаемой информации, может выступать государство, юридическое лицо, группа физических лиц, в т. ч. общественная организация, отдельное физическое лицо.

Система защиты информации — совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Под *информационной безопасностью* понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной.

Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, и стихийные бедствия (землетрясение, ураган, пожар) и т. п.

Современная *автоматизированная система* (АС) *обработки информации* представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. *Компоненты АС* можно разбить на следующие группы:

- *аппаратные средства* — компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства — дисководы, принтеры, контроллеры, кабели, линии связи и т. д.);
- *программное обеспечение* — приобретенные программы, исходные, объектные, загрузочные модули; ОС и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;
- *данные* — хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;
- *персонал* — обслуживающий персонал и пользователи.

Одной из особенностей обеспечения информационной безопасности в АС является то, что таким абстрактным понятиям, как информация, объекты и субъекты системы, соответствуют физические представления в компьютерной среде:

- *для представления информации — машинные носители информации* в виде внешних устройств компьютерных систем (терминалов, печатающих устройств, различных накопителей, линий и каналов связи), оперативной памяти, файлов, записей и т. д.;
- *объектам системы* — пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем информации;
- *субъектам системы* — активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы.

Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и дос-

товерности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы. Перечисленные выше *базовые свойства информации* нуждаются в более полном толковании.

Конфиденциальность данных — это статус, предоставленный данным и определяющий требуемую степень их защиты. К конфиденциальным данным можно отнести, например, следующие: личную информацию пользователей; учетные записи (имена и пароли); данные о кредитных картах; данные о разработках и различные внутренние документы; бухгалтерские сведения. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Установление градаций важности защиты защищаемой информации (объекта защиты) называют *категорированием защищаемой информации.*

Под *целостностью информации* понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, т. е. если не произошло их случайного или преднамеренного искажения или разрушения. Обеспечение целостности данных является одной из сложных задач защиты информации.

Достоверность информации — свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Юридическая значимость информации означает, что документ, являющийся носителем информации, обладает юридической силой.

Доступность данных. Работа пользователя с данными возможна только в том случае, если он имеет к ним доступ.

Доступ к информации — получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств. *Субъект доступа к информации* — участник правоотношений в информационных процессах.

Оперативность доступа к информации — это способность информации или некоторого информационного ресурса быть дос-

тупными для конечного пользователя в соответствии с его оперативными потребностями.

Собственник информации — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Владелец информации — субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Пользователь (потребитель) информации — субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Право доступа к информации — совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации.

Правило доступа к информации — совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации — это доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ к информации — нарушение установленных правил разграничения доступа. Лицо или процесс, осуществляющие НСД к информации, являются нарушителями правил разграничения доступа. НСД является наиболее распространенным видом компьютерных нарушений.

Ответственным за защиту компьютерной системы от НСД к информации является *администратор защиты.*

Доступность информации подразумевает также *доступность компонента* или *ресурса* компьютерной системы, т. е. свойство компонента или ресурса быть доступным для законных субъектов системы. Примерный перечень ресурсов, которые могут быть доступны, включает: принтеры, серверы, рабочие станции, данные пользователей, любые критические данные, необходимые для работы.

Целостность ресурса или *компонента системы* — это свойство ресурса или компонента быть неизменным в семантическом

смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий.

С допуском к информации и ресурсам системы связана группа таких важных понятий, как идентификация, аутентификация, авторизация. С каждым субъектом системы (сети) связывают некоторую информацию (число, строку символов), идентифицирующую субъект. Эта информация является *идентификатором* субъекта системы (сети). Субъект, имеющий зарегистрированный идентификатор, является *законным* (*легальным*) *субъектом*. *Идентификация субъекта* — это процедура распознавания субъекта по его идентификатору. Идентификация выполняется при попытке субъекта войти в систему (сеть). Следующим шагом взаимодействия системы с субъектом является аутентификация субъекта. *Аутентификация субъекта* — это проверка подлинности субъекта с данным идентификатором. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил. После идентификации и аутентификации субъекта выполняют процедуру авторизации. *Авторизация субъекта* — это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Под *угрозой безопасности* АС понимаются возможные действия, способные прямо или косвенно нанести ущерб ее безопасности. *Ущерб безопасности* подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в системе (сети). С понятием угрозы безопасности тесно связано понятие уязвимости компьютерной системы (сети). *Уязвимость компьютерной системы* — это присущее системе неудачное свойство, которое может привести к реализации угрозы. *Атака* на компьютерную систему — это поиск и/или использование злоумышленником той или иной уязвимости системы. Иными словами, атака — это реализация угрозы безопасности.

Противодействие угрозам безопасности является целью средств защиты компьютерных систем и сетей.

Защищенная система — это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации — техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации

Комплекс средств защиты (КСЗ) — совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы (сети). КСЗ создается и поддерживается в соответствии с принятой в данной организации политикой безопасности.

Техника защиты информации — средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Корпоративные сети относятся к распределенным автоматизированным системам (АС), осуществляющим обработку информации. Обеспечение безопасности АС предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования АС, а также попыткам модификации, хищения, выведения из строя или разрушения ее компонентов, т. е. защиту всех компонентов АС — аппаратных средств, программного обеспечения (ПО), данных и персонала. Конкретный подход к проблеме обеспечения безопасности основан на разработанной для АС политике безопасности [30, 63].

Политика безопасности — это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы от заданного множества угроз. Более подробные сведения о видах политики безопасности и процессе ее разработки приводятся в гл. 3.

1.2. Анализ угроз информационной безопасности

Под *угрозой* (в общем смысле) обычно понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам. В дальнейшем под *угрозой безопасности* АС обработки информации будем понимать возможность воздействия на АС, которое прямо или косвенно может нанести ущерб ее безопасности.

В настоящее время известен обширный перечень угроз информационной безопасности АС, содержащий сотни позиций.

Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе защиты.

Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты АС. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Необходимость классификации угроз информационной безопасности АС обусловлена тем, что хранимая и обрабатываемая информация в современных АС подвержена воздействию чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Поэтому для защищаемой системы обычно определяют не полный перечень угроз, а перечень классов угроз.

Классификация возможных угроз информационной безопасности АС может быть проведена по следующим базовым признакам [63].

1. По природе возникновения:

- *естественные угрозы*, вызванные воздействиями на АС объективных физических процессов или стихийных природных явлений;
- *искусственные угрозы* безопасности АС, вызванные деятельностью человека.

2. По степени преднамеренности проявления:

- *угрозы, вызванные ошибками или халатностью* персонала, например некомпетентное использование средств защиты, ввод ошибочных данных и т. п.;
- *угрозы преднамеренного действия*, например действия злоумышленников.

3. По непосредственному источнику угроз:

- *природная среда*, например стихийные бедствия, магнитные бури и пр.;
- *человек*, например вербовка путем подкупа персонала, разглашение конфиденциальных данных и т. п.;
- *санкционированные программно-аппаратные средства*, например удаление данных, отказ в работе ОС;

- *несанкционированные программно-аппаратные средства*, например заражение компьютера вирусами с деструктивными функциями.

4. По положению источника угроз:

- *вне контролируемой зоны АС*, например перехват данных, передаваемых по каналам связи, перехват побочных электромагнитных, акустических и других излучений устройств;
- *в пределах контролируемой зоны АС*, например применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т. п.;
- *непосредственно в АС*, например некорректное использование ресурсов АС.

5. По степени зависимости от активности АС:

- *независимо от активности АС*, например вскрытие шифров криптозащиты информации;
- *только в процессе обработки данных*, например угрозы выполнения и распространения программных вирусов.

6. По степени воздействия на АС:

- *пассивные угрозы*, которые при реализации ничего не меняют в структуре и содержании АС, например угроза копирования секретных данных;
- *активные угрозы*, которые при воздействии вносят изменения в структуру и содержание АС, например внедрение троянских коней и вирусов.

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

- *угрозы, проявляющиеся на этапе доступа к ресурсам АС*, например угрозы несанкционированного доступа в АС;
- *угрозы, проявляющиеся после разрешения доступа к ресурсам АС*, например угрозы несанкционированного или некорректного использования ресурсов АС.

8. По способу доступа к ресурсам АС:

- *угрозы, осуществляемые с использованием стандартного пути доступа к ресурсам АС*, например незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя;
- *угрозы, осуществляемые с использованием скрытого нестандартного пути доступа к ресурсам АС*, например несанкционированный доступ к ресурсам АС путем использования недокументированных возможностей ОС.

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

- *угрозы доступа к информации, находящейся на внешних запоминающих устройствах*, например несанкционированное копирование секретной информации с жесткого диска;
- *угрозы доступа к информации, находящейся в оперативной памяти*, например чтение остаточной информации из оперативной памяти, доступ к системной области оперативной памяти со стороны прикладных программ;
- *угрозы доступа к информации, циркулирующей в линиях связи*, например незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений, незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений;
- *угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере*, например запись отображаемой информации на скрытую видеокамеру.

Как уже отмечалось, опасные воздействия на АС подразделяют на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации АС показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни и функционирования АС.

Причинами **случайных воздействий** при эксплуатации АС могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Ошибки в ПО являются распространенным видом компьютерных нарушений. ПО серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, поэтому оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляют никакой опасности, некоторые же могут привести к серьезным последствиям, таким как получение злоумышленником контроля над сервером, неработо-

способность сервера, несанкционированное использование ресурсов (использование компьютера в качестве плацдарма для атаки и т. п.). Обычно подобные ошибки устраняются с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких пакетов является необходимым условием безопасности информации.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. В качестве нарушителя может быть служащий, посетитель, конкурент, наемник и т. д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т. п.

Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить гипотетическую модель потенциального нарушителя [40]:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

В частности, для банковских АС можно выделить следующие преднамеренные угрозы:

- НСД лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
- ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;
- несанкционированное копирование программ и данных;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных банковских документов;
- умышленное уничтожение информации;
- несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
- фальсификация сообщений, передаваемых по каналам связи;
- отказ от авторства сообщения, переданного по каналам связи;

- отказ от факта получения информации;
- навязывание ранее переданного сообщения;
- разрушение информации, вызванное вирусными воздействиями;
- разрушение архивной банковской информации, хранящейся на магнитных носителях;
- кража оборудования.

Несанкционированный доступ — наиболее распространенный и многообразный вид компьютерных нарушений. Суть НСД состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами АС, так и специально созданными аппаратными и программными средствами.

Основные каналы НСД, через которые нарушитель может получить доступ к компонентам АС и осуществить хищение, модификацию и/или разрушение информации:

- штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;
- технологические пульты управления;
- линии связи между аппаратными средствами АС;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

Из всего разнообразия способов и приемов НСД остановимся на следующих распространенных и связанных между собой нарушениях:

- перехват паролей;
- «маскарад»;
- незаконное использование привилегий.

Перехват паролей осуществляется специально разработанными программами. При попытке законного пользователя войти в систему программа-перехватчик имитирует на экране дисплея ввод имени и пароля пользователя, которые сразу пересылаются владельцу программы-перехватчика, после чего на экран выводится сообщение об ошибке и управление возвращается ОС.

Пользователь предполагает, что допустил ошибку при вводе пароля. Он повторяет ввод и получает доступ в систему. Владелец программы-перехватчика, получивший имя и пароль законного пользователя, может теперь использовать их в своих целях. Существуют и другие способы перехвата паролей.

«Маскарад» — это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями. Целью «маскарада» является приписывание каких-либо действий другому пользователю либо присвоение полномочий и привилегий другого пользователя. Примерами реализации «маскарада» являются:

- вход в систему под именем и паролем другого пользователя (этому «маскараду» предшествует перехват пароля);
- передача сообщений в сети от имени другого пользователя.

«Маскарад» особенно опасен в банковских системах электронных платежей, где неправильная идентификация клиента из-за «маскарада» злоумышленника может привести к большим убыткам законного клиента банка.

Незаконное использование привилегий. Большинство систем защиты устанавливают определенные наборы привилегий для выполнения заданных функций. Каждый пользователь получает свой набор привилегий: обычные пользователи — минимальный, администраторы — максимальный. Несанкционированный захват привилегий, например посредством «маскарада», приводит к возможности выполнения нарушителем определенных действий в обход системы защиты. Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

Принято считать, что вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие важные свойства информации и систем ее обработки: *конфиденциальность, целостность и доступность.*

Иными словами, в соответствии с существующими подходами считают, что информационная безопасность АС обеспечена в случае, если для информационных ресурсов в системе поддерживаются определенные уровни:

- конфиденциальности (невозможности несанкционированного получения какой-либо информации);

- целостности (невозможности несанкционированной или случайной ее модификации);
- доступности (возможности за разумное время получить требуемую информацию).

Соответственно для АС рассматривают три основных вида угроз.

Угрозы нарушения конфиденциальности, направленные на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен НСД к некоторой закрытой информации, хранящейся в компьютерной системе или передаваемой от одной системы к другой.

Угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, которые направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена умышленно, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации — компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется полномочными лицами с обоснованной целью (таким изменением, например, является периодическая коррекция некоторой БД).

Угрозы нарушения работоспособности (*отказ в обслуживании*), направленные на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АС, либо блокируют доступ к некоторым ее ресурсам. Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным.

Эти виды угроз можно считать первичными или непосредственными, поскольку реализация этих угроз ведет к непосредственному воздействию на защищаемую информацию.

Для современных ИТ подсистемы защиты являются неотъемлемой частью АС обработки информации. Атакующая сторона

должна преодолеть эту подсистему защиты, чтобы нарушить, например, конфиденциальность АС. Однако нужно сознавать, что не существует абсолютно стойкой системы защиты, вопрос лишь во времени и средствах, требующихся на ее преодоление. Исходя из данных условий, рассмотрим следующую модель: защита информационной системы считается преодоленной, если в ходе исследования этой системы определены все ее уязвимости.

Преодоление защиты также представляет собой угрозу, поэтому для защищенных систем можно рассматривать четвертый вид угрозы — *угрозу раскрытия параметров АС*, включающей в себя подсистему защиты. На практике любое проводимое мероприятие предваряется этапом разведки, в ходе которого определяются основные параметры системы, ее характеристики и т. п. Результатом этого этапа является уточнение поставленной задачи, а также выбор наиболее оптимального технического средства.

Угрозу раскрытия параметров АС можно считать опосредованной угрозой. Последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность реализовать первичные или непосредственные угрозы, перечисленные выше.

При рассмотрении вопросов защиты АС целесообразно использовать четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой АС информации. Такая градация доступа поможет систематизировать как возможные угрозы, так и меры по их нейтрализации и парированию, т. е. поможет систематизировать весь спектр методов обеспечения защиты, относящихся к информационной безопасности. Это следующие уровни доступа:

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

Введение этих уровней обусловлено следующими соображениями.

Во-первых, информация для удобства манипулирования чаще всего фиксируется на некотором материальном носителе, которым может быть дискета или что-нибудь подобное.

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. Например, для чте-

Таблица 1.1. **Основные методы реализации угроз информационной безопасности**

Уровень доступа к информации в АС	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза отказа служб (отказа доступа к информации)
Уровень носителей информации	Определение типа и параметров носителей информации	Хищение (копирование) носителей информации Перехват ПЭМИН	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Уровень средств взаимодействия с носителем	Получение информации о программно-аппаратной среде Получение детальной информации о функциях, выполняемых АС Получение данных о применяемых системах защиты	Несанкционированный доступ к ресурсам АС Совершение пользователем несанкционированных действий Несанкционированное копирование программного обеспечения Перехват данных, передаваемых по каналам связи	Внесение пользователем несанкционированных изменений в программы и данные Установка и использование нештатного программного обеспечения Заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонент АС Обход механизмов защиты АС
Уровень представления информации	Определение способа представления информации	Визуальное наблюдение Раскрытие представления информации (дешифрование)	Внесение искажения в представление данных; уничтожение данных	Искажение соответствия синтаксических и семантических конструкций *языка*
Уровень содержания информации	Определение содержания данных на качественном уровне	Раскрытие содержания информации	Внедрение дезинформации	Запрет на использование информации

ния информации с дискеты необходим компьютер, оборудованный дисководом соответствующего типа.

В-третьих, как уже было отмечено, информация может быть охарактеризована способом своего представления: языком символов, языком жестов и т. п.

В-четвертых, человеку должен быть доступен смысл представленной информации, ее семантика.

К основным направлениям реализации злоумышленником информационных угроз относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
- внедрение в технические средства АС программных или технических механизмов, нарушающих предполагаемую структуру и функции АС.

В табл. 1.1 перечислены основные методы реализации угроз информационной безопасности.

Для достижения требуемого уровня информационной безопасности АС необходимо обеспечить противодействие различным техническим угрозам и минимизировать возможное влияние «человеческого фактора».

Угрозы и уязвимости компьютерных сетей подробно рассматриваются в гл. 2.

Глава 2
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ

Основным свойством, отличающим компьютерные сети от автономных компьютеров, является наличие обмена информацией между сетевыми узлами, связанными линиями передачи данных.

Объединение компьютеров в компьютерные сети позволяет значительно повысить эффективность использования компьютерной системы в целом. Повышение эффективности при этом достигается за счет возможности обмена информацией между компьютерами сети, а также за счет возможности использования на каждом компьютере общих сетевых ресурсов (информации, внешней памяти, программных приложений, внешних устройств).

Одним из основных признаков корпоративной сети является применение глобальных связей для объединения отдельных локальных сетей филиалов предприятия и компьютеров его удаленных сотрудников с центральной локальной сетью. В последние годы интенсивно развиваются беспроводные компьютерные сети, и в частности беспроводные локальные сети WLAN (Wireless Local Area Network).

2.1. Введение в сетевой информационный обмен

Стремительное развитие ИТ привело к появлению и быстрому росту глобальной сети Internet. Развитие компьютерных сетей немыслимо без строгого соблюдения принципов стандартизации аппаратного и ПО. Днем рождения Интернета в современном понимании этого слова стала дата стандартизации в 1983 г. стека

коммуникационных протоколов TCP/IP, лежащего в основе Всемирной сети Интернет. Интернет представляет собой совокупность соединенных между собой компьютерных сетей, в которых используются единые согласованные правила обмена данными между компьютерами.

2.1.1. Использование сети Интернет

Развитие глобальной сети Internet способствовало использованию для построения глобальных корпоративных связей более дешевого и более доступного (по сравнению с выделенными каналами) транспорта Internet. Сеть Internet предлагает разнообразные методы коммуникации и способы доступа к информации, поэтому для многих компаний она стала неотъемлемой частью их ИС.

Влияние Internet на корпоративные сети способствовало появлению нового понятия — intranet (интранет, интрасети), при котором способы доставки и обработки информации, присущие Internet, переносятся в корпоративную сеть.

Отметим основные возможности, предоставляемые сетью Internet для построения корпоративных сетей [5, 9].

Дешевые и доступные коммуникационные каналы Internet. К началу XXI в. в связи с бурным развитием Internet и сетей коллективного доступа в мире произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные коммуникационные каналы Internet. Стремясь к экономии средств, предприятия стали активно использовать эти каналы для передачи критичной коммерческой и управленческой информации.

Универсальность. Глобальная сеть Internet была создана для обеспечения обмена информацией между удаленными пользователями. Развитие Internet-технологий привело к возникновению популярной глобальной службы World Wide Web (WWW), что позволило пользователям работать с информацией в режиме прямого подключения. Эта технология подразумевает подключение пользователя к глобальной сети и использования WWW-браузеров для просмотра информации. Стандартизация интерфейсов обмена данными между утилитами просмотра информации и информационными серверами позволила организовать одинаковый интерфейс с пользователем для различных платформ.

Доступ к разнообразной информации и услугам в Internet. Кроме транспортных услуг по транзитной передаче данных для абонентов любых типов, сеть Интернет обеспечивает также достаточно широкий набор высокоуровневых Интернет-сервисов: всемирная паутина World Wide Web; сервис имен доменов DNS; доступ к файловым архивам FTP; электронная почта (e-mail); телеконференции (Usenet); сервисы общения ICQ, IRC; сервис Telnet; поиск информации в Интернете. Компьютеры, предоставляющие эти услуги, называются *серверами,* соответственно компьютеры, пользующиеся услугами, называются *клиентами.* Эти же термины относятся и к ПО, используемому на компьютерах-серверах и компьютерах-клиентах. Сеть Internet обеспечивает доступ к обширной и разнообразной информации с помощью огромного числа подключенных к ней хост-узлов. *Хост* — это компьютер или группа компьютеров, имеющих прямое сетевое соединение с Internet и предоставляющих пользователям доступ к своим средствам и службам. Многие из этих компьютеров выполняют роль серверов, предлагающих любому пользователю, имеющему выход в Internet, доступ к электронным ресурсам — данным, приложениям и услугам. Связав свои сети с внешними ресурсами, компании могут реализовать постоянные коммуникации и организовать эффективный поток информации между людьми. Соединение внутренних сетей с внешними организациями и ресурсами позволяет компаниям воспользоваться преимуществами этих сетей — снижением затрат и повышением эффективности.

Простота использования. При использовании Интернет-технологий не требуется специального обучения персонала.

Для объединения локальных сетей в глобальные используются специализированные компьютеры (маршрутизаторы и шлюзы), с помощью которых локальные сети подключаются к межсетевым каналам связи. Маршрутизаторы и шлюзы физически соединяют локальные сети друг с другом и, используя специальное ПО, передают данные из одной сети в другую. Глобальные сети имеют сложную разветвленную структуру и избыточные связи. Маршрутизаторы и шлюзы обеспечивают поиск оптимального маршрута при передаче данных в глобальных сетях, благодаря чему достигается максимальная скорость потока сообщений. Высокоскоростные каналы связи между локальными сетями могут быть реализованы на основе волоконно-оптических кабелей или с помощью спутниковой связи. В качестве медлен-

ных межсетевых каналов связи используются различные виды телефонных линий.

Построение корпоративных компьютерных сетей с применением технологии интрасетей означает прежде всего использование стека TCP/IP для транспортировки данных и технологии Web для их представления.

2.1.2. Модель ISO/OSI и стек протоколов TCP/IP

Основная задача, решаемая при создании компьютерных сетей, — обеспечение совместимости оборудования по электрическим и механическим характеристикам и совместимости информационного обеспечения (программ и данных) по системам кодирования и формату данных. Решение этой задачи относится к области стандартизации. Методологической основой стандартизации в компьютерных сетях является многоуровневый подход к разработке средств сетевого взаимодействия. На основе этого подхода и технических предложений Международной организации стандартов ISO (International Standards Organization) в начале 1980-х гг. была разработана *стандартная модель взаимодействия открытых систем OSI* (Open Systems Interconnection). Модель ISO/OSI сыграла важную роль в развитии компьютерных сетей.

Модель OSI определяет различные уровни взаимодействия систем и указывает, какие функции должен выполнять каждый уровень. В модели OSI средства взаимодействия делятся на семь уровней: прикладной (Application), представительный (Presentation), сеансовый (Session), транспортный (Transport), сетевой (Network), канальный (Data Link) и физический (Physical). Самый верхний уровень — прикладной. На этом уровне пользователь взаимодействует с приложениями. Самый нижний уровень — физический. Этот уровень обеспечивает обмен сигналами между устройствами.

Обмен данными через каналы связи происходит путем перемещения данных с верхнего уровня на нижний, затем транспортировки по линиям связи и, наконец, обратным воспроизведением данных в компьютере клиента в результате их перемещения с нижнего уровня на верхний.

Для обеспечения необходимой совместимости на каждом из уровней архитектуры компьютерной сети действуют *специальные стандартные протоколы.* Они представляют собой формализо-

ванные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах сети.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется *стеком коммуникационных протоколов.* Следует четко различать модель ISO/OSI и стек протоколов ISO/OSI. *Модель ISO/OSI* является концептуальной схемой взаимодействия открытых систем, а *стек протоколов ISO/OSI* представляет собой набор вполне конкретных спецификаций протоколов для семи уровней взаимодействия, которые определены в модели ISO/OSI.

Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней — как правило, чисто программными средствами.

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле сети, должны взаимодействовать друг с другом также в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть *межуровневым интерфейсом.* Межуровневый интерфейс определяет набор сервисов, предоставляемых данным уровнем соседнему уровню. В сущности, протокол и интерфейс являются близкими понятиями, но традиционно в сетях за ними закреплены разные области действия: *протоколы* определяют правила взаимодействия модулей одного уровня в разных узлах сети, а *интерфейсы* определяют правила взаимодействия модулей соседних уровней в одном узле.

Стек протоколов TCP/IP (Transmission Control Protocol/ Internet Protocol) является промышленным стандартом стека коммуникационных протоколов, разработанным для глобальных сетей. Стандарты TCP/IP опубликованы в серии документов, названных Request for Comment (RFC). Документы RFC описывают внутреннюю работу сети Internet. Некоторые RFC описывают сетевые сервисы или протоколы и их реализацию, в то время как другие обобщают условия применения.

Стек TCP/IP объединяет набор взаимодействующих между собой протоколов. Самыми важными из них являются протокол IP, отвечающий за поиск маршрута (или маршрутов) в Интернете от одного компьютера к другому через множество промежуточных сетей, шлюзов и маршрутизаторов и передачу блоков данных

по этим маршрутам, и протокол TCP, обеспечивающий надежную доставку, безошибочность и правильный порядок приема передаваемых данных.

Большой вклад в развитие стека TCP/IP внес Калифорнийский университет в Беркли (США), который реализовал протоколы стека в своей версии ОС UNIX, сделав как сами программы, так и их исходные тексты бесплатными и общедоступными. Популярность этой ОС привела к широкому распространению протоколов IP, TCP и других протоколов стека. Сегодня этот стек используется для связи компьютеров всемирной информационной сети Internet, а также в огромном числе корпоративных сетей. Стек TCP/IP является самым распространенным средством организации составных компьютерных сетей.

Широкое распространение стека TCP/IP объясняется следующим:

- это наиболее завершенный стандартный и в то же время популярный стек сетевых протоколов, имеющий многолетнюю историю;
- почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP;
- все современные ОС поддерживают стек TCP/IP.

Кроме того, это:

- метод получения доступа к сети Internet;
- гибкая технология для соединения разнородных систем как на уровне транспортных подсистем, так и на уровне прикладных сервисов;
- основа для создания intranet — корпоративной сети, использующей транспортные услуги Internet и гипертекстовую технологию WWW, разработанную в Internet;
- устойчивая масштабируемая межплатформенная среда для приложений клиент—сервер [46].

Структура и функциональность стека протоколов TCP/IP

Стек TCP/IP был разработан до появления модели взаимодействия открытых систем OSI и также имеет многоуровневую структуру. Структура протоколов TCP/IP приведена на рис. 2.1. Стек протоколов TCP/IP имеет четыре уровня — прикладной (Application), транспортный (Transport), уровень межсетевого взаимодействия (Internet) и уровень сетевых интерфейсов

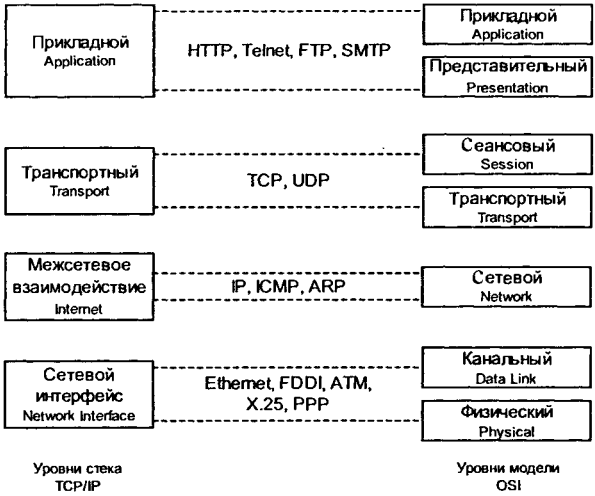


Рис. 2.1. Уровни стека протоколов TCP/IP

(Network). Для сравнения на рис. 2.1 показаны также семь уровней модели OSI. Следует отметить, что соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

Прикладной уровень (Application) включает большое число прикладных протоколов и сервисов. К ним относятся такие популярные протоколы, как протокол копирования файлов FTP, протокол эмуляции терминала Telnet, почтовый протокол SMPT, используемый в электронной почте сети Internet, гипертекстовые сервисы доступа к удаленной информации, такие как WWW, и многие другие. Рассмотрим подробнее некоторые из этих протоколов [46].

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Для того чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений — TCP. Кроме пересылки файлов, протокол FTP предлагает и другие услуги. Например, пользователю предоставляется возможность интерактивной работы с удаленной машиной, в частности, он может распечатать содержимое ее каталогов. Наконец, FTP выполняет аутентификацию пользователей. Прежде чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Для доступа к публичным каталогам FTP-архивов

Internet не требуется парольная аутентификация, и ее можно обойти путем использования для такого доступа предопределенного имени пользователя Anonymous.

Протокол Telnet обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленного компьютера. При использовании сервиса Telnet пользователь фактически управляет удаленным компьютером так же, как и локальный пользователь, поэтому такой вид доступа требует хорошей защиты. Серверы Telnet всегда используют, как минимум, аутентификацию по паролю, а иногда и более мощные средства защиты, например систему Kerberos.

Протокол SNMP (Simple Network Management Protocol) используется для организации сетевого управления. Сначала протокол SNMP был разработан для удаленного контроля и управления маршрутизаторами Internet. С ростом популярности протокол SNMP стали применять для управления разным коммуникационным оборудованием — концентраторами, мостами, сетевыми адаптерами и др. В стандарте SNMP определена спецификация информационной базы данных управления сетью. Эта спецификация, известная как база данных MIB (Management Information Base), определяет те элементы данных, которые управляемое устройство должно сохранять, и допустимые операции над ними.

На **транспортном уровне (Transport)** стека TCP/IP, называемом также основным уровнем, функционируют протокол TCP и протокол UDP.

Протокол управления передачей TCP (Transport Control Protocol) решает задачу обеспечения надежной информационной связи между двумя конечными узлами. Этот протокол называют протоколом «с установлением соединения». Это означает, что два узла, связывающиеся при помощи этого протокола, «договариваются» о том, что они будут обмениваться потоком данных и принимают некоторые соглашения об управлении этим потоком. Согласно протоколу TCP, отправляемые данные «нарезаются» на небольшие стандартные пакеты, после чего каждый пакет маркируется таким образом, чтобы в нем были данные для правильной сборки документа на компьютере получателя.

Протокол дейтаграмм пользователя UDP (User Datagram Protocol) обеспечивает передачу прикладных пакетов дейтаграммным способом, т. е. каждый блок передаваемой информации (пакет) обрабатывается и распространяется от узла к узлу

как независимая единица информации — дейтаграмма. При этом протокол UDP выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами. Необходимость в протоколе UDP обусловлена тем, что UDP «умеет» различать приложения и доставляет информацию от приложения к приложению.

Уровень межсетевого взаимодействия (Internet) реализует концепцию коммутации пакетов без установления соединений. Основным протоколом этого уровня является *адресный протокол IP.* Этот протокол изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого числа локальных сетей, объединенных как локальными, так и глобальными связями.

Суть протокола IP состоит в том, что у каждого пользователя Всемирной сети Internet должен быть свой уникальный адрес (IP-адрес). Без этого нельзя говорить о точной доставке TCP-пакетов в нужное рабочее место. Этот адрес выражается очень просто — четырьмя байтами, например: 185.47.39.14. Структура IP-адреса организована таким образом, что каждый компьютер, через который проходит какой-либо TCP-пакет, может по этим четырем числам определить, кому из ближайших «соседей» надо переслать пакет, чтобы он оказался «ближе» к получателю. В результате конечного числа переброс TCP-пакет достигает адресата. В данном случае оценивается не географическая «близость». В расчет принимаются условия связи и пропускная способность линии. Два компьютера, находящиеся на разных континентах, но связанные высокопроизводительной линией космической связи, считаются более близкими друг другу, чем два компьютера из соседних городов, связанных обычной телефонной связью. Решением вопросов, что считать «ближе», а что «дальше» занимаются специальные средства — маршрутизаторы. Роль маршрутизатора в сети может выполнять как специализированный компьютер, так и специализированная программа, работающая на узловом сервере сети.

К уровню межсетевого взаимодействия относятся и протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как *протоколы сбора маршрутной информации RIP* (Routing Internet Protocol) и *OSPF* (Open Shortest Path First), а также *протокол межсетевых управляющих сообщений ICMP* (Internet Control Message Protocol). Последний протокол предназначен

для обмена информацией об ошибках между маршрутизаторами сети и узлом — источником пакета.

Уровень сетевого интерфейса (Network) соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, для глобальных сетей — протоколы соединений «точка—точка» SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, frame relay. Разработана спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня.

Разделенные на уровни протоколы стека TCP/IP спроектированы таким образом, что конкретный уровень хоста назначения получает именно тот объект, который был отправлен эквивалентным уровнем хоста источника. Каждый уровень стека одного хоста образует логическое соединение с одноименным уровнем стека другого хоста. При реализации физического соединения уровень передает свои данные интерфейсу уровня, расположенного выше или ниже в том же хосте (рис. 2.2). Вертикальные стрелки показывают физическое соединение в рамках одного хоста, а горизонтальные стрелки показывают логическое соединение между одноименными уровнями в различных хостах.

Следует обратить внимание на терминологию, традиционно используемую для обозначения информационных объектов, распространяющихся на интерфейсах между различными уровнями управления стека протоколов TCP/IP.

Приложение передает транспортному уровню сообщение (message), которое имеет соответствующее данному приложению размер и семантику. Транспортный уровень «разрезает» это сообщение (если оно достаточно велико) на пакеты (packets), которые передаются уровню межсетевого взаимодействия (т. е. протоколу IP). Протокол IP формирует свои IP-пакеты (еще говорят — IP-дейтаграммы) и затем упаковывает их в формат, приемлемый для данной физической среды передачи информации. Эти, уже аппаратно-зависимые, пакеты обычно называют кадрами (frame).

Когда данные передаются от прикладного уровня к транспортному уровню, затем уровню межсетевого взаимодействия и далее через уровень сетевого интерфейса в сеть, каждый протокол выполняет соответствующую обработку и инкапсулирует

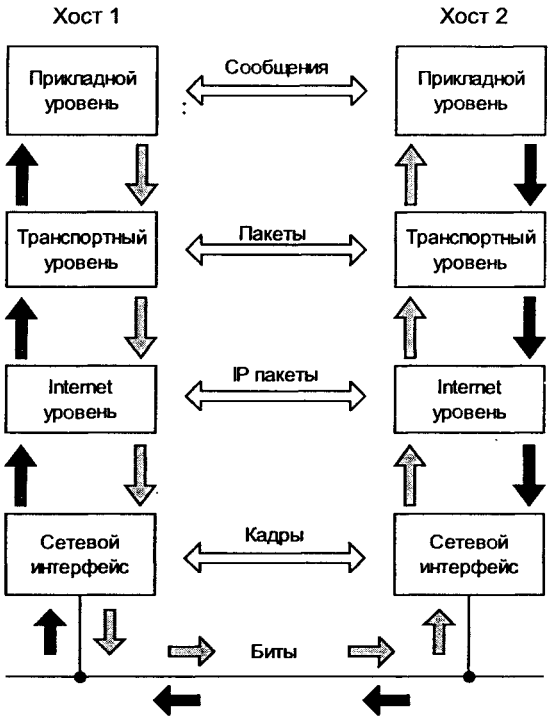


Рис. 2.2. Логические и физические соединения между уровнями стека TCP/IP

результат этой обработки, присоединяя спереди свой заголовок (рис. 2.3).

В системе, принимающей данный поток информации, эти заголовки последовательно удаляются по мере обработки данных и передачи их вверх по стеку. Такой подход обеспечивает необходимую гибкость в обработке передаваемых данных, поскольку верхним уровням вовсе не нужно касаться технологии, используемой в нижних уровнях. Например, если шифруются данные на уровне IP, уровень TCP и прикладной уровень остаются неизменными.

Что касается безопасности протоколов TCP/IP, т. е. безопасности передачи данных в Интернете в целом, пользователям необходимо иметь в виду, что если не приняты специальные меры, то все данные передаются протоколами TCP/IP в открытом виде. Это значит, что любой узел (и соответственно его оператор), находящийся на пути следования данных от отправителя к

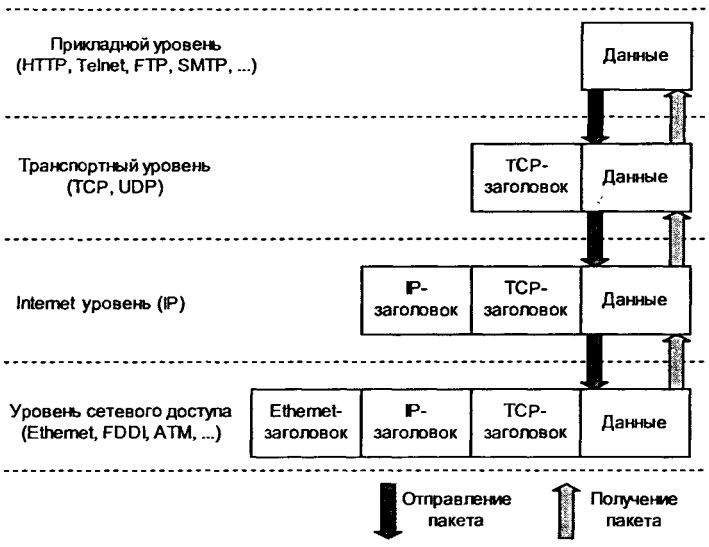


Рис. 2.3. Схема инкапсуляции данных в стеке протоколов TCP/IP

получателю, может скопировать себе все передаваемые данные и использовать их в дальнейшем в своих целях. В равной мере данные могут быть искажены или уничтожены.

2.2. Анализ угроз сетевой безопасности

Для организации коммуникаций в неоднородной сетевой среде применяется набор протоколов TCP/IP, обеспечивая совместимость между компьютерами разных типов. Совместимость — одно из основных преимуществ TCP/IP, поэтому большинство компьютерных сетей поддерживает эти протоколы. Кроме того, протоколы TCP/IP предоставляют доступ к ресурсам глобальной сети Интернет.

Благодаря своей популярности TCP/IP стал стандартом де-факто для межсетевого взаимодействия. Однако повсеместное распространение стека протоколов TCP/IP обнажило и его слабые стороны. Создавая свое детище, архитекторы стека TCP/IP не видели причин для беспокойства о защите сетей, строящихся на его основе. Поэтому в спецификациях ранних версий протокола IP отсутствовали требования безопасности, что привело к изначальной уязвимости реализации этого протокола.

2.2.1. Проблемы безопасности IP-сетей

Рост популярности Интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. д. Хакеры и другие злоумышленники подвергают угрозам сетевые информационные ресурсы, пытаясь получить к ним доступ с помощью специальных атак. Эти атаки становятся все более изощренными по воздействию и несложными в исполнении. Этому способствуют два основных фактора.

Во-первых, это повсеместное проникновение Интернета. К этой сети подключены миллионы компьютеров. В ближайшем будущем их число во много раз возрастет, поэтому вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям также постоянно возрастает. Кроме того, широкое распространение Интернета позволяет хакерам обмениваться информацией в глобальном масштабе.

Во-вторых, это всеобщее распространение простых в использовании ОС и сред разработки. Этот фактор резко снижает требования к уровню знаний злоумышленника. Раньше от хакера требовались хорошие знания и навыки программирования, чтобы создавать и распространять вредоносные программы. Теперь, для того чтобы получить доступ к хакерскому средству, нужно просто знать IP-адрес нужного сайта, а для проведения атаки достаточно щелкнуть мышкой.

Проблемы обеспечения информационной безопасности в корпоративных компьютерных сетях обусловлены угрозами безопасности для локальных рабочих станций, локальных сетей и атаками на корпоративные сети, имеющими выход в общедоступные сети передачи данных.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Одни атаки отличаются большой сложностью, другие может осуществить обычный оператор, даже не предполагающий, какие последствия будет иметь его деятельность.

Цели нарушителя, осуществляющего атаку:

- нарушение конфиденциальности передаваемой информации;
- нарушение целостности и достоверности передаваемой информации;

- нарушение работоспособности всей системы или отдельных ее частей.

Распределенные системы подвержены прежде всего *удаленным атакам*, поскольку компоненты распределенных систем обычно используют открытые каналы передачи данных, и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик (активное воздействие). И если активное воздействие на трафик может быть зафиксировано, то пассивное воздействие практически не поддается обнаружению. Но поскольку в ходе функционирования распределенных систем обмен служебной информацией между компонентами системы осуществляется тоже по открытым каналам передачи данных, то служебная информация становится таким же объектом атаки, как и данные пользователя.

Трудность выявления факта проведения удаленной атаки выводит этот вид неправомерных действий на первое место по степени опасности и препятствует своевременному реагированию на осуществленную угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

Безопасность локальной сети отличается от безопасности межсетевого взаимодействия тем, что на первое по значимости место выходят *нарушения зарегистрированных пользователей*, поскольку в этом случае каналы передачи данных локальной сети находятся на контролируемой территории и защита от несанкционированного подключения к которым реализуется административными методами.

На практике IP-сети уязвимы для многих способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий (например с появлением мобильных Java-приложений и элементов ActiveX) список возможных типов сетевых атак на IP-сети постоянно расширяется [9].

Наиболее распространены следующие атаки.

Подслушивание (sniffing). В основном данные по компьютерным сетям передаются в незащищенном формате (открытым текстом), что позволяет злоумышленнику, получившему доступ к линиям передачи данных в сети подслушивать или считывать трафик. Для подслушивания в компьютерных сетях используют сниффер. *Сниффер пакетов* представляет собой прикладную про-

грамму, которая перехватывает все сетевые пакеты, передаваемые через определенный домен.

В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т. д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват пароля, передаваемого по сети в незашифрованной форме, путем «подслушивания» канала является разновидностью атаки подслушивания, которую называют *password sniffing*. Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.

Предотвратить угрозу сниффинга пакетов можно с помощью применения для аутентификации однократных паролей, установки аппаратных или программных средств, распознающих снифферы, применения криптографической защиты каналов связи.

Изменение данных. Злоумышленник, получивший возможность прочитать ваши данные, сможет сделать и следующий шаг — изменить их. Данные в пакете могут быть изменены, даже если злоумышленник ничего не знает ни об отправителе, ни о получателе. Даже если вы не нуждаетесь в строгой конфиденциальности всех передаваемых данных, то наверняка не захотите, чтобы они были изменены по пути.

Анализ сетевого трафика. Целью атак подобного типа является прослушивание каналов связи и анализ передаваемых данных и служебной информации для изучения топологии и архитектуры построения системы, получения критической пользовательской информации (например, паролей пользователей или номеров кредитных карт, передаваемых в открытом виде). Атакам этого типа подвержены такие протоколы, как FTP или Telnet, особенностью которых является то, что имя и пароль пользователя передаются в рамках этих протоколов в открытом виде.

Подмена доверенного субъекта. Большая часть сетей и ОС используют IP-адрес компьютера, для того чтобы определять, тот ли это адресат, который нужен. В некоторых случаях возможно некорректное присвоение IP-адреса (подмена IP-адреса отправителя другим адресом). Такой способ атаки называют *фальсификацией адреса* (*IP-spoofing*).

IP-спуфинг имеет место, когда злоумышленник, находящийся внутри корпорации или вне ее, выдает себя за законного пользователя. Он может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Злоумышленник может также использовать специальные программы, формирующие IP-пакеты таким образом, чтобы они выглядели как исходящие с разрешенных внутренних адресов корпоративной сети.

Атаки IP-спуфинга часто становятся отправной точкой для других атак. Классическим примером является атака типа «отказ в обслуживании» (DoS), которая начинается с чужого адреса, скрывающего истинную личность хакера.

Угрозу спуфинга можно ослабить (но не устранить) с помощью правильной настройки управления доступом из внешней сети, пресечения попыток спуфинга чужих сетей пользователями своей сети.

Следует иметь в виду, что IP-спуфинг может быть осуществлен при условии, что аутентификация пользователей производится на базе IP-адресов, поэтому атаки IP-спуфинга можно предотвратить путем введения дополнительных методов аутентификации пользователей (на основе одноразовых паролей или других методов криптографии).

Посредничество. Эта атака подразумевает активное подслушивание, перехват и управление передаваемыми данными невидимым промежуточным узлом. Когда компьютеры взаимодействуют на низких сетевых уровнях, они не всегда могут определить, с кем именно они обмениваются данными.

Посредничество в обмене незашифрованными ключами (атака man-in-the-middle). Для проведения атаки man-in-the-middle (человек-в-середине) злоумышленнику нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера ISP в любую другую сеть, может, например, получить сотрудник этого провайдера. Для атак этого типа часто

используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации.

Атаки man-in-the-middle проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа man-in-the-middle можно только с помощью криптографии. Для противодействия атакам этого типа используется *инфраструктура управления открытыми ключами — PKI* (Public Key Infrastructure).

Перехват сеанса (session hijacking). По окончании начальной процедуры аутентификации соединение, установленное законным пользователем, например с почтовым сервером, переключается злоумышленником на новый хост, а исходному серверу выдается команда разорвать соединение. В результате «собеседник» законного пользователя оказывается незаметно подмененным.

После получения доступа к сети атакующий злоумышленник может:

- посылать некорректные данные приложениям и сетевым службам, что приводит к их аварийному завершению или неправильному функционированию;
- наводнить компьютер или всю сеть трафиком, пока не произойдет останов системы в результате перегрузки;
- блокировать трафик, что приведет к потере доступа авторизованных пользователей к сетевым ресурсам.

Отказ в обслуживании (Denial of Service, DoS). Эта атака отличается от атак других типов: она не нацелена на получение доступа к сети или на получение из этой сети какой-либо информации. Атака DoS делает сеть организации недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, ОС или приложения. По существу, она лишает обычных пользователей доступа к ресурсам или компьютерам сети организации.

Большинство атак DoS опирается на общие слабости системной архитектуры. В случае использования некоторых серверных приложений (таких как web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак

DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol).

Атаки DoS трудно предотвратить, так как для этого требуется координация действий с провайдером. Если трафик, предназначенный для переполнения сети, не остановить у провайдера, то на входе в сеть это сделать уже нельзя, потому что вся полоса пропускания будет занята.

Если атака этого типа проводится одновременно через множество устройств, то говорят о распределенной атаке отказа в обслуживании DDoS (distributed DoS). Простота реализации атак DoS и огромный вред, причиняемый ими организациям и пользователям, привлекают к ним пристальное внимание администраторов сетевой безопасности.

Парольные атаки. Их цель — завладение паролем и логином законного пользователя. Злоумышленники могут проводить парольные атаки, используя такие методы, как:

- подмена IP-адреса (IP-спуфинг);
- подслушивание (сниффинг);
- простой перебор.

IP-спуфинг и сниффинг пакетов были рассмотрены выше. Эти методы позволяют завладеть паролем и логином пользователя, если они передаются открытым текстом по незащищенному каналу.

Часто хакеры пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой метод носит название *атака полного перебора* (brute force attack). Для этой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу). Если в результате злоумышленнику удается подобрать пароль, он получает доступ к ресурсам на правах обычного пользователя.

Парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Использование одноразовых паролей и криптографической аутентификации может практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают указанные методы аутентификации.

При использовании обычных паролей необходимо придумать такой пароль, который было бы трудно подобрать. Минимальная длина пароля должна быть не менее 8 символов. Пароль должен включать символы верхнего регистра, цифры и специальные символы (#, $, &, % и т. д.).

Угадывание ключа. Криптографический ключ представляет собой код или число, необходимое для расшифровки защищенной информации. Хотя узнать ключ доступа не просто и требует больших затрат ресурсов, тем не менее это возможно. В частности, для определения значения ключа может быть использована специальная программа, реализующая метод полного перебора. Ключ, к которому получает доступ атакующий, называется *скомпрометированным*. Атакующий использует скомпрометированный ключ для получения доступа к защищенным передаваемым данным без ведома отправителя и получателя. Ключ дает возможность расшифровывать и изменять данные.

Атаки на уровне приложений могут проводиться несколькими способами.

Самый распространенный из них состоит в использовании известных слабостей серверного ПО (FTP, HTTP, web-сервера).

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через межсетевой экран. Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам исправить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.

Невозможно полностью исключить атаки на уровне приложений. Хакеры постоянно открывают и публикуют на своих сайтах в Интернете все новые уязвимые места прикладных программ.

Здесь важно осуществлять хорошее системное администрирование. Чтобы снизить уязвимость от атак этого типа, можно предпринять следующие меры:

- анализировать log-файлы ОС и сетевые log-файлы с помощью специальных аналитических приложений;
- отслеживать данные CERT о слабых местах прикладных программ;
- пользоваться самыми свежими версиями ОС и приложений и самыми последними коррекционными модулями (патчами);
- использовать системы распознавания атак IDS (Intrusion Detection Systems).

Сетевая разведка — это сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации.

Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (ping sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. В результате добывается информация, которую можно использовать для взлома.

Системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера (ISP), в сети которого установлена система, проявляющая чрезмерное любопытство.

Злоупотребление доверием. Данный тип действий не является атакой в полном смысле этого слова. Он представляет собой злонамеренное использование отношений доверия, существующих в сети. Типичный пример такого злоупотребления — ситуация в периферийной части корпоративной сети. В этом сегменте обычно располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат одному и тому же сегменту, взлом одного из них приводит к взлому и всех остальных, так как эти серверы доверяют другим системам своей сети.

Риск злоупотребления доверием можно снизить за счет более жесткого контроля уровней доверия в пределах своей сети. Системы, расположенные с внешней стороны межсетевого экрана, никогда не должны пользоваться абсолютным доверием со стороны систем, защищенных межсетевым экраном.

Отношения доверия должны ограничиваться определенными протоколами и аутентифицироваться не только по IP-адресам, но и по другим параметрам.

Компьютерные вирусы, сетевые «черви», программа «троянский конь». Вирусы представляют собой вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя. Вирус обычно разрабатывается злоумышленниками таким образом, чтобы как можно дольше оставаться необнаруженным в компьютерной системе. Начальный период «дремоты» вирусов является механизмом их выживания. Вирус проявляется в полной мере в конкретный момент времени, когда

происходит некоторое событие вызова, например пятница 13-е, известная дата и т. п.

Разновидностью программы-вируса является сетевой «червь», который распространяется по глобальной сети и не оставляет своей копии на магнитном носителе. Этот термин используется для именования программ, которые подобно ленточным червям перемещаются по компьютерной сети от одной системы к другой. «Червь» использует механизмы поддержки сети для определения узла, который может быть поражен. Затем с помощью этих же механизмов передает свое тело в этот узел и либо активизируется, либо ждет подходящих условий для активизации. Сетевые «черви» являются опасным видом вредоносных программ, так как объектом их атаки может стать любой из миллионов компьютеров, подключенных к глобальной сети Internet. Для защиты от «червя» необходимо принять меры предосторожности против несанкционированного доступа к внутренней сети.

К компьютерным вирусам примыкают так называемые «троянские кони» (троянские программы). «Троянский конь» — это программа, которая имеет вид полезного приложения, а на деле выполняет вредные функции (разрушение ПО, копирование и пересылка злоумышленнику файлов с конфиденциальными данными и т. п.). Термин «троянский конь» был впервые использован хакером Даном Эдварсом, позднее ставшим сотрудником Агентства национальной безопасности США. Опасность «троянского коня» заключается в дополнительном блоке команд, вставленном в исходную безвредную программу, которая затем предоставляется пользователям АС. Этот блок команд может срабатывать при наступлении какого-либо условия (даты, состояния системы) либо по команде извне. Пользователь, запустивший такую программу, подвергает опасности как свои файлы, так и всю АС в целом. Рабочие станции конечных пользователей очень уязвимы для вирусов, сетевых «червей» и «троянских коней».

Для защиты от указанных вредоносных программ необходимо:

- исключение несанкционированного доступа к исполняемым файлам;
- тестирование приобретаемых программных средств;
- контроль целостности исполняемых файлов и системных областей;
- создание замкнутой среды исполнения программ.

Борьба с вирусами, «червями» и «троянскими конями» ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и, возможно, на уровне сети. Антивирусные средства обнаруживают большинство вирусов, «червей» и «троянских коней» и пресекают их распространение. Получение самой свежей информации о вирусах помогает эффективнее бороться с ними. По мере появления новых вирусов, «червей» и «троянских коней» нужно обновлять базы данных антивирусных средств и приложений.

Перечисленные атаки на IP-сети возможны в результате:

- использования общедоступных каналов передачи данных. Важнейшие данные, передаются по сети в незашифрованном виде;
- уязвимости в процедурах идентификации, реализованных в стеке TCP/IP. Идентифицирующая информация на уровне IP передается в открытом виде;
- отсутствия в базовой версии стека протоколов TCP/IP механизмов, обеспечивающих конфиденциальность и целостность передаваемых сообщений;
- аутентификации отправителя по его IP-адресу. Процедура аутентификации выполняется только на стадии установления соединения, а в дальнейшем подлинность принимаемых пакетов не проверяется;
- отсутствия контроля за маршрутом прохождения сообщений в сети Internet, что делает удаленные сетевые атаки практически безнаказанными,

Первые средства защиты передаваемых данных появились практически сразу после того, как уязвимость IP-сетей дала о себе знать на практике. Характерными примерами разработок в этой области могут служить: PGP/Web-of-Trust для шифрования сообщений электронной почты, Secure Sockets Layer (SSL) для защиты Web-трафика, Secure SHell (SSH) для защиты сеансов Telnet и процедур передачи файлов.

Общим недостатком подобных широко распространенных решений является их «привязанность» к определенному типу приложений, а значит, неспособность удовлетворять тем разнообразным требованиям к системам сетевой защиты, которые предъявляют крупные корпорации или Internet-провайдеры.

Самый радикальный способ преодоления указанного ограничения сводится к построению системы защиты не для отдельных классов приложений (пусть и весьма популярных), а для сети в

целом. Применительно к IP-сетям это означает, что системы защиты должны действовать *на сетевом уровне* модели OSI.

В 1993 г. в составе консорциума IETF была создана рабочая группа IP Security Working Group, занявшаяся разработкой архитектуры и протоколов для шифрования данных, передаваемых по сетям IP. В результате появился *набор протоколов IPSec*, основанных на современных технологиях шифрования и электронной цифровой подписи данных. Поскольку архитектура протоколов IPSec совместима с протоколом IPv4, ее поддержку достаточно обеспечивать на обоих концах соединения; промежуточные сетевые узлы могут вообще ничего «не знать» о применении IPSec.

Архитектура стека протоколов IPSec и его применение для построения *защищенных виртуальных каналов и сетей VPN* (Virtual Private Networks) подробно рассматриваются в гл. 12.

2.2.2. Угрозы и уязвимости проводных корпоративных сетей

На начальном этапе развития сетевых технологий ущерб от вирусных и других типов компьютерных атак был невелик, так как зависимость мировой экономики от информационных технологий была мала. В настоящее время в условиях значительной зависимости бизнеса от электронных средств доступа и обмена информацией и постоянно растущего числа атак ущерб от самых незначительных атак, приводящих к потерям машинного времени, исчисляется миллионами долларов, а совокупный годовой ущерб мировой экономике составляет десятки миллиардов долларов [9].

Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют:

- увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации;
- сосредоточение в базах данных информации различного уровня важности и конфиденциальности;
- расширение доступа круга пользователей к информации, хранящейся в базах данных, и к ресурсам вычислительной сети;
- увеличение числа удаленных рабочих мест;

- широкое использование глобальной сети Internet и различных каналов связи;
- автоматизация обмена информацией между компьютерами пользователей.

Анализ наиболее распространенных угроз, которым подвержены современные проводные корпоративные сети, показывает, что источники угроз могут изменяться от неавторизованных вторжений злоумышленников до компьютерных вирусов, при этом весьма существенной угрозой безопасности являются человеческие ошибки. Необходимо учитывать, что источники угроз безопасности могут находиться как внутри КИС — внутренние источники, так и вне ее — внешние источники. Такое деление вполне оправдано потому, что для одной и той же угрозы (например кражи) методы противодействия для внешних и внутренних источников различны. Знание возможных угроз, а также уязвимых мест КИС необходимо для выбора наиболее эффективных средств обеспечения безопасности.

Самыми частыми и опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки пользователей, операторов и системных администраторов, обслуживающих КИС. Иногда такие ошибки приводят к прямому ущербу (неправильно введенные данные, ошибка в программе, вызвавшая остановку или разрушение системы), а иногда создают слабые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования) [43].

Согласно данным Национального института стандартов и технологий США (NIST), 55 % случаев нарушения безопасности ИС — следствие непреднамеренных ошибок. Работа в глобальной ИС делает этот фактор достаточно актуальным, причем источником ущерба могут быть как действия пользователей организации, так и пользователей глобальной сети, что особенно опасно. На рис. 2.4 приведена круговая диаграмма, иллюстрирующая статистические данные по источникам нарушений безопасности в КИС.

На втором месте по размерам ущерба располагаются кражи и подлоги. В большинстве расследованных случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами. Наличие мощного информационного канала связи с глобальными сетями при отсутствии должного контроля за его работой может дополнительно способствовать такой деятельности.

Рис. 2.4. Источники нарушений безопасности

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны вредить весьма эффективно. Поэтому при увольнении сотрудника его права доступа к информационным ресурсам должны аннулироваться.

Преднамеренные попытки получения НСД через внешние коммуникации занимают около 10 % всех возможных нарушений. Хотя эта величина кажется не столь значительной, опыт работы в Internet показывает, что почти каждый Internet-сервер по нескольку раз в день подвергается попыткам проникновения. Тесты Агентства защиты информационных систем (США) показали, что 88 % компьютеров имеют слабые места с точки зрения информационной безопасности, которые могут активно использоваться для получения НСД. Отдельно следует рассматривать случаи удаленного доступа к информационным структурам организаций.

До построения политики безопасности необходимо оценить риски, которым подвергается компьютерная среда организации и предпринять соответствующие действия. Очевидно, что затраты организации на контроль и предотвращение угроз безопасности не должны превышать ожидаемых потерь.

Приведенные статистические данные могут подсказать администрации и персоналу организации, куда следует направить усилия для эффективного снижения угроз безопасности корпоративной сети и системы. Конечно, нужно заниматься проблемами физической безопасности и мерами по снижению негативного воздействия на безопасность ошибок человека, но в то же

время необходимо уделять самое серьезное внимание решению задач сетевой безопасности по предотвращению атак на корпоративную сеть и систему как извне, так и изнутри системы.

2.2.3. Угрозы и уязвимости беспроводных сетей

При построении беспроводных сетей также стоит проблема обеспечения их безопасности. Если в обычных сетях информация передается по проводам, то радиоволны, используемые для беспроводных решений, достаточно легко перехватить при наличии соответствующего оборудования. Принцип действия беспроводной сети приводит к возникновению большого числа возможных уязвимостей для атак и проникновений.

Оборудование беспроводных локальных сетей WLAN (Wireless Local Area Network) включает точки беспроводного доступа и рабочие станции для каждого абонента.

Точки доступа AP (Access Point) выполняют роль концентраторов, обеспечивающих связь между абонентами и между собой, а также функцию мостов, осуществляющих связь с кабельной локальной сетью и с Интернет. Каждая точка доступа может обслуживать несколько абонентов. Несколько близкорасположенных точек доступа образуют зону доступа *Wi-Fi*, в пределах которой все абоненты, снабженные беспроводными адаптерами, получают доступ к сети. Такие зоны доступа создаются в местах массового скопления людей: в аэропортах, студенческих городках, библиотеках, магазинах, бизнес-центрах и т. д.

У точки доступа есть идентификатор набора сервисов SSID (Service Set Identifier). SSID — это 32-битная строка, используемая в качестве имени беспроводной сети, с которой ассоциируются все узлы. Идентификатор SSID необходим для подключения рабочей станции к сети. Чтобы связать рабочую станцию с точкой доступа, обе системы должны иметь один и тот же SSID. Если рабочая станция не имеет нужного SSID, то она не сможет связаться с точкой доступа и соединиться с сетью.

Главное отличие между проводными и беспроводными сетями — наличие неконтролируемой области между конечными точками беспроводной сети. Это позволяет атакующим, находящимся в непосредственной близости от беспроводных структур, производить ряд нападений, которые невозможны в проводном мире.

При использовании беспроводного доступа к локальной сети угрозы безопасности существенно возрастают (рис. 2.5).

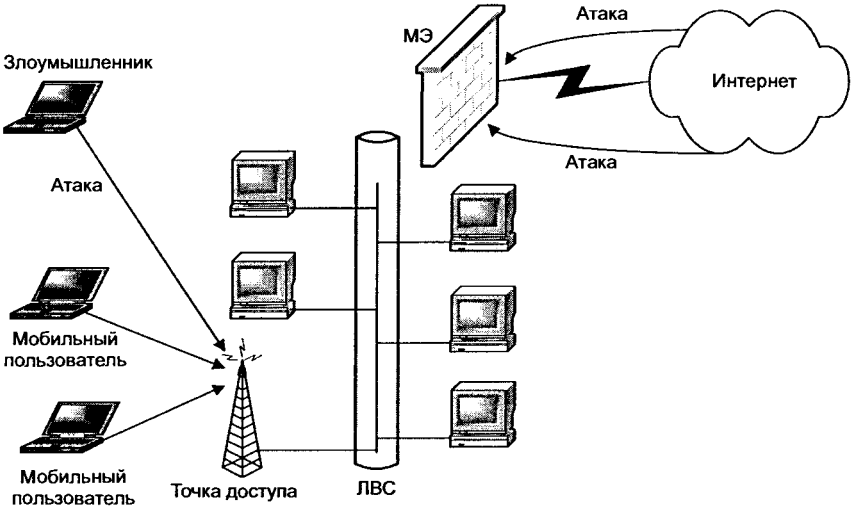


Рис. 2.5. Угрозы при беспроводном доступе к локальной сети

Перечислим основные уязвимости и угрозы беспроводных сетей.

Вещание радиомаяка. Точка доступа включает с определенной частотой широковещательный радиомаяк, чтобы оповещать окрестные беспроводные узлы о своем присутствии. Эти широковещательные сигналы содержат основную информацию о точке беспроводного доступа, включая, как правило, SSID, и приглашают беспроводные узлы зарегистрироваться в данной области. Любая рабочая станция, находящаяся в режиме ожидания, может получить SSID и добавить себя в соответствующую сеть. Вещание радиомаяка является «врожденной патологией» беспроводных сетей. Многие модели позволяют отключать содержащую SSID часть этого вещания, чтобы несколько затруднить беспроводное подслушивание, но SSID, тем не менее, посылается при подключении, поэтому все равно существует небольшое окно уязвимости.

Обнаружение WLAN. Для обнаружения беспроводных сетей WLAN используется, например, утилита NetStumber совместно со спутниковым навигатором глобальной системы позициониро-

вания GPS. Данная утилита идентифицирует SSID сети WLAN, а также определяет, используется ли в ней система шифрования WEP. Применение внешней антенны на портативном компьютере делает возможным обнаружение сетей WLAN во время обхода нужного района или поездки по городу. Надежным методом обнаружения WLAN является обследование офисного здания с переносным компьютером в руках.

Подслушивание. Подслушивание ведут для сбора информации о сети, которую предполагается атаковать впоследствии. Перехватчик может использовать добытые данные для того, чтобы получить доступ к сетевым ресурсам. Оборудование, используемое для подслушивания в сети, может быть не сложнее того, которое используется для обычного доступа к этой сети. Беспроводные сети по своей природе позволяют соединять с физической сетью компьютеры, находящиеся на некотором расстоянии от нее, как если бы эти компьютеры находились непосредственно в сети. Например, подключиться к беспроводной сети, располагающейся в здании, может человек, сидящий в машине на стоянке рядом. Атаку посредством пассивного прослушивания практически невозможно обнаружить.

Ложные точки доступа в сеть. Опытный атакующий может организовать ложную точку доступа с имитацией сетевых ресурсов. Абоненты, ничего не подозревая, обращаются к этой ложной точке доступа и сообщают ей свои важные реквизиты, например аутентификационную информацию. Этот тип атак иногда применяют в сочетании с прямым «глушением» истинной точки доступа в сеть.

Отказ в обслуживании. Полную парализацию сети может вызвать атака типа DoS (Denial of Service) — отказ в обслуживании. Ее цель состоит в создании помехи при доступе пользователя к сетевым ресурсам. Беспроводные системы особенно восприимчивы к таким атакам. Физический уровень в беспроводной сети — абстрактное пространство вокруг точки доступа. Злоумышленник может включить устройство, заполняющее весь спектр на рабочей частоте помехами и нелегальным трафиком — такая задача не вызывает особых трудностей. Сам факт проведения DoS-атаки на физическом уровне в беспроводной сети трудно доказать.

Атаки типа «человек-в-середине». Атаки этого типа выполняются на беспроводных сетях гораздо проще, чем на проводных, так как в случае проводной сети требуется реализовать опреде-

ленный вид доступа к ней. Обычно атаки «человек-в-середине» используются для разрушения конфиденциальности и целостности сеанса связи. Атаки MITM более сложные, чем большинство других атак: для их проведения требуется подробная информация о сети. Злоумышленник обычно подменяет идентификацию одного из сетевых ресурсов. Он использует возможность прослушивания и нелегального захвата потока данных с целью изменения его содержимого, необходимого для удовлетворения некоторых своих целей, например для спуфинга IP-адресов, изменения MAC-адреса для имитирования другого хоста и т. д.

Анонимный доступ в Интернет. Незащищенные беспроводные ЛВС обеспечивают хакерам наилучший анонимный доступ для атак через Интернет. Хакеры могут использовать незащищенную беспроводную ЛВС организации для выхода через нее в Интернет, где они будут осуществлять противоправные действия, не оставляя при этом своих следов. Организация с незащищенной ЛВС формально становится источником атакующего трафика, нацеленного на другую компьютерную систему, что связано с потенциальным риском правовой ответственности за причиненный ущерб жертве атаки хакеров.

Описанные выше атаки не являются единственными атаками, используемыми хакерами для взлома беспроводных сетей.

2.3. Обеспечение информационной безопасности сетей

2.3.1. Способы обеспечения информационной безопасности

Существует два подхода к проблеме обеспечения безопасности компьютерных систем и сетей (КС): «фрагментарный» и комплексный [4, 62].

«Фрагментарный» подход направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т. п.

Достоинством такого подхода является высокая избирательность к конкретной угрозе. Существенный недостаток — отсутст-

вие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов КС только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты.

Комплексный подход ориентирован на создание защищенной среды обработки информации в КС, объединяющей в единый комплекс разнородные меры противодействия угрозам. Организация защищенной среды обработки информации позволяет гарантировать определенный уровень безопасности КС, что является несомненным достоинством комплексного подхода. К недостаткам этого подхода относятся: ограничения на свободу действий пользователей КС, чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

Комплексный подход применяют для защиты КС крупных организаций или небольших КС, выполняющих ответственные задачи или обрабатывающих особо важную информацию. Нарушение безопасности информации в КС крупных организаций может нанести огромный материальный ущерб как самим организациям, так и их клиентам. Поэтому такие организации вынуждены уделять особое внимание гарантиям безопасности и реализовывать комплексную защиту. Комплексного подхода придерживаются большинство государственных и крупных коммерческих предприятий и учреждений. Этот подход нашел свое отражение в различных стандартах.

Комплексный подход к проблеме обеспечения безопасности основан на разработанной для конкретной КС политике безопасности. Политика безопасности регламентирует эффективную работу средств защиты КС. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Надежная система безопасности сети не может быть создана без эффективной политики сетевой безопасности. Политики безопасности подробно рассматриваются в гл. 3.

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного (стандарты, законы, нормативные акты и т. п.);
- административно-организационного (действия общего характера, предпринимаемые руководством организа-

ции, и конкретные меры безопасности, имеющие дело с людьми);

- программно-технического (конкретные технические меры).

Меры законодательного уровня очень важны для обеспечения информационной безопасности. К этому уровню относится комплекс мер, направленных на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности.

Информационная безопасность — это новая область деятельности, здесь важно не только запрещать и наказывать, но и учить, разъяснять, помогать. Общество должно осознать важность данной проблематики, понять основные пути решения соответствующих проблем. Государство может сделать это оптимальным образом. Здесь не нужно больших материальных затрат, требуются интеллектуальные вложения.

Меры административно-организационного уровня. Администрация организации должна сознавать необходимость поддержания режима безопасности и выделять на эти цели соответствующие ресурсы. Основой мер защиты административно-организационного уровня является политика безопасности (см. гл. 3) и комплекс организационных мер.

К комплексу организационных мер относятся меры безопасности, реализуемые людьми. Выделяют следующие группы организационных мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Для каждой группы в каждой организации должен существовать набор регламентов, определяющих действия персонала.

Меры и средства программно-технического уровня. Для поддержания режима информационной безопасности особенно важны меры программно-технического уровня, поскольку основная угроза компьютерным системам исходит от них самих: сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т. п. В рамках современных информационных систем должны быть доступны следующие механизмы безопасности:

- идентификация и проверка подлинности пользователей;
- управление доступом;

- протоколирование и аудит;
- криптография;
- экранирование;
- обеспечение высокой доступности.

Необходимость применения стандартов. Информационные системы (ИС) компаний почти всегда построены на основе программных и аппаратных продуктов различных производителей. Пока нет ни одной компании-разработчика, которая предоставила бы потребителю полный перечень средств (от аппаратных до программных) для построения современной ИС. Чтобы обеспечить в разнородной ИС надежную защиту информации требуются специалисты высокой квалификации, которые должны отвечать за безопасность каждого компонента ИС: правильно их настраивать, постоянно отслеживать происходящие изменения, контролировать работу пользователей. Очевидно, что чем разнороднее ИС, тем сложнее обеспечить ее безопасность. Изобилие в корпоративных сетях и системах устройств защиты, межсетевых экранов (МЭ), шлюзов и VPN, а также растущий спрос на доступ к корпоративным данным со стороны сотрудников, партнеров и заказчиков приводят к созданию сложной среды защиты, трудной для управления, а иногда и несовместимой.

Интероперабельность продуктов защиты является неотъемлемым требованием для КИС. Для большинства гетерогенных сред важно обеспечить согласованное взаимодействие с продуктами других производителей. Принятое организацией решение безопасности должно гарантировать защиту на всех платформах в рамках этой организации. Поэтому вполне очевидна потребность в применении единого набора стандартов как поставщиками средств защиты, так и компаниями — системными интеграторами и организациями, выступающими в качестве заказчиков систем безопасности для своих корпоративных сетей и систем.

Стандарты образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности, и определяют критерии, которым должно следовать управление безопасностью. Стандарты являются необходимой основой, обеспечивающей совместимость продуктов разных производителей, что чрезвычайно важно при создании систем сетевой безопасности в гетерогенных средах. Международные и отечественные стандарты информационной безопасности рассматриваются в гл. 4.

Комплексный подход к решению проблемы обеспечения безопасности, рациональное сочетании законодательных, административно-организационных и программно-технических мер и обязательное следование промышленным, национальным и международным стандартам — это тот фундамент, на котором строится вся система защиты корпоративных сетей.

2.3.2. Пути решения проблем защиты информации в сетях

Для поиска решений проблем информационной безопасности при работе в сети Интернет был создан независимый консорциум ISTF (Internet Security Task Force) — общественная организация, состоящая из представителей и экспертов компаний-поставщиков средств информационной безопасности, электронных бизнесов и провайдеров Internet-инфраструктуры. Цель консорциума — разработка технических, организационных и операционных руководств по безопасности работы в Internet.

Консорциум ISTF выделил 12 областей информационной безопасности, на которых в первую очередь должны сконцентрировать свое внимание создатели электронного бизнеса, чтобы обеспечить его работоспособность. Этот список, в частности, включает:

- аутентификацию (механизм объективного подтверждения идентифицирующей информации);
- право на частную, персональную информацию (обеспечение конфиденциальности информации);
- определение событий безопасности (Security Events);
- защиту корпоративного периметра;
- определение атак;
- контроль за потенциально опасным содержимым;
- контроль доступа;
- администрирование;
- реакцию на события (Incident Response).

Рекомендации ISTF предназначены для существующих или вновь образуемых компаний электронной коммерции и электронного бизнеса.

Их реализация означает, что защита информации в системе электронного бизнеса должна быть комплексной.

Для комплексной защиты от угроз и гарантии экономически выгодного и безопасного использования коммуникационных ресурсов для электронного бизнеса необходимо:

- проанализировать угрозы безопасности для системы электронного бизнеса;
- разработать политику информационной безопасности;
- защитить внешние каналы передачи информации, обеспечив конфиденциальность, целостность и подлинность передаваемой по ним информации;
- гарантировать возможность безопасного доступа к открытым ресурсам внешних сетей и Internet, а также общения с пользователями этих сетей;
- защитить отдельные наиболее коммерчески значимые ИС независимо от используемых ими каналов передачи данных;
- предоставить персоналу защищенный удаленный доступ к информационным ресурсам корпоративной сети;
- обеспечить надежное централизованное управление средствами сетевой защиты.

Согласно рекомендациям ISTF, первым и важнейшим этапом разработки системы информационной безопасности электронного бизнеса являются механизмы управления доступом к сетям общего пользования и доступом из них, а также механизмы безопасных коммуникаций, реализуемые МЭ и продуктами защищенных виртуальных сетей VPN.

Сопровождая их средствами интеграции и управления всей ключевой информацией системы защиты (PKI — инфраструктура открытых ключей), можно получить целостную, централизованно управляемую систему информационной безопасности.

Следующий этап включает интегрируемые в общую структуру средства контроля доступа пользователей в систему вместе с системой однократного входа и авторизации (Single Sign On).

Антивирусная защита, средства аудита и обнаружения атак, по существу, завершают создание интегрированной целостной системы безопасности, если речь не идет о работе с конфиденциальными данными. В этом случае требуются средства криптографической защиты данных и электронно-цифровой подписи.

Для реализации основных функциональных компонентов системы безопасности для электронного бизнеса применяются различные методы и средства защиты информации:

- защищенные коммуникационные протоколы;
- средства криптографии;

- механизмы аутентификации и авторизации;
- средства контроля доступа к рабочим местам сети и из сетей общего пользования;
- антивирусные комплексы;
- программы обнаружения атак и аудита;
- средства централизованного управления контролем доступа пользователей, а также безопасного обмена пакетами данных и сообщениями любых приложений по открытым IP-сетям.

Применение комплекса средств защиты на всех уровнях корпоративной системы позволяет построить эффективную и надежную систему обеспечения информационной безопасности.

Перечисленные выше методы и средства защиты информации подробно рассматриваются в последующих главах книги.

Глава 3
ПОЛИТИКА БЕЗОПАСНОСТИ

Под *политикой безопасности* организации понимают совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности является тем средством, с помощью которого реализуется деятельность в компьютерной информационной системе организации. Вообще политика безопасности определяется используемой компьютерной средой и отражает специфические потребности организации.

Обычно КИС представляет собой сложный комплекс разнородного, иногда плохо согласующегося между собой аппаратного и программного обеспечения: компьютеров, ОС, сетевых средств, СУБД, разнообразных приложений. Все эти компоненты обычно обладают собственными средствами защиты, которые нужно согласовать между собой. Поэтому в качестве согласованной платформы по обеспечению безопасности корпоративной системы очень важна эффективная политика безопасности. По мере роста компьютерной системы и интеграции ее в глобальную сеть, необходимо обеспечить отсутствие в системе слабых мест, поскольку все усилия по защите информации могут быть обесценены лишь одной оплошностью.

Политику безопасности можно построить таким образом, чтобы она устанавливала, кто имеет доступ к конкретным активам и приложениям, какие роли и обязанности будут иметь конкретные лица, а также предусмотреть процедуры безопасности, которые четко предписывают, как должны выполняться конкретные задачи безопасности. Особенности работы конкретного сотрудника могут потребовать доступа к информации, которая не должна быть доступна другим работникам. Например, менеджер по персоналу может иметь доступ к частной информации любого сотрудника, в то время как специалист по отчетности

может иметь доступ только к финансовым данным этих сотрудников, а рядовой сотрудник будет иметь доступ только к своей собственной персональной информации.

Политика безопасности определяет позицию организации по рациональному использованию компьютеров и сети, а также процедуры по предотвращению и реагированию на инциденты безопасности. В большой корпоративной системе может применяться широкий диапазон разных политик — от бизнес-политик до специфичных правил доступа к наборам данных. Эти политики полностью определяются конкретными потребностями организации.

3.1. Основные понятия политики безопасности

Политика безопасности определяет стратегию управления в области информационной безопасности, а также меру внимания и количество ресурсов, которые считает целесообразным выделить руководство.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для ИС организации. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого конкретными документами специализированных политик и процедур безопасности.

Высокоуровневая политика безопасности должна периодически пересматриваться, гарантируя тем самым учет текущих потребностей организации. Документ политики составляют таким образом, чтобы политика была относительно независимой от конкретных технологий, в этом случае документ не потребуется изменять слишком часто.

Для того чтобы познакомиться с основными понятиями политики безопасности рассмотрим в качестве конкретного примера гипотетическую локальную сеть, принадлежащую некоторой организации, и ассоциированную с ней политику безопасности [5, 63].

Политика безопасности обычно оформляется в виде документа, включающего такие разделы, как описание проблемы, область применения, позиция организации, распределение ролей и обязанностей, санкции и др.

Описание проблемы. Информация, циркулирующая в рамках локальной сети, является критически важной. Локальная сеть позволяет пользователям совместно использовать программы и данные, что увеличивает угрозу безопасности. Поэтому каждый из компьютеров, входящих в сеть, нуждается в более сильной защите. Эти повышенные меры безопасности и являются темой данного документа, который призван продемонстрировать сотрудникам организации важность защиты сетевой среды, описать их роль в обеспечении безопасности, а также распределить конкретные обязанности по защите информации, циркулирующей в сети.

Область применения. В сферу действия данной политики попадают все аппаратные, программные и информационные ресурсы, входящие в локальную сеть предприятия. Политика ориентирована также на людей, работающих с сетью, в том числе на пользователей, субподрядчиков и поставщиков.

Позиция организации. Основные цели — обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности. К частным целям относятся:

- обеспечение уровня безопасности, соответствующего нормативным документам;
- следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности);
- обеспечение безопасности в каждой функциональной области локальной сети;
- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
- обеспечение анализа регистрационной информации;
- предоставление пользователям достаточной информации для сознательного поддержания режима безопасности;
- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;
- обеспечение соответствия с имеющимися законами и общеорганизационной политикой безопасности.

Распределение ролей и обязанностей. За реализацию сформулированных выше целей отвечают соответствующие должностные лица и пользователи сети.

Руководители подразделений отвечают за доведение положений политики безопасности до пользователей и за контакты с ними.

Администраторы локальной сети обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности. Они обязаны:

- обеспечивать защиту оборудования локальной сети, в том числе интерфейсов с другими сетями;
- оперативно и эффективно реагировать на события, таящие угрозу, информировать администраторов сервисов о попытках нарушения защиты;
- использовать проверенные средства аудита и обнаружения подозрительных ситуаций, ежедневно анализировать регистрационную информацию, относящуюся к сети в целом и к файловым серверам в особенности;
- не злоупотреблять своими полномочиями, так как пользователи имеют право на тайну;
- разрабатывать процедуры и подготавливать инструкции для защиты локальной сети от вредоносного программного обеспечения, оказывать помощь в обнаружении и ликвидации вредоносного кода;
- регулярно выполнять резервное копирование информации, хранящейся на файловых серверах;
- выполнять все изменения сетевой аппаратно-программной конфигурации;
- гарантировать обязательность процедуры идентификации и аутентификации для доступа к сетевым ресурсам, выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;
- периодически производить проверку надежности защиты локальной сети, не допускать получения привилегий неавторизованными пользователями.

Администраторы сервисов отвечают за конкретные сервисы, и в частности за построение защиты в соответствии с общей политикой безопасности. Они обязаны:

- управлять правами доступа пользователей к обслуживаемым объектам;

- оперативно и эффективно реагировать на события, таящие угрозу, оказывать помощь в отражении угрозы, выявлении нарушителей и предоставлении информации для их наказания;
- регулярно выполнять резервное копирование информации, обрабатываемой сервисом;
- выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;
- ежедневно анализировать регистрационную информацию, относящуюся к сервису, регулярно контролировать сервис на предмет вредоносного программного обеспечения;
- периодически производить проверку надежности защиты сервиса, не допускать получения привилегий неавторизованными пользователями.

Пользователи работают с локальной сетью в соответствии с политикой безопасности, подчиняются распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставят в известность руководство обо всех подозрительных ситуациях. Они обязаны:

- знать и соблюдать законы, правила, принятые в данной организации, политику безопасности, процедуры безопасности, использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;
- использовать механизм защиты файлов и должным образом задавать права доступа;
- выбирать качественные пароли, регулярно менять их, не записывать пароли на бумаге, не сообщать их другим лицам;
- информировать администраторов или руководство о нарушениях безопасности и иных подозрительных ситуациях;
- не использовать слабости в защите сервисов и локальной сети в целом, не совершать неавторизованной работы с данными, не создавать помех другим пользователям;
- всегда сообщать корректную идентификационную и аутентификационную информацию, не пытаться работать от имени других пользователей;
- обеспечивать резервное копирование информации с жесткого диска своего компьютера;
- знать принципы работы вредоносного программного обеспечения, пути его проникновения и распространения, знать и соблюдать процедуры для предупреждения про-

никновения вредоносного кода, его обнаружения и уничтожения;

- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

Санкции. Нарушение политики безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Случаи нарушения безопасности со стороны персонала должны оперативно рассматриваться руководством для принятия дисциплинарных мер вплоть до увольнения.

Дополнительная информация. Конкретным группам исполнителей могут потребоваться для ознакомления дополнительные документы, в частности, документы специализированных политик и процедур безопасности, а также другие руководящие указания. Необходимость в дополнительных документах политик безопасности в значительной степени зависит от размеров и сложности организации. Для достаточно большой организации могут потребоваться в дополнение к базовой политике специализированные политики безопасности. Организации меньшего размера нуждаются только в некотором подмножестве специализированных политик. Многие из этих документов поддержки могут быть краткими — объемом в одну-две страницы.

Управленческие меры обеспечения информационной безопасности

Главной целью мер, предпринимаемых на управленческом уровне, является формирование программы работ в области информационной безопасности и обеспечение ее выполнения путем выделения необходимых ресурсов и осуществления регулярного контроля состояния дел. Основой этой программы является многоуровневая политика безопасности, отражающая комплексный подход организации к защите своих ресурсов и информационных активов.

С практической точки зрения политики безопасности можно разделить на три уровня: верхний, средний и нижний [5, 6].

Верхний уровень политики безопасности определяет решения, затрагивающие организацию в целом. Эти решения носят весьма общий характер и исходят, как правило, от руководства организации.

Такие решения могут включать в себя следующие элементы:

- формулировку целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- формирование или пересмотр комплексной программы обеспечения информационной безопасности, определение ответственных лиц за продвижение программы;
- обеспечение материальной базы для соблюдения законов и правил;
- формулировку управленческих решений по вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Политика безопасности верхнего уровня формулирует цели организации в области информационной безопасности в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане должна стоять *целостность* данных. Для организации, занимающейся продажами, важна актуальность информации о предоставляемых услугах и ценах, а также ее *доступность* максимальному числу потенциальных покупателей. Режимная организация в первую очередь будет заботиться о *конфиденциальности* информации, т. е. о ее защите от НСД.

На верхний уровень выносится управление ресурсами безопасности и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко определять сферу своего влияния. В нее могут быть включены не только все компьютерные системы организации, но и домашние компьютеры сотрудников, если политика регламентирует некоторые аспекты их использования. Возможна и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и по проведению ее в жизнь, т. е. политика может служить основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за вы-

работку программы безопасности. В-третьих, необходимо обеспечить исполнительскую дисциплину персонала с помощью системы поощрений и наказаний.

Средний уровень политики безопасности определяет решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией. Примеры таких вопросов — отношение к доступу в Internet (проблема сочетания свободы получения информации с защитой от внешних угроз), использование домашних компьютеров и т. д.

Политика безопасности среднего уровня должна определять для каждого аспекта информационной безопасности следующие моменты:

- *описание аспекта* — позиция организации может быть сформулирована в достаточно общем виде, а именно как набор целей, которые преследует организация в данном аспекте;
- *область применения* — следует специфицировать, где, когда, как, по отношению к кому и чему применяется данная политика безопасности;
- *роли и обязанности* — документ должен содержать информацию о должностных лицах, отвечающих за проведение политики безопасности в жизнь;
- *санкции* — 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 должностное лицо.

Нижний уровень политики безопасности относится к конкретным сервисам. Она включает два аспекта — цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть более детальной, т. е. при следовании политике безопасности нижнего уровня необходимо дать ответ, например, на такие вопросы:

- кто имеет право доступа к объектам, поддерживаемым сервисом;
- при каких условиях можно читать и модифицировать данные;
- как организован удаленный доступ к сервису.

Политика безопасности нижнего уровня может исходить из соображений целостности, доступности и конфиденциальности, но она не должна на них останавливаться. В общем случае цели должны связывать между собой объекты сервиса и осмысленные действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем детальнее правила, чем более четко и формально они изложены, тем проще поддерживать их выполнение программно-техническими мерами. Обычно наиболее формально задаются права доступа к объектам.

3.2. Структура политики безопасности организации

Для большинства организаций политика безопасности абсолютно необходима. Она определяет отношение организации к обеспечению безопасности и необходимые действия организации по защите своих ресурсов и активов. На основе политики безопасности устанавливаются необходимые средства и процедуры безопасности, а также определяются роли и ответственность сотрудников организации в обеспечении безопасности.

Обычно политика безопасности организации включает:

- базовую политику безопасности;
- специализированные политики безопасности;
- процедуры безопасности.

Основные положения политики безопасности организации описываются в следующих документах:

- *обзор политики безопасности* — раскрывает цель политики безопасности, описывает структуру политики безопасности, подробно излагает, кто и за что отвечает, устанавливает процедуры и предполагаемые временные рамки для внесения изменений. В зависимости от масштаба организации политика безопасности может содержать больше или меньше разделов;
- *описание базовой политики безопасности* — определяет разрешенные и запрещенные действия, а также необходимые средства управления в рамках реализуемой архитектуры безопасности;
- *руководство по архитектуре безопасности* — описывает реализацию механизмов безопасности в компонентах архитектуры, используемых в сети организации (рис. 3.1).

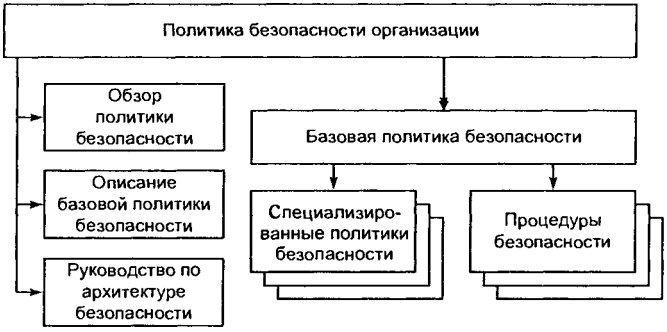


Рис. 3.1. Структура политики безопасности организации

Главным компонентом политики безопасности организации является базовая политика безопасности [9].

3.2.1. Базовая политика безопасности

Базовая политика безопасности устанавливает, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать.

Нисходящий подход, реализуемый базовой политикой безопасности, дает возможность постепенно и последовательно выполнять работу по созданию системы безопасности, не пытаясь сразу выполнить ее целиком. Базовая политика позволяет в любое время ознакомиться с политикой безопасности в полном объеме и выяснить текущее состояние безопасности в организации.

Структура и состав политики безопасности зависит от размера и целей компании. Обычно базовая политика безопасности организации поддерживается набором специализированных политик и процедур безопасности.

3.2.2. Специализированные политики безопасности

Потенциально существуют десятки специализированных политик, которые могут применяться большинством организаций среднего и большого размера. Некоторые политики предназначаются для каждой организации, другие — специфичны для определенных компьютерных окружений.

С учетом особенностей применения специализированные политики безопасности можно разделить на две группы:

- политики, затрагивающие значительное число пользователей;
- политики, связанные с конкретными техническими областями.

К специализированным политикам, затрагивающим значительное число пользователей, относятся:

- политика допустимого использования;
- политика удаленного доступа к ресурсам сети;
- политика защиты информации;
- политика защиты паролей и др.

К специализированным политикам, связанным с конкретными техническими областями, относятся:

- политика конфигурации межсетевых экранов;
- политика по шифрованию и управлению криптоключами;
- политика безопасности виртуальных защищенных сетей VPN;
- политика по оборудованию беспроводной сети и др.

Рассмотрим подробнее некоторые из ключевых специализированных политик.

Политика допустимого использования. Ее цель — установление стандартных норм безопасного использования компьютерного оборудования и сервисов в компании, а также соответствующих мер безопасности сотрудников для защиты корпоративных ресурсов и собственной информации. Неправильное использование компьютерного оборудования и сервисов подвергает компанию рискам, включая вирусные атаки, компрометацию сетевых систем и сервисов. Конкретный тип и количество политик допустимого использования зависят от результатов анализа требований бизнеса, оценки рисков и корпоративной культуры в организации.

Политика допустимого использования применяется к сотрудникам, консультантам, временным служащим и другим работникам компании, включая сотрудников сторонних организаций. Политика допустимого использования предназначена в основном для конечных пользователей и указывает им, какие действия разрешаются, а какие запрещены. Без зафиксированной в соответствующем документе политики допустимого использования, штатные сотрудники управления и поддержки сети не имеют формальных оснований для применения санкций к своему или

стороннему сотруднику, который допустил грубое нарушение правил безопасной работы на компьютере или в сети.

Политика допустимого использования устанавливает:

- ответственность пользователей за защиту любой информации, используемой и/или хранимой их компьютерами;
- правомочность пользователей читать и копировать файлы, которые не являются их собственными, но доступны им;
- уровень допустимого использования электронной почты и Web-доступа.

Для образовательных и государственных учреждений политика допустимого использования, по существу, просто обязательна.

Специального формата для политики допустимого использования не существует: должно быть указано имя сервиса, системы или подсистемы (например политика использования компьютера, электронной почты, компактных компьютеров и паролей) и описано в самых четких терминах разрешенное и запрещенное поведение, а также последствия нарушения ее правил и санкции, накладываемые на нарушителя.

Разработка политики допустимого использования выполняется квалифицированными специалистами по соответствующему сервису, системе или подсистеме под контролем комиссии (команды), которой поручена разработка политики безопасности организации.

Политика удаленного доступа. Ее цель — установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании. Стандартные нормы призваны минимизировать ущерб компании из-за возможного неавторизованного использования ресурсов компании. К такому ущербу относятся: утрата интеллектуальной собственности компании, потеря конфиденциальных данных, искажение имиджа компании, повреждения критических внутренних систем компании и т. д.

Эта политика касается всех сотрудников, поставщиков и агентов компании при использовании ими для удаленного соединения с сетью компании компьютеров или рабочих станций, являющихся собственностью компании или находящихся в личной собственности.

Политика удаленного доступа:

- намечает и определяет допустимые методы удаленного соединения с внутренней сетью;
- существенна в большой организации, где сети территориально распределены;

- должна охватывать по возможности все распространенные методы удаленного доступа к внутренним ресурсам.

Политика удаленного доступа определяет:

- какие методы разрешаются для удаленного доступа;
- ограничения на данные, к которым можно получить удаленный доступ;
- кто может иметь удаленный доступ.

Защищенный удаленный доступ должен быть строго контролируемым. Применяемая процедура контроля должна гарантировать, что доступ к надлежащей информации или сервисам получат только прошедшие проверку люди. Сотрудник компании не должен передавать свой логин и пароль никогда и никому, включая членов семьи. Управление удаленным доступом не должно быть сложным и приводить к возникновению ошибок.

Контроль доступа целесообразно выполнять с помощью одноразовой парольной аутентификации или с помощью открытых/секретных ключей (см. гл. 7 и 13).

Сотрудники компании с правами удаленного доступа должны гарантировать, что принадлежащие им или компании персональный компьютер или рабочая станция, которые удаленно подсоединены к корпоративной сети компании, не будут связаны в это же время с какой-либо другой сетью, за исключением персональных сетей, находящихся под полным контролем пользователя. Кроме того, их соединение удаленного доступа должно иметь такие же характеристики безопасности, как обычное локальное соединение с компанией.

Все хосты, которые подключены к внутренним сетям компании с помощью технологий удаленного доступа, должны использовать самое современное антивирусное обеспечение. Это требование относится и к персональным компьютерам компании.

Любой сотрудник компании, уличенный в нарушении данной политики, может быть подвергнут дисциплинарному взысканию вплоть до увольнения с работы.

3.2.3. Процедуры безопасности

Процедуры безопасности являются необходимым и важным дополнением к политикам безопасности. Политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты. Процедуры безопасности определяют,

как защитить ресурсы и каковы механизмы исполнения политики, т. е. как реализовывать политики безопасности.

По существу процедуры безопасности представляют собой пошаговые инструкции для выполнения оперативных задач. Часто процедура является тем инструментом, с помощью которого политика преобразуется в реальное действие. Например, политика паролей формулирует правила конструирования паролей, правила о том, как защитить пароль и как часто его заменять. Процедура управления паролями описывает процесс создания новых паролей, их распределения, а также процесс гарантированной смены паролей на критичных устройствах.

Процедуры безопасности детально определяют действия, которые нужно предпринять при реагировании на конкретные события; обеспечивают быстрое реагирование в критической ситуации; помогают устранить проблему единой точки отказа в работе, если, например, во время кризиса работник неожиданно покидает рабочее место или оказывается недоступен.

Многие процедуры, связанные с безопасностью, должны быть стандартными средствами в любом подразделении. В качестве примеров можно указать процедуры для резервного копирования и внесистемного хранения защищенных копий, а также процедуры для вывода пользователя из активного состояния и/или архивирования логина и пароля пользователя, применяемые сразу, как только данный пользователь увольняется из организации.

Рассмотрим несколько важных процедур безопасности, которые необходимы почти каждой организации.

Процедура реагирования на события является необходимым средством безопасности для большинства организаций. Организация особенно уязвима, когда обнаруживается вторжение в ее сеть или когда она сталкивается со стихийным бедствием.

Процедуру реагирования на события иногда называют *процедурой обработки событий* или *процедурой реагирования на инциденты*. Практически невозможно указать отклики на все события нарушений безопасности, но нужно стремиться охватить основные типы нарушений, которые могут произойти. Например: сканирование портов сети, атака типа «отказ в обслуживании», компрометация хоста, НСД и др.

Данная процедура определяет:

- обязанности членов команды реагирования;
- какую информацию регистрировать и прослеживать;

- как обрабатывать исследование отклонений от нормы и атаки вторжения;
- кого и когда уведомлять;
- кто может выпускать в свет информацию и какова процедура выпуска информации;
- как должен выполняться последующий анализ и кто будет в этом участвовать.

В команду реагирования могут быть включены должностные лица компании, менеджер маркетинга (для связи с прессой), системный и сетевой администраторы и представитель соответствующих правоохранительных органов. Процедура должна указать, когда и в каком порядке они вызываются.

Процедура управления конфигурацией обычно определяется на корпоративном уровне или уровне подразделения. Эта процедура должна определить процесс документирования и запроса изменений конфигурации на всех уровнях принятия решений. В принципе должна существовать центральная группа, которая рассматривает все запросы на изменения конфигурации и принимает необходимые решения.

Процедура управления конфигурацией определяет:

- кто имеет полномочия выполнить изменения конфигурации аппаратного и программного обеспечения;
- как тестируется и инсталлируется новое аппаратное и программное обеспечение;
- как документируются изменения в аппаратном и программном обеспечении;
- кто должен быть проинформирован, когда случаются изменения в аппаратном и программном обеспечении.

Процесс управления конфигурацией важен, так как документирует сделанные изменения и обеспечивает возможность аудита; документирует возможный простой системы; дает способ координировать изменения так, чтобы одно изменение не помешало другому.

Глава 4
СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проблемой информационной компьютерной безопасности начали заниматься с того момента, когда компьютер стал обрабатывать данные, ценность которых высока для пользователя. С развитием компьютерных сетей и ростом спроса на электронные услуги ситуация в сфере информационной безопасности серьезно обострилась, а вопрос стандартизации подходов к ее решению стал особенно актуальным как для разработчиков, так и для пользователей ИТ-средств.

4.1. Роль стандартов информационной безопасности

Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов ИТ. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности.

Потребители заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности. Потребители также нуждаются в инструменте, с помощью которого они могли бы формулировать свои требования производителям. При этом потребителей интересуют исключительно характеристики и свойства конечного продукта, а не методы и средства их достижения. К сожалению, многие потребители не понимают, что требования безопасности обязательно противоречат функциональным требованиям (удобству работы, быстродействию и т. д.), накладывают ограничения на совместимость и, как

правило, вынуждают отказаться от широко распространенных и поэтому незащищенных прикладных программных средств.

Производители нуждаются в стандартах как средстве сравнения возможностей своих продуктов, в применении процедуры сертификации как механизма объективной оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора. С точки зрения производителя требования безопасности должны быть максимально конкретными и регламентировать необходимость применения тех или иных средств, механизмов, алгоритмов и т. д. Кроме того, требования не должны противоречить существующим парадигмам обработки информации, архитектуре вычислительных систем и технологиям создания информационных продуктов. Однако такой подход также нельзя признать в качестве доминирующего, так как он не учитывает нужд пользователей и пытается подогнать требования защиты под существующие системы и технологии.

Эксперты по квалификации и *специалисты по сертификации* рассматривают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый продуктами ИТ, и предоставить потребителям возможность сделать обоснованный выбор. Эксперты по квалификации находятся в двойственном положении: с одной стороны, они, как и производители, заинтересованы в четких и простых критериях, над которыми не надо ломать голову, как их применить к конкретному продукту, а с другой стороны, они должны дать обоснованный ответ пользователям — удовлетворяет продукт их нужды или нет.

Таким образом, перед стандартами информационной безопасности стоит непростая задача — примирить три разные точки зрения и создать эффективный механизм взаимодействия всех сторон. Причем ущемление потребностей хотя бы одной из них приведет к невозможности взаимопонимания и взаимодействия и, следовательно, не позволит решить общую задачу — создание защищенной системы обработки информации.

Необходимость в таких стандартах была осознана достаточно давно, и в этом направлении достигнут существенный прогресс, закрепленный в документах разработки 1990-х гг. Первым и наиболее известным документом была *Оранжевая книга* (по цвету обложки) «Критерии безопасности компьютерных систем» Министерства обороны США. В этом документе определе-

ны 4 *уровня безопасности* — D, C, B и A. По мере перехода от уровня D до A к надежности системы предъявляются все более жесткие требования. Уровни C и B подразделяются на *классы* (C1, C2, B1, B2, B3). Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому *классу*, ее защита должна удовлетворять оговоренным требованиям. К другим важным стандартам информационной безопасности этого поколения относятся: «Руководящие документы Гостехкомиссии России», «Европейские критерии безопасности информационных технологий», «Федеральные критерии безопасности информационных технологий США», «Канадские критерии безопасности компьютерных систем» [30, 63].

В последнее время в разных странах появилось новое поколение стандартов, посвященных практическим вопросам управления информационной безопасностью компании. Это прежде всего международные стандарты управления информационной безопасностью ISO 15408, ISO 17799 и некоторые другие. Представляется целесообразным проанализировать наиболее важные из этих документов, сопоставить содержащиеся в них требования и критерии, а также оценить эффективность их практического применения.

4.2. Международные стандарты информационной безопасности

В соответствии с международными и национальными стандартами обеспечение информационной безопасности в любой компании предполагает следующее:

- определение целей обеспечения информационной безопасности компьютерных систем;
- создание эффективной системы управления информационной безопасностью;
- расчет совокупности детализированных качественных и количественных показателей для оценки соответствия информационной безопасности поставленным целям;
- применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
- использование методик управления безопасностью, позволяющих объективно оценить защищенность информацион-

ных активов и управлять информационной безопасностью компании.

Рассмотрим наиболее известные международные стандарты в области защиты информации, которые могут быть использованы в отечественных условиях [52].

4.2.1. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)

Международный стандарт ISO/IEC 17799:2000 (BS 7799—1:2000) «Управление информационной безопасностью — Информационные технологии» («Information technology — Information security management») является одним из наиболее известных стандартов в области защиты информации. Данный стандарт был разработан на основе первой части Британского стандарта BS 7799—1:1995 «Практические рекомендации по управлению информационной безопасностью» («Information security management — Part 1: Code of practice for information security management») и относится к новому поколению стандартов информационной безопасности компьютерных ИС.

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799—1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;
- классификация и управление корпоративными информационными ресурсами;
- кадровый менеджмент и информационная безопасность;
- физическая безопасность;
- администрирование безопасности КИС;
- управление доступом;
- требования по безопасности к КИС в ходе их разработки, эксплуатации и сопровождения;
- управление бизнес-процессами компании с точки зрения информационной безопасности;
- внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799—2:2000 «Спецификации систем управления информационной безопасностью» («Information security management — Part 2: Specification for information security management systems»), определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита КИС.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов — British Standards Institution (BSI), изданные в 1995—2003 гг. в виде следующей серии:

- «Введение в проблему управления информационной безопасностью» («Information security managment: an introduction»);
- «Возможности сертификации на требования стандарта BS 7799» («Preparing for BS 7799 sertification»);
- «Руководство BS 7799 по оценке и управлению рисками» («Guide to BS 7799 risk assessment and risk management»);
- «Руководство для проведения аудита на требования стандарта» («BS 7799 Guide to BS 7799 auditing»);
- «Практические рекомендации по управлению безопасностью информационных технологий» («Code of practice for IT management»).

В 2002 г. международный стандарт ISO 17799 (BS 7799) был пересмотрен и существенно дополнен. В новом варианте этого стандарта большое внимание уделено вопросам повышения культуры защиты информации в различных международных компаниях. По мнению специалистов, обновление международного стандарта ISO 17799 (BS 7799) позволит не только повысить культуру защиты информационных активов компании, но и скоординировать действия различных ведущих государственных и коммерческих структур в области защиты информации.

4.2.2. Германский стандарт BSI

В отличие от ISO 17799 германское «Руководство по защите информационных технологий для базового уровня защищенности» посвящено детальному рассмотрению частных вопросов управления информационной безопасностью компании.

В германском стандарте BSI представлены:

- общая методика управления информационной безопасностью (организация менеджмента в области информационной безопасности, методология использования руководства);
- описания компонентов современных ИТ;
- описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса);
- характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны);
- характеристики основных информационных активов компании (в том числе аппаратное и программное обеспечение, например рабочие станции и серверы под управлением ОС семейства DOS, Windows и UNIX);
- характеристики компьютерных сетей на основе различных сетевых технологий, например сети Novell NetWare, сети UNIX и Windows).
- характеристика активного и пассивного телекоммуникационного оборудования ведущих поставщиков, например Cisco Systems;
- подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).

Вопросы защиты приведенных информационных активов компании рассматриваются по определенному сценарию: общее описание информационного актива компании — возможные угрозы и уязвимости безопасности — возможные меры и средства контроля и защиты.

4.2.3. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»

Одним из главных результатов стандартизации в сфере систематизации требований и характеристик защищенных информационных комплексов стала система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных документов. Важное место в этой

системе стандартов занимает стандарт ISO 15408, известный как «Common Criteria».

В 1990 г. Международная организация по стандартизации (ISO) приступила к разработке международного стандарта по критериям оценки безопасности ИТ для общего использования. В разработке участвовали: Национальный институт стандартов и технологии и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Голландия), органы исполнения Программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция), которые опирались на свой солидный задел.

За десятилетие разработки лучшими специалистами мира документ неоднократно редактировался. Первые две версии были опубликованы соответственно в январе и мае 1998 г. Версия 2.1 этого стандарта утверждена 8 июня 1999 г. Международной организацией по стандартизации (ISO) в качестве международного стандарта информационной безопасности ISO/IEC 15408 под названием «Общие критерии оценки безопасности информационных технологий», или «Common Criteria».

«Общие критерии» (ОК) обобщили содержание и опыт использования Оранжевой книги, развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США.

В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК — полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.

Ведущие мировые производители оборудования ИТ сразу стали поставлять заказчикам средства, полностью отвечающие требованиям ОК.

ОК разрабатывались для удовлетворения запросов трех групп специалистов, в равной степени являющихся пользователями этого документа: производителей и потребителей продуктов ИТ, а также экспертов по оценке уровня их безопасности. ОК обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламенти-

руют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

ОК рассматривают информационную безопасность, во-первых, как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ-продуктом, а также доступности ресурсов ВС и, во-вторых, ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации. Поэтому в концепцию ОК входят все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности.

Потребители ИТ-продуктов озабочены наличием угроз безопасности, приводящих к определенным рискам для обрабатываемой информации. Для противодействия этим угрозам ИТ-продукты должны включать в свой состав средства защиты, противодействующие этим угрозам и направленные на устранение уязвимостей, однако ошибки в средствах защиты в свою очередь могут приводить к появлению новых уязвимостей. Сертификация средств защиты позволяет подтвердить их адекватность угрозам и рискам.

ОК регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов. ОК предлагают концепцию процесса разработки и квалификационного анализа ИТ-продуктов, требующую от потребителей и производителей большой работы по составлению и оформлению объемных и подробных нормативных документов.

Требования ОК являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности ИТ.

Стандарт ISO 15408 поднял стандартизацию ИТ на межгосударственный уровень. Возникла реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных ИС, что в свою очередь откроет новые сферы применения ИТ.

Принятый базовый стандарт информационной безопасности ISO 15408, безусловно, очень важен и для российских разработчиков.

В разд. 4.3 рассматривается отечественный ГОСТ Р ИСО/МЭК 15408—2002, являющийся аналогом стандарта ISO 15408.

4.2.4. Стандарты для беспроводных сетей

Стандарт IEEE 802.11. В 1990 г. Комитет IEEE 802 сформировал рабочую группу 802.11 для разработки стандарта для беспроводных локальных сетей. Работы по созданию стандарта были завершены через 7 лет. В 1997 г. была ратифицирована первая спецификация беспроводного стандарта IEEE 802.11, обеспечивающего передачу данных с гарантированной скоростью 1 Мб/с (в некоторых случаях до 2 Мб/с) в полосе частот 2,4 ГГц. Эта полоса частот доступна для нелицензионного использования в большинстве стран мира.

Стандарт IEEE 802.11 является базовым стандартом и определяет протоколы, необходимые для организации беспроводных локальных сетей WLAN (Wireless Local Area Network). Основные из них — протокол управления доступом к среде MAC (Medium Accsess Control — нижний подуровень канального уровня) и протокол PHY передачи сигналов в физической среде. В качестве физической среды допускается использование радиоволн и инфракрасного излучения.

В основу стандарта IEEE 802.11 положена сотовая архитектура, причем сеть может состоять как из одной, так и нескольких ячеек. Каждая из них управляется базовой станцией, называемой *точкой доступа AP* (Access Point), которая вместе с находящимися в пределах радиуса ее действия рабочими станциями пользователей образует *базовую зону обслуживания BSS* (Basic Service Set). Точки доступа многосотовой сети взаимодействуют между собой через *распределительную систему DS* (Distribution System), представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему образует *расширенную зону обслуживания ESS* (Extended Service Set). Стандартом предусмотрен также односотовый вариант беспроводной сети, который может быть реализован и без точки доступа, при этом часть ее функций выполняются непосредственно рабочими станциями.

Для обеспечения перехода мобильных рабочих станций из зоны действия одной точки доступа к другой в многосотовых

системах предусмотрены специальные процедуры сканирования (активного и пассивного прослушивания эфира) и присоединения (Association), однако строгих спецификаций по реализации роуминга стандарт IEEE 802.11 не предусматривает.

Для защиты WLAN стандартом IEEE 802.11 предусмотрен алгоритм WEP (Wired Equivalent Privacy). Он включает средства противодействия НСД к сети, а также шифрование для предотвращения перехвата информации.

Однако заложенная в первую спецификацию стандарта IEEE 802.11 скорость передачи данных в беспроводной сети перестала удовлетворять потребностям пользователей: алгоритм WEP имел ряд существенных недостатков — отсутствие управления ключом, использование общего статического ключа, малые разрядности ключа и вектора инициализации, сложности использования алгоритма RC4.

Чтобы сделать технологию Wireless LAN недорогой, популярной и удовлетворяющей жестким требованиям бизнес-приложений, разработчики создали семейство новых спецификаций стандарта IEEE 802.11 — a, b, ..., i. Стандарты этого семейства, по сути, являются беспроводными расширениями протокола Ethernet, что обеспечивает хорошее взаимодействие с проводными сетями Ethernet.

Стандарт IEEE 802.11b был ратифицирован IEEE в сентябре 1999 г. как развитие базового стандарта 802.11; в нем используется полоса частот 2,4 ГГц, скорость передачи достигает 11 Мб/с (подобно Ethernet). Благодаря ориентации на освоенный диапазон 2,4 ГГц стандарт 802.11b завоевал большую популярность у производителей оборудования. В качестве базовой радиотехнологии в нем используется метод распределенного спектра с прямой последовательностью DSSS (Direct Sequence Spread Spectrum), который отличается высокой устойчивостью к искажению данных помехами, в том числе преднамеренными. Этот стандарт получил широкое распространение, и беспроводные LAN стали привлекательным решением с технической и финансовой точки зрения.

Стандарт IEEE 802.11a предназначен для работы в частотном диапазоне 5 ГГц. Скорость передачи данных до 54 Мбит/с, т. е. примерно в 5 раз быстрее сетей 802.11b. Ассоциация WECA называет этот стандарт Wi-Fi5. Это наиболее широкополосный стандарт из семейства стандартов 802.11. Определены три обязательные скорости — 6, 12 и 24 Мбит/с и пять необязательных — 9, 18, 36, 48 и 54 Мбит/с. В качестве метода модуляции сигнала

принято ортогональное частотное мультиплексирование OFDM (Orthogonal Frequency Division Multiplexing). Его отличие от метода DSSS заключается в том, что OFDM предполагает параллельную передачу полезного сигнала одновременно по нескольким частотам диапазона, в то время как технологии расширения спектра DSSS передают сигналы последовательно. В результате повышается пропускная способность канала и качество сигнала. К недостаткам стандарта 802.11a относится большая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия (около 100 м).

Для простоты запоминания в качестве общего имени для стандартов 802.11b и 802.11a, а также всех последующих, относящихся к беспроводным локальным сетям (WLAN), Ассоциацией беспроводной совместимости с Ethernet WECA (Wireless Ethernet Compatibility Aliance) был введен термин Wi-Fi (Wireless Fidelity). Если устройство помечено этим знаком, оно протестировано на совместимость с другими устройствами 802.11.

Стандарт IEEE 802.11g представляет собой развитие 802.11b и обратно совместим с 802.11b; предназначен для обеспечения скоростей передачи данных до 54 Мбит/с. В числе достоинств 802.11g надо отметить низкую потребляемую мощность, большие расстояния (до 300 м) и высокую проникающую способность сигнала.

Стандарт IEEE 802.11i — стандарт обеспечения безопасности в беспроводных сетях; ратифицирован IEEE в 2004 г. Этот стандарт решил существовавшие проблемы в области аутентификации и протокола шифрования, обеспечив значительно более высокий уровень безопасности. Стандарт 802.11i может применяться в сетях Wi-Fi, независимо от используемого стандарта — 802.11a, b или g.

Существуют два очень похожих стандарта — WPA и 802.11i. WPA был разработан в Wi-Fi Alliance как решение, которое можно применить немедленно, не дожидаясь завершения длительной процедуры ратификации 802.11i в IEEE. Оба стандарта используют механизм 802.1x (см. далее) для обеспечения надежной аутентификации, оба используют сильные алгоритмы шифрования и предназначены для замены протокола WEP.

Их основное отличие заключается в использовании различных механизмов шифрования. В WPA применяется протокол TKIP (Temporal Key Integrity Protocol), который, также как и WEP, использует шифр RC4, но значительно более безопасным способом. Обеспечение конфиденциальности данных в стандарте IEEE 802.11i основано на использовании алгоритма шифрова-

ния AES (Advanced Encryption Standard). Использующий его защитный протокол получил название CCMP (Counter-Mode CBC MAC Protocol). Алгоритм AES обладает высокой криптостойкостью. Длина ключа AES равна 128, 192 или 256 бит, что обеспечивает наиболее надежное шифрование из доступных сейчас.

Стандарт 802.11i предполагает наличие трех участников процесса аутентификации. Это сервер аутентификации AS (Authentication Server), точка доступа AP (Access Point) и рабочая станция STA (Station). В процессе шифрования данных участвуют только AP и STA (AS не используется). Стандарт предусматривает двустороннюю аутентификацию (в отличие от WEP, где аутентифицируется только рабочая станция, но не точка доступа). При этом местами принятия решения о разрешении доступа являются сервер аутентификации AS и рабочая станция STA, а местами исполнения этого решения — точка доступа AP и STA.

Для работы по стандарту 802.11i создается иерархия ключей, содержащая мастер-ключ MK (Master Key), парный мастер-ключ PMK (Pairwise Master Key), парный временный ключ PTK (Pairwise Transient Key), а также групповые временные ключи GTK (Group Transient Key), служащие для защиты широковещательного сетевого трафика.

MK — это симметричный ключ, реализующий решение STA и AS о взаимной аутентификации. Для каждой сессии создается новый MK.

PMK — обновляемый симметричный ключ, владение которым означает разрешение (авторизацию) на доступ к среде передачи данных в течение данной сессии. PMK создается на основе MK. Для каждой пары STA и AP в каждой сессии создается новый PMK.

PTK — это коллекция операционных ключей, которые используются для привязки PMK к данным STA и AP, распространения GTK и шифрования данных.

Процесс аутентификации и доставки ключей определяется стандартом 802.1x. Он предоставляет возможность использовать в беспроводных сетях такие традиционные серверы аутентификации, как RADIUS (Remote Authentication Dial-In User Server). Стандарт 802.11i не определяет тип сервера аутентификации, но использование RADIUS для этой цели является стандартным решением.

Транспортом для сообщений 802.1x служит протокол EAP (Extensible Authentication Protocol). EAP позволяет легко добавлять

новые методы аутентификации. Точке доступа не требуется знать об используемом методе аутентификации, поэтому изменение метода никак не затрагивает точку доступа. Наиболее популярные методы EAP — это LEAP, PEAP, TTLS и FAST. Каждый из методов имеет свои сильные и слабые стороны, условия применения, по-разному поддерживается производителями оборудования и ПО.

Выделяют пять фаз работы 802.11i.

Первая фаза — обнаружение. В этой фазе рабочая станция STA находит точку доступа AP, с которой может установить связь и получает от нее используемые в данной сети параметры безопасности. Таким образом STA узнает идентификатор сети SSID и методы аутентификации, доступные в данной сети. Затем STA выбирает метод аутентификации, и между STA и AP устанавливается соединение. После этого STA и AP готовы к началу второй фазы 802.1x.

Вторая фаза — аутентификация. В этой фазе выполняется взаимная аутентификация STA и сервера AS, создаются MK и PMK. В данной фазе STA и AP блокируют весь трафик, кроме трафика 802.1x.

Третья фаза — AS перемещает ключ PMK на AP. Теперь STA и AP владеют действительными ключами PMK.

Четвертая фаза — управление ключами 802.1x. В этой фазе происходит генерация, привязка и верификация ключа PTK.

Пятая фаза — шифрование и передача данных. Для шифрования используется соответствующая часть PTK.

Стандартом 802.11i предусмотрен режим PSK (Pre-Shared Key), который позволяет обойтись без сервера аутентификации AS. При использовании этого режима на STA и на AP вручную вводится Pre-Shared Key, который используется в качестве PMK. Дальше генерация PTK происходит описанным выше порядком. Режим PSK может использоваться в небольших сетях, где нецелесообразно устанавливать AS.

4.2.5. Стандарты информационной безопасности в Интернете

По оценке Комитета ООН по предупреждению преступности и борьбе с ней, компьютерная преступность вышла на уровень одной из международных проблем. Поэтому чрезвычайно важно добиваться эффективного решения проблем обеспечения безо-

пасности коммерческой информации в глобальной сети Интернет и смежных Интранет-сетях, которые по своей технической сущности не имеют принципиальных отличий и различаются в основном масштабами и открытостью.

Рассмотрим особенности стандартизации процесса обеспечения безопасности коммерческой информации в сетях с протоколом передачи данных IP/TCP и с акцентом на защиту телекоммуникаций [90].

Обеспечение безопасности ИТ особенно актуально для открытых систем коммерческого применения, обрабатывающих информацию ограниченного доступа, не содержащую государственную тайну. Под *открытыми системами* понимают совокупности всевозможного вычислительного и телекоммуникационного оборудования разного производства, совместное функционирование которого обеспечивается соответствием требованиям международных стандартов.

Термин «открытые системы» подразумевает также, что если вычислительная система соответствует стандартам, то она будет открыта для взаимосвязи с любой другой системой, которая соответствует тем же стандартам. Это, в частности, относится и к механизмам криптографической защиты информации или к защите от НСД к информации.

Важная заслуга Интернета состоит в том, что он заставил по-новому взглянуть на такие технологии. Во-первых, Интернет поощряет применение открытых стандартов, доступных для внедрения всем, кто проявит к ним интерес. Во-вторых, он представляет собой крупнейшую в мире, и вероятно, единственную, сеть, к которой подключается такое множество разных компьютеров. И наконец, Интернет становится общепринятым средством представления быстроменяющейся новой продукции и новых технологий на мировом рынке.

В Интернете уже давно существует ряд комитетов, в основном из организаций-добровольцев, которые осторожно проводят предлагаемые технологии через процесс стандартизации. Эти комитеты, составляющие основную часть Рабочей группы инженеров Интернета IETF (Internet Engineering Task Force) провели стандартизацию нескольких важных протоколов, ускоряя их внедрение в Интернете. Непосредственными результатами усилий IETF являются такие протоколы, как семейство TCP/IP для передачи данных, SMTP (Simple Mail Transport Protocol) и POP

(Post Office Protocol) для электронной почты, а также SNMP (Simple Network Management Protocol) для управления сетью.

В Интернете популярны протоколы безопасной передачи данных, а именно SSL, SET, IPSec. Перечисленные протоколы появились в Интернете сравнительно недавно как необходимость защиты ценной информации и сразу стали стандартами де-факто.

Протокол SSL (Secure Socket Layer) — популярный сетевой протокол с шифрованием данных для безопасной передачи по сети. Он позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи. Протокол SSL обеспечивает защиту данных между сервисными протоколами (такими как HTTP, FTP и др.) и транспортными протоколами (TCP/IP) с помощью современной криптографии. Протокол SSL подробно рассмотрен в главе 11.

Протокол SET (Security Electronics Transaction) — перспективный стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через сеть Интернет. Протокол SET основан на использовании цифровых сертификатов по стандарту X.509.

Протокол выполнения защищенных транзакций SET является стандартом, разработанным компаниями MasterCard и Visa при значительном участии IBM, GlobeSet и других партнеров. Он позволяет покупателям приобретать товары через Интернет, используя защищенный механизм выполнения платежей.

SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей с использованием пластиковых карточек в Интернете. SET обеспечивает кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты, а также целостность и секретность сообщения, шифрование ценных и уязвимых данных. Поэтому SET более правильно можно назвать стандартной технологией или системой протоколов выполнения безопасных платежей с использованием пластиковых карт через Интернет. SET позволяет потребителям и продавцам подтверждать подлинность всех участников сделки, происходящей в Интернете, с помощью криптографии, в том числе применяя цифровые сертификаты.

Как упоминалось ранее, базовыми задачами защиты информации являются обеспечение ее доступности, конфиденциальности, целостности и юридической значимости. SET, в отличии от других протоколов, позволяет решать указанные задачи защиты информации в целом.

В частности, он обеспечивает следующие специальные требования защиты операций электронной коммерции:

- секретность данных оплаты и конфиденциальность информации заказа, переданной наряду с данными об оплате;
- сохранение целостности данных платежей. Целостность информации платежей обеспечивается с помощью цифровой подписи;
- специальную криптографию с открытым ключом для проведения аутентификации;
- аутентификацию держателя по кредитной карточке. Она обеспечивается применением цифровой подписи и сертификатов держателя карт;
- аутентификацию продавца и его возможности принимать платежи по пластиковым карточкам с применением цифровой подписи и сертификатов продавца;
- аутентификацию того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым карточкам через связь с процессинговой карточной системой. Аутентификация банка продавца обеспечивается использованием цифровой подписи и сертификатов банка продавца;
- готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;
- безопасность передачи данных посредством преимущественного использования криптографии.

Основное преимущество SET по сравнению с другими существующими системами обеспечения информационной безопасности заключается в использовании цифровых сертификатов (стандарт X509, версия 3), которые ассоциируют держателя карты, продавца и банк продавца с банковскими учреждениями платежных систем Visa и Mastercard. Кроме того, SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами и интегрируется с существующими системами.

Протокол IPSec. Спецификация IPSec входит в стандарт IP v.6 и является дополнительной по отношению к текущей версии протоколов TCP/IP. Она разработана Рабочей группой IP Security IETF. В настоящее время IPSec включает 3 алгоритмо-независимых базовых спецификации, представляющих соответствующие RFC-стандарты. Протокол IPSec обеспечивает стандартный способ шифрования трафика на сетевом (третьем) уровне IP и защи-

щает информацию на основе сквозного шифрования: независимо от работающего приложения при этом шифруется каждый пакет данных, проходящий по каналу. Это позволяет организациям создавать в Интернете виртуальные частные сети. Протокол IPSec подробно рассмотрен в гл. 12.

Инфраструктура управления открытыми ключами PKI (Public Key Infrastructure) предназначена для защищенного управления криптографическими ключами электронного документооборота, основанного на применении криптографии с открытыми ключами. Эта инфраструктура подразумевает использование цифровых сертификатов, удовлетворяющих рекомендациям международного стандарта X.509 и развернутой сети центров сертификации, обеспечивающих выдачу и сопровождение цифровых сертификатов для всех участников электронного обмена документами. Инфраструктура PKI подробно рассматривается в гл. 13.

4.3. Отечественные стандарты безопасности информационных технологий

Исторически сложилось так, что в России проблемы безопасности ИТ изучались и своевременно решались в основном в сфере охраны государственной тайны. Аналогичные задачи коммерческого сектора экономики долгое время не находили соответствующих решений.

Информация, содержащаяся в системах или продуктах ИТ, является критическим ресурсом, позволяющим организациям успешно решать свои задачи. Кроме того, частные лица вправе ожидать, что их персональная информация, будучи размещенной в продуктах или системах ИТ, останется приватной, доступной им по мере необходимости и не сможет быть подвергнута несанкционированной модификации.

Проблема защиты информации в коммерческой АС имеет свои особенности, которые необходимо учитывать, поскольку они оказывают серьезное влияние на информационную безопасность (ИБ). Перечислим основные из них.

Приоритет экономических факторов. Для коммерческой АС важно снизить либо исключить финансовые потери и обеспечить получение прибыли владельцем и пользователями данного инструментария в условиях реальных рисков. Важным условием

при этом, в частности, является минимизация типично банковских рисков (например потерь за счет ошибочных направлений платежей, фальсификации платежных документов и т. п.).

Открытость проектирования, предусматривающая создание подсистемы защиты информации из средств, широко доступных на рынке и работающих в открытых системах.

Юридическая значимость коммерческой информации, которую можно определить как свойство безопасной информации, позволяющее обеспечить юридическую силу электронным документам или информационным процессам в соответствии с законодательством Российской Федерации.

Среди различных стандартов по безопасности ИТ, существующих в настоящее время в России, следует выделить нормативные документы по критериям оценки защищенности средств вычислительной техники и АС и документы, регулирующие информационную безопасность (табл. 4.1, строки 1—10). К ним можно добавить нормативные документы по криптографической защите систем обработки информации и информационных технологий (табл. 4.1, строки 11—13).

Таблица 4.1. **Российские стандарты, регулирующие информационную безопасность**

№ п/п	Стандарт	Наименование
1	ГОСТ Р ИСО/МЭК 15408-1—2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
2	ГОСТ Р ИСО/МЭК 15408-2—2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
3	ГОСТ Р ИСО/МЭК 15408-3—2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
4	ГОСТ Р 50739—95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

Окончание табл. 4.1

№ п/п	Стандарт	Наименование
5	ГОСТ Р 50922—96	Защита информации. Основные термины и определения
6	ГОСТ Р 51188—98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство
7	ГОСТ Р 51275—99	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
8	ГОСТ Р ИСО 7498-1—99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель
9	ГОСТ Р ИСО 7498-2—99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации
10	ГОСТ Р 50739—95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
11	ГОСТ 28147—89	Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
12	ГОСТ Р 34.10—2001	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
13	ГОСТ Р 34.11—94	Информационная технология. Криптографическая защита информации. Функция хэширования

Стандарты в структуре ИБ выступают как связующее звено между технической и концептуальной стороной вопроса.

Введение в 1999 г. Международного стандарта ISO 15408 в области обеспечения ИБ имело большое значение как для разработчиков компьютерных ИС, так и для их пользователей. Стан-

дарт ISO 15408—2002 стал своего рода гарантией качества и надежности сертифицированных по нему программных продуктов. Этот стандарт позволил потребителям лучше ориентироваться при выборе ПО и приобретать продукты, соответствующие их требованиям безопасности, и, как следствие этого, повысил конкурентоспособность IT-компаний, сертифицирующих свою продукцию в соответствии с ISO 15408.

ГОСТ Р ИСО/МЭК 15408—2002 «Критерии оценки безопасности информационных технологий» действует в России с января 2004 г. и является аналогом стандарта ISO 15408. ГОСТ Р ИСО/МЭК 15408, называемый также «Общими критериями» (ОК), является на сегодня самым полным стандартом, определяющим инструменты оценки безопасности ИС и порядок их использования [18, 19, 20].

ОК направлены на защиту информации от несанкционированного раскрытия, модификации, полной или частичной потери и применимы к защитным мерам, реализуемым аппаратными, программно-аппаратными и программными средствами.

ОК предназначены служить основой при оценке характеристик безопасности продуктов и систем ИТ. Заложенные в стандарте наборы требований позволяют сравнивать результаты независимых оценок безопасности. На основании этих результатов потребитель может принимать решение о том, достаточно ли безопасны ИТ-продукты или системы для их применения с заданным уровнем риска.

ГОСТ Р ИСО/МЭК 15408—2002 состоит из трех частей.

Часть 1 (ГОСТ Р ИСО/МЭК 15408-1 «Введение и общая модель») устанавливает общий подход к формированию требований безопасности и оценке безопасности. На их основе разрабатываются основные конструкции (профиль защиты и задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки (ОО) по методологии ОК определяются, исходя из целей безопасности, которые основываются на анализе назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

Часть 2 (ГОСТ Р ИСО/МЭК 15408-2 «Функциональные требования безопасности») содержит универсальный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Часть 3 (ГОСТ Р ИСО/МЭК 15408-3 «Требования доверия к безопасности») включает систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. Здесь же содержатся оценочные уровни доверия (ОУД), определяющие шкалу требований, которые позволяют с возрастающей степенью полноты и строгости оценить проектную, тестовую и эксплуатационную документацию, правильность реализации функций безопасности ОО, уязвимости продукта или системы ИТ, стойкость механизмов защиты и сделать заключение об уровне доверия к безопасности объекта оценки.

Обобщая вышесказанное, можно отметить, что каркас безопасности, заложенный частью 1 ГОСТ Р ИСО/МЭК 15408, заполняется содержимым из классов, семейств и компонентов части 2, а часть 3 определяет, как оценить прочность всего «строения».

Стандарт «Критерии оценки безопасности информационных технологий» отражает достижения последних лет в области ИБ. Впервые документ такого уровня содержит разделы, адресованные потребителям, производителям и экспертам по оценке безопасности ИТ-продуктов.

Главные достоинства ГОСТ Р ИСО/МЭК 15408:

- полнота требований к ИБ;
- гибкость в применении;
- открытость для последующего развития с учетом новейших достижений науки и техники.

Часть 2
ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ

Безопасность данных означает их конфиденциальность, целостность и подлинность. Критерии безопасности данных могут быть определены следующим образом.

Конфиденциальность данных предполагает их доступность только для тех лиц, которые имеют на это соответствующие полномочия. Под *обеспечением конфиденциальности* информации понимается создание таких условий, при которых понять содержание передаваемых данных может только законный получатель, которому данная информация предназначена.

Целостность информации предполагает ее неизменность в процессе передачи от отправителя к получателю. Под *обеспечением целостности* информации понимается достижение идентичности отправляемых и принимаемых данных.

Подлинность информации предполагает соответствие этой информации ее явному описанию и содержанию, в частности, соответствие действительным характеристикам указанных: отправителя, времени отправления и содержания. *Обеспечение подлинности* информации, реализуемое на основе аутентификации, состоит в достоверном установлении отправителя, а также защите информации от изменения при ее передаче от отправителя к получателю.

Своевременно обнаруженное нарушение подлинности и целостности полученного сообщения позволяет предотвратить отрицательные последствия, связанные с дальнейшим использованием такого искаженного сообщения.

Глава 5
ПРИНЦИПЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Основные понятия криптографической защиты информации

Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Исторически криптография (в переводе с греческого этот термин означает «тайнопись») зародилась как способ скрытой передачи сообщений. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей. Такие преобразования обеспечивают решение трех главных проблем защиты данных: обеспечение конфиденциальности, целостности и подлинности передаваемых или сохраняемых данных.

Для обеспечения безопасности данных необходимо поддерживать три основные функции:

- защиту конфиденциальности передаваемых или хранимых в памяти данных;
- подтверждение целостности и подлинности данных;
- аутентификацию абонентов при входе в систему и при установлении соединения;

Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации.

Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а так-

же путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т. п.

Целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования.

Аутентификация разрешает устанавливать соединения только между легальными пользователями и предотвращает доступ к средствам сети нежелательных лиц. Абонентам, доказавшим свою легальность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

Обеспечение конфиденциальности, целостности и подлинности передаваемых и сохраняемых данных осуществляется прежде всего правильным использованием криптографических способов и средств защиты информации. Основой большинства криптографических средств защиты информации является *шифрование данных.*

Под *шифром* понимают совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования. Под *зашифровыванием информации* понимается процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют *расшифровыванием* (дешифрованием).

Обобщенная схема криптосистемы шифрования показана на рис. 5.1. Исходный текст передаваемого сообщения (или хранимой информации) M зашифровывается с помощью криптографического преобразования E_{k_1} с получением в результате *шифртекста* C:

$$C = E_{k_1}(M),$$

где k_1 — параметр функции E, называемый *ключом шифрования.*

Шифртекст C, называемый также *криптограммой*, содержит исходную информацию M в полном объеме, однако последовательность знаков в нем внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования k_1.

Ключ шифрования является тем элементом, с помощью которого можно варьировать результат криптографического преобра-

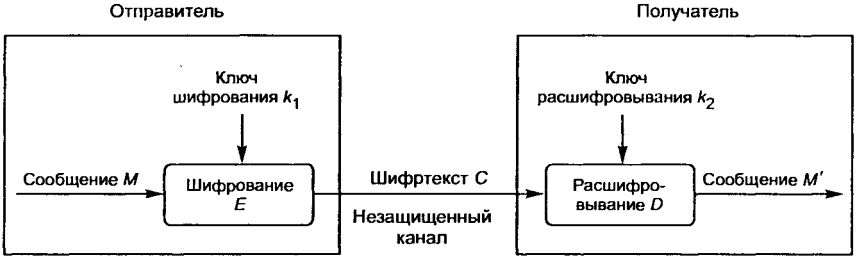


Рис. 5.1. Обобщенная схема криптосистемы шифрования

зования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (или владельцами).

Обратное преобразование информации выглядит следующим образом:

$$M' = D_{k_2}(C).$$

Функция D является обратной к функции E и производит расшифровывание шифртекста. Она также имеет дополнительный параметр в виде ключа k_2. Ключ расшифровывания k_2 должен однозначно соответствовать ключу k_1, в этом случае полученное в результате расшифровывания сообщение M' будет эквивалентно M. При отсутствии верного ключа k_2 получить исходное сообщение $M' = M$ с помощью функции D невозможно.

Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифровывания. Соответственно различают два класса криптосистем:

- симметричные криптосистемы (с единым ключом);
- асимметричные криптосистемы (с двумя ключами).

5.2. Симметричные криптосистемы шифрования

Исторически первыми появились симметричные криптографические системы. В *симметричной криптосистеме шифрования* используется один и тот же ключ для зашифровывания и расшифровывания информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение.

Соответственно с целью предотвращения несанкционированного раскрытия зашифрованной информации все ключи шифрования в симметричных криптосистемах должны держаться в секрете. Именно поэтому симметричные криптосистемы называют *криптосистемами с секретным ключом* — ключ шифрования должен быть доступен только тем, кому предназначено сообщение. Симметричные криптосистемы называют еще *одноключевыми криптографическими системами*, или *криптосистемами с закрытым ключом*. Схема симметричной криптосистемы шифрования показана на рис. 5.2.

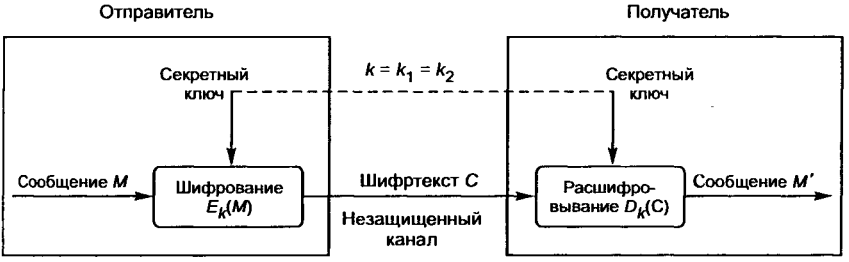


Рис. 5.2. Схема симметричной криптосистемы шифрования

Данные криптосистемы характеризуются наиболее высокой скоростью шифрования, и с их помощью обеспечиваются как конфиденциальность и подлинность, так и целостность передаваемой информации [31]. Конфиденциальность передачи информации с помощью симметричной криптосистемы зависит от надежности шифра и обеспечения конфиденциальности ключа шифрования.

Обычно ключ шифрования представляет собой файл или массив данных и хранится на персональном ключевом носителе, например дискете или смарт-карте; обязательно принятие мер, обеспечивающих недоступность персонального ключевого носителя кому-либо, кроме его владельца.

Подлинность обеспечивается за счет того, что без предварительного расшифровывания практически невозможно осуществить смысловую модификацию и подлог криптографически закрытого сообщения. Фальшивое сообщение не может быть правильно зашифровано без знания секретного ключа.

Целостность данных обеспечивается присоединением к передаваемым данным специального кода (имитовставки), выраба-

тываемой по секретному ключу. Имитовставка является разновидностью контрольной суммы, т. е. некоторой эталонной характеристикой сообщения, по которой осуществляется проверка целостности последнего. Алгоритм формирования имитовставки должен обеспечивать ее зависимость по некоторому сложному криптографическому закону от каждого бита сообщения. Проверка целостности сообщения выполняется получателем сообщения путем выработки по секретному ключу имитовставки, соответствующей полученному сообщению, и ее сравнения с полученным значением имитовставки. При совпадении делается вывод о том, что информация не была модифицирована на пути от отправителя к получателю.

Симметричное шифрование идеально подходит для шифрования информации «для себя», например, с целью предотвращения НСД к ней в отсутствие владельца. Это может быть как архивное шифрование выбранных файлов, так и прозрачное (автоматическое) шифрование целых логических или физических дисков.

Обладая высокой скоростью шифрования, одноключевые криптосистемы позволяют решать многие важные задачи защиты информации. Однако автономное использование симметричных криптосистем в компьютерных сетях порождает проблему распределения ключей шифрования между пользователями.

Перед началом обмена зашифрованными данными необходимо обменяться секретными ключами со всеми адресатами. Передача секретного ключа симметричной криптосистемы не может быть осуществлена по общедоступным каналам связи, секретный ключ надо передавать отправителю и получателю по защищенному каналу. Для обеспечения эффективной защиты циркулирующих в сети сообщений необходимо огромное число часто меняющихся ключей (один ключ на каждую пару пользователей). При передаче ключей пользователям необходимо обеспечить конфиденциальность, подлинность и целостность ключей шифрования, что требует больших дополнительных затрат. Эти затраты связаны с необходимостью передачи секретных ключей по закрытым каналам связи или распределением таких ключей с помощью специальной службы доставки, например с помощью курьеров.

Проблема распределения секретных ключей при большом числе пользователей является весьма трудоемкой и сложной задачей. В сети на N пользователей необходимо распределить $N(N-1)/2$ секретных ключей, т. е. число распределяемых сек-

ретных ключей растет по квадратичному закону с увеличением числа абонентов сети.

В разд. 5.6 рассматриваются методы, обеспечивающие защищенное распределение ключей абонентам сети.

5.3. Асимметричные криптосистемы шифрования

Асимметричные криптографические системы были разработаны в 1970-х гг. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифровывания используются различные ключи:

- *открытый ключ* K используется для шифрования информации, вычисляется из секретного ключа k;
- *секретный ключ* k используется для расшифровывания информации, зашифрованной с помощью парного ему открытого ключа K.

Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ k из открытого ключа K. Поэтому открытый ключ K может свободно передаваться по каналам связи.

Асимметричные системы называют также *двухключевыми криптографическими системами*, или *криптосистемами с открытым ключом.*

Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом показана на рис. 5.3.

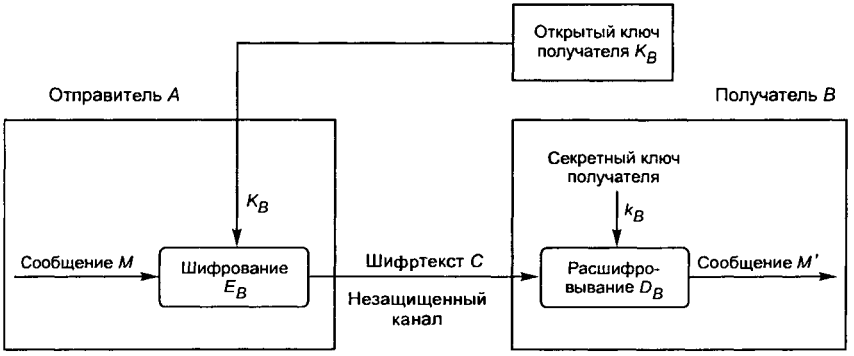


Рис. 5.3. Обобщенная схема асимметричной криптосистемы шифрования

Для криптографического закрытия и последующего расшифровывания передаваемой информации используются открытый и секретный ключи получателя B сообщения.

В качестве ключа зашифровывания должен использоваться открытый ключ получателя, а в качестве ключа расшифровывания — его секретный ключ.

Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у его владельца и быть надежно защищен от НСД (аналогично ключу шифрования в симметричных алгоритмах). Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа.

Процесс передачи зашифрованной информации в асимметричной криптосистеме осуществляется следующим образом.

Подготовительный этап:

- абонент B генерирует пару ключей: секретный ключ k_B и открытый ключ K_B;
- открытый ключ K_B посылается абоненту A и остальным абонентам (или делается доступным, например на разделяемом ресурсе).

Использование — обмен информацией между абонентами A и B:

- абонент A зашифровывает сообщение с помощью открытого ключа K_B абонента B и отправляет шифртекст абоненту B;
- абонент B расшифровывает сообщение с помощью своего секретного ключа k_B. Никто другой (в том числе абонент A) не может расшифровать данное сообщение, так как не имеет секретного ключа абонента B. Защита информации в асимметричной криптосистеме основана на секретности ключа k_B получателя сообщения.

Характерные особенности асимметричных криптосистем:

- открытый ключ K_B и криптограмма C могут быть отправлены по незащищенным каналам, т. е. противнику известны K_B и C;
- алгоритмы шифрования и расшифровывания:

$$E_B : M \to C;$$

$$D_B : C \to M$$

являются открытыми.

У. Диффи и М. Хеллман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы [28].

1. Вычисление пары ключей (K_B, k_B) получателем B должно быть простым.

2. Отправитель A, зная открытый ключ K_B и сообщение M, может легко вычислить криптограмму

$$C = E_{K_B}(M).$$

3. Получатель B, используя секретный ключ k_B и криптограмму C, может легко восстановить исходное сообщение

$$M = D_{k_B}(C).$$

4. Противник, зная открытый ключ K_B, при попытке вычислить секретный ключ k_B наталкивается на непреодолимую вычислительную проблему.

5. Противник, зная пару (K_B, C), при попытке вычислить исходное сообщение M наталкивается на непреодолимую вычислительную проблему.

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных функций. *Однонаправленной функцией* называется функция $F(X)$, обладающая двумя свойствами:

- существует алгоритм вычисления значений функции $Y = F(X)$;
- не существует эффективного алгоритма обращения (инвертирования) функции F (т. е. не существует решения уравнения $F(X) = Y$ относительно X).

В качестве примера однонаправленной функции можно указать *целочисленное умножение*. Прямая задача — вычисление произведения двух очень больших целых чисел P и Q, т. е. нахождение значения $N = P \cdot Q$ — относительно несложная задача для компьютера.

Обратная задача — факторизация, или разложение на множители большого целого числа, т. е. нахождение делителей P и Q большого целого числа $N = P \cdot Q$, — является практически неразрешимой при достаточно больших значениях N.

Другой характерный пример однонаправленной функции — это *модульная экспонента с фиксированными основанием и модулем* [62].

Как и в случае симметричных криптографических систем, с помощью асимметричных криптосистем обеспечивается не только конфиденциальность, но также подлинность и целостность передаваемой информации. Подлинность и целостность любого сообщения обеспечивается формированием цифровой подписи этого сообщения и отправкой в зашифрованном виде сообщения вместе с цифровой подписью. Проверка соответствия подписи полученному сообщению после его предварительного расшифровывания представляет собой проверку целостности и подлинности принятого сообщения. Процедуры формирования и проверки электронной цифровой подписи рассмотрены в разд. 5.5.

Преимущества асимметричных криптографических систем перед симметричными криптосистемами:

- в асимметричных криптосистемах решена сложная проблема распределения ключей между пользователями, так как каждый пользователь может сгенерировать свою пару ключей сам, а открытые ключи пользователей могут свободно публиковаться и распространяться по сетевым коммуникациям;
- исчезает квадратичная зависимость числа ключей от числа пользователей; в асимметричной криптосистеме число используемых ключей связано с числом абонентов линейной зависимостью (в системе из N пользователей используются $2N$ ключей), а не квадратичной, как в симметричных системах;
- асимметричные криптосистемы позволяют реализовать протоколы взаимодействия сторон, которые не доверяют друг другу, поскольку при использовании асимметричных криптосистем закрытый ключ должен быть известен только его владельцу.

Недостатки асимметричных криптосистем:

- на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах функций;
- асимметричное шифрование существенно медленнее симметричного, поскольку при шифровании и расшифровке используются весьма ресурсоемкие операции. По этой же причине реализовать аппаратный шифратор с асимметричным алгоритмом существенно сложнее, чем реализовать аппаратно симметричный алгоритм;
- необходимость защиты открытых ключей от подмены.

5.4. Комбинированная криптосистема шифрования

Анализ рассмотренных выше особенностей симметричных и асимметричных криптографических систем показывает, что при совместном использовании они эффективно дополняют друг друга, компенсируя недостатки.

Действительно, главным достоинством асимметричных криптосистем с открытым ключом является их потенциально высокая безопасность: нет необходимости ни передавать, ни сообщать кому-либо значения секретных ключей, ни убеждаться в их подлинности. Однако их быстродействие обычно в сотни (и более) раз меньше быстродействия симметричных криптосистем с секретным ключом.

В свою очередь, быстродействующие симметричные криптосистемы страдают существенным недостатком: обновляемый секретный ключ симметричной криптосистемы должен регулярно передаваться партнерам по информационному обмену и во время этих передач возникает опасность раскрытия секретного ключа.

Совместное использование этих криптосистем позволяет эффективно реализовывать такую базовую функцию защиты, как криптографическое закрытие передаваемой информации с целью обеспечения ее конфиденциальности. Комбинированное применение симметричного и асимметричного шифрования устраняет основные недостатки, присущие обоим методам, и позволяет сочетать преимущества высокой секретности, предоставляемые асимметричными криптосистемами с открытым ключом, с преимуществами высокой скорости работы, присущими симметричным криптосистемам с секретным ключом.

Метод комбинированного использования симметричного и асимметричного шифрования заключается в следующем.

Симметричную криптосистему применяют для шифрования исходного открытого текста, а асимметричную криптосистему с открытым ключом применяют только для шифрования секретного ключа симметричной криптосистемы. В результате асимметричная криптосистема с открытым ключом не заменяет, а лишь дополняет симметричную криптосистему с секретным ключом, позволяя повысить в целом защищенность передаваемой информации. Такой подход иногда называют схемой *электронного «цифрового конверта»*.

Пусть пользователь *A* хочет использовать комбинированный метод шифрования для защищенной передачи сообщения *M* пользователю *B*.

Тогда последовательность действий пользователей *A* и *B* будет следующей.

Действия пользователя *A*:

1. Он создает (например, генерирует случайным образом) сеансовый секретный ключ K_S, который будет использован в алгоритме симметричного шифрования для зашифрования конкретного сообщения или цепочки сообщений.

2. Зашифровывает симметричным алгоритмом сообщение *M* на сеансовом секретном ключе K_S.

3. Зашифровывает асимметричным алгоритмом секретный сеансовый ключ K_S на открытом ключе K_B пользователя *B* (получателя сообщения).

4. Передает по открытому каналу связи в адрес пользователя *B* зашифрованное сообщение *M* вместе с зашифрованным сеансовым ключом K_S.

Действия пользователя *A* иллюстрируются схемой шифрования сообщения комбинированным методом (рис. 5.4).

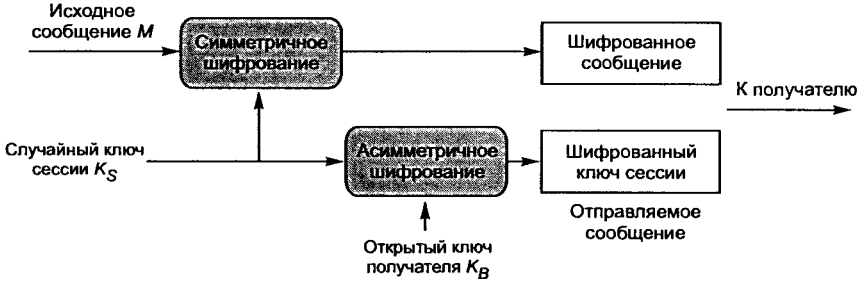


Рис. 5.4. Схема шифрования сообщения комбинированным методом

Действия пользователя *B* (при получении электронного «цифрового конверта» — зашифрованного сообщения *M* и зашифрованного сеансового ключа K_S):

5. Расшифровывает асимметричным алгоритмом сеансовый ключ K_S с помощью своего секретного ключа k_B.

6. Расшифровывает симметричным алгоритмом принятое сообщение *M* с помощью полученного сеансового ключа K_S.

Действия пользователя *B* иллюстрируются схемой расшифровывания сообщения комбинированным методом (рис. 5.5).

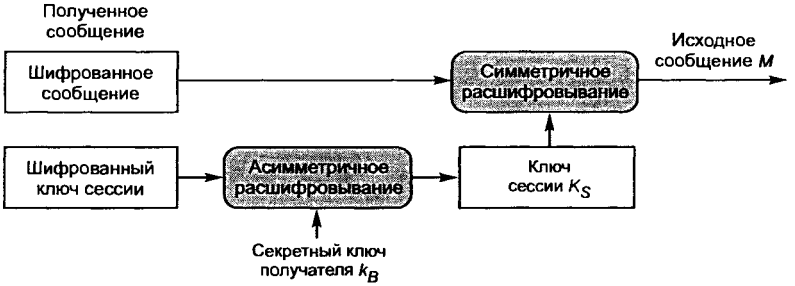


Рис. 5.5. Схема расшифровывания сообщения комбинированным методом

Полученный электронный «цифровой конверт» может раскрыть только законный получатель — пользователь *B*. Только пользователь *B*, владеющий личным секретным ключом k_B сможет правильно расшифровать секретный сеансовый ключ K_S и затем с помощью этого ключа расшифровать и прочитать полученное сообщение *M*.

При методе «цифрового конверта» недостатки симметричного и асимметричного криптоалгоритмов компенсируются следующим образом:

- проблема распространения ключей симметричного криптоалгоритма устраняется тем, что сеансовый ключ K_S, на котором шифруются собственно сообщения, передается по открытым каналам связи в зашифрованном виде; для зашифровывания ключа K_S используется асимметричный криптоалгоритм;
- проблемы медленной скорости асимметричного шифрования в данном случае практически не возникает, поскольку асимметричным криптоалгоритмом шифруется только короткий ключ K_S, а все данные шифруются быстрым симметричным криптоалгоритмом.

В результате получают быстрое шифрование в сочетании с удобным распределением ключей.

Когда требуется реализовать протоколы взаимодействия не доверяющих друг другу сторон, используется следующий способ взаимодействия. Для каждого сообщения на основе случайных параметров генерируется отдельный секретный ключ симметричного шифрования, который и зашифровывается асимметричной системой для передачи вместе с сообщением, зашифрованным этим ключом. В этом случае разглашение ключа симметричного шифрования не будет иметь смысла, так как для зашифровыва-

ния следующего сообщения будет использован другой случайный секретный ключ.

При комбинированном методе шифрования применяются криптографические ключи как симметричных, так и асимметричных криптосистем. Очевидно, выбор длин ключей для криптосистемы каждого типа следует осуществлять таким образом, чтобы злоумышленнику было одинаково трудно атаковать любой механизм защиты комбинированной криптосистемы.

5.5. Электронная цифровая подпись и функция хэширования

Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. При таком обмене существенно снижаются затраты на обработку и хранение документов, убыстряется их поиск. Но возникает проблема аутентификации автора электронного документа и самого документа, т. е. установления подлинности автора и отсутствия изменений в полученном электронном документе.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

- *активный перехват* — нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
- *маскарад* — абонент *C* посылает документ абоненту *B* от имени абонента *A*;
- *ренегатство* — абонент *A* заявляет, что не посылал сообщения абоненту *B*, хотя на самом деле послал;
- *подмена* — абонент *B* изменяет или формирует новый документ и заявляет, что получил его от абонента *A*;
- *повтор* — абонент *C* повторяет ранее переданный документ, который абонент *A* посылал абоненту *B*.

Эти виды злоумышленных действий могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, частным лицам, применяющим в своей деятельности компьютерные ИТ.

Проблему проверки целостности сообщения и подлинности автора сообщения позволяет эффективно решить методология электронной цифровой подписи.

5.5.1. Основные процедуры цифровой подписи

Функционально цифровая подпись аналогична обычной рукописной подписи и обладает ее основными достоинствами:

- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
- гарантирует целостность подписанного текста.

Электронная цифровая подпись (ЭЦП) представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом.

ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности цифровой подписи. ЭЦП реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа.

Система ЭЦП включает две основные процедуры:

- формирования цифровой подписи;
- проверки цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи — открытый ключ отправителя.

Процедура формирования цифровой подписи. На подготовительном этапе этой процедуры абонент A — отправитель сообщения — генерирует пару ключей: секретный ключ k_A и открытый ключ K_A. Открытый ключ K_A вычисляется из парного ему секретного ключа k_A. Открытый ключ K_A рассылается остальным абонентам сети (или делается доступным, например на разделяемом ресурсе) для использования при проверке подписи. Для формирования цифровой подписи отправитель A прежде всего

вычисляет значение хэш-функции $h(M)$ подписываемого текста M (рис. 5.6).

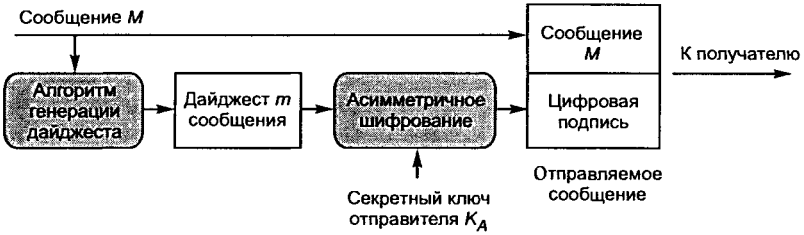


Рис. 5.6. Схема формирования электронной цифровой подписи

Хэш-функция служит для сжатия исходного подписываемого текста M в *дайджест* m — относительно короткое число, состоящее из фиксированного небольшого числа битов и характеризующее весь текст M в целом (см. разд. 5.5.2). Далее отправитель A шифрует дайджест m своим секретным ключом k_A. Получаемая при этом пара чисел представляет собой цифровую подпись для данного текста M. Сообщение M вместе с цифровой подписью отправляется в адрес получателя.

Процедура проверки цифровой подписи. Абоненты сети могут проверить цифровую подпись полученного сообщения M с помощью открытого ключа K_A отправителя этого сообщения (рис. 5.7).

При проверке ЭЦП абонент B — получатель сообщения M — расшифровывает принятый дайджест m открытым ключом K_A отправителя A. Кроме того, получатель сам вычисляет с помощью хэш-функции $h(M)$ дайджест m' принятого сообщения M и сравнивает его с расшифрованным. Если m и m' совпадают, то

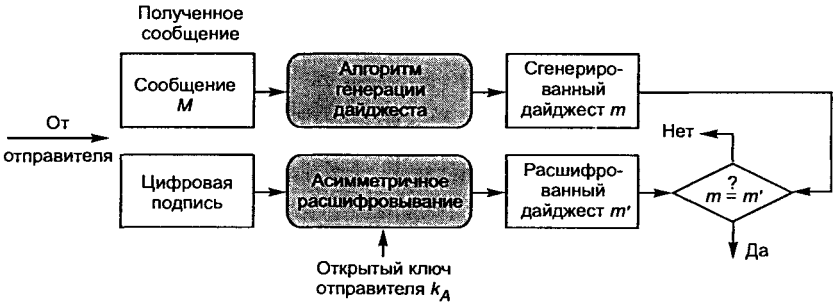


Рис. 5.7. Схема проверки электронной цифровой подписи

цифровая подпись является подлинной. В противном случае либо подпись подделана, либо изменено содержание сообщения.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания. Поэтому необходимо защитить секретный ключ подписывания от НСД. Секретный ключ ЭЦП аналогично ключу симметричного шифрования рекомендуется хранить на персональном ключевом носителе в защищенном виде.

Электронная цифровая подпись представляет собой уникальное число, зависящее от подписываемого документа и секретного ключа абонента. В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей.

Помещаемая в подписываемый файл (или в отдельный файл электронной подписи) структура ЭЦП обычно содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация добавляется к документу до вычисления ЭЦП, что обеспечивает и ее целостность. Каждая подпись содержит следующую информацию:

- дату подписи;
- срок окончания действия ключа данной подписи;
- информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
- идентификатор подписавшего (имя открытого ключа);
- собственно цифровую подпись.

Важно отметить, что с точки зрения конечного пользователя процесс формирования и проверки цифровой подписи отличается от процесса криптографического закрытия передаваемых данных следующими особенностями.

При формировании цифровой подписи используются закрытый ключ отправителя, тогда как при зашифровывании используется открытый ключ получателя. При проверке цифровой подписи используется открытый ключ отправителя, а при расшифровывании — закрытый ключ получателя.

Проверить сформированную подпись может любое лицо, так как ключ проверки подписи является открытым. При положительном результате проверки подписи делается заключение о подлинности и целостности полученного сообщения, т. е. о том, что это сообщение действительно отправлено тем или иным отправителем и не было модифицировано при передаче по сети.

Однако, если пользователя интересует, не является ли полученное сообщение повторением ранее отправленного или не было ли оно задержано на пути следования, то он должен проверить дату и время его отправки, а при наличии — порядковый номер.

Аналогично асимметричному шифрованию, необходимо обеспечить невозможность подмены открытого ключа, используемого для проверки ЭЦП. Открытые ключи ЭЦП можно защитить от подмены с помощью соответствующих цифровых сертификатов (см. гл. 13).

Сегодня существует несколько стандартов ЭЦП, например ГОСТ 34.10—2001.

5.5.2. Функция хэширования

Как видно из схемы на рис. 5.7, в качестве исходного значения для вычисления ЭЦП берется не сам электронный документ, а его хэш-значение, или дайджест.

Хэш-значение $h(M)$ — это *дайджест сообщения* M, т. е. сжатое двоичное представление основного сообщения M произвольной длины. Хэш-значение $h(M)$ формируется функцией хэширования. *Функция хэширования* (*хэш-функция*) представляет собой преобразование, на вход которого подается сообщение переменной длины M, а выходом является строка фиксированной длины $h(M)$. Иначе говоря, хэш-функция $h(\cdot)$ принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение (хэш) $H = h(M)$ фиксированной длины (рис. 5.8).

Рис. 5.8. Схема формирования хэша $H = h(M)$

Функция хэширования позволяет сжать подписываемый документ M до 128 и более бит (в частности до 128 или 256 бит), тогда как M может быть размером в мегабайт или более. Следует отметить, что значение хэш-функции $h(M)$ зависит сложным образом от документа M и не позволяет восстановить сам документ M.

Функция хэширования должна обладать следующими свойствами.

1. Хэш-функция может быть применена к аргументу любого размера.

2. Выходное значение хэш-функции имеет фиксированный размер.

3. Хэш-функцию $h(x)$ достаточно просто вычислить для любого x. Скорость вычисления хэш-функции должна быть такой, чтобы скорость выработки и проверки ЭЦП при использовании хэш-функции была значительно больше, чем при использовании самого сообщения.

4. Хэш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки и т. п.

5. Хэш-функция должна быть однонаправленной, т. е. обладать свойством необратимости, иными словами, задача подбора документа M', который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима.

6. Вероятность того, что значения хэш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала; т. е. для любого фиксированного x с вычислительной точки зрения невозможно найти $x' \neq x$, такое, что $h(x') = h(x)$.

Теоретически возможно, что два различных сообщения могут быть сжаты в одну и ту же свертку (так называемая коллизия, или «столкновение»). Поэтому для обеспечения стойкости функции хэширования необходимо избегать столкновений. Полностью столкновений избежать нельзя, поскольку в общем случае количество возможных сообщений превышает количество возможных выходных значений функции хэширования. Однако вероятность столкновения должна быть низкой.

Свойство 5 эквивалентно тому, что $h(\cdot)$ является односторонней функцией. Свойство 6 гарантирует, что не может быть найдено другое сообщение, дающее ту же свертку. Это предотвращает фальсификацию сообщения.

Таким образом, функция хэширования может использоваться для обнаружения изменений сообщения, т. е. может служить для формирования *криптографической контрольной суммы* (также называемой *кодом обнаружения изменений* или *кодом аутентификации сообщения*). В этом качестве хэш-функция используется для контроля целостности сообщения при формировании и проверке ЭЦП.

Хэш-функции широко используются также для аутентификации пользователей. В ряде технологий информационной безопасности применяется своеобразный прием шифрования — *шифрование с помощью односторонней хэш-функции.* Своеобразие этого шифрования заключается в том, что оно по существу является односторонним, т. е. не сопровождается обратной процедурой — расшифровыванием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования на основе хэш-функции [62, 82].

Известные алгоритмы хэширования:

- отечественный стандарт ГОСТ Р34.11—94 [12]. Вычисляет хэш размером 32 байта;
- MD (Message Digest) — ряд алгоритмов хэширования, наиболее распространенных в мире. Например, алгоритм MD5 [62, 72] применяется в последних версиях Microsoft Windows для преобразования пароля пользователя в 16-байтное число;
- SHA-1 (Secure Hash Algorithm) — это алгоритм вычисления дайджеста сообщений, вырабатывающий 160-битовый *хэш-код* входных данных, широко распространен в мире, используется во многих сетевых протоколах защиты информации.

Хэш-функции широко используются также для аутентификации пользователей.

5.6. Управление криптоключами

Любая криптографическая система основана на использовании криптографических ключей. Под *ключевой информацией* понимают совокупность всех действующих в информационной сети или системе ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации в сети или системе. *Управление ключами* включает реализацию таких функций, как генерация, хранение и распределение ключей. Распределение ключей — самый ответственный процесс в управлении ключами.

При использовании симметричной криптосистемы две вступающие в информационный обмен стороны должны сначала согласовать секретный сессионный ключ, т. е. ключ для шифрова-

ния всех сообщений, передаваемых в процессе обмена. Этот ключ должен быть неизвестен всем остальным и должен периодически обновляться одновременно у отправителя и получателя. Процесс согласования сессионного ключа называют также обменом или распределением ключей.

Асимметричная криптосистема предполагает использование двух ключей — открытого и закрытого (секретного). Открытый ключ можно разглашать, а закрытый — следует хранить в тайне. При обмене сообщениями необходимо пересылать только открытый ключ, обеспечив подлинность пересылаемого открытого ключа.

К распределению ключей предъявляются следующие требования:

- оперативность и точность распределения;
- конфиденциальность и целостность распределяемых ключей.

Для распределения ключей между пользователями компьютерной сети применяются два основных способа [9]:

1) использование одного или нескольких центров распределения ключей;

2) прямой обмен ключами между пользователями сети.

Оба подхода влекут за собой некоторые проблемы. В первом случае центру распределения ключей известно, кому и какие ключи распределены, и это позволяет читать все сообщения, передаваемые по сети. Возможные злоупотребления могут существенно нарушить безопасность сети. Во втором — необходимо надежно удостовериться в подлинности субъектов сети.

Задача распределения ключей сводится к построению такого протокола распределения ключей, который обеспечивает:

- взаимное подтверждение подлинности участников сеанса;
- подтверждение достоверности сеанса;
- использование минимального числа сообщений при обмене ключами.

Характерным примером реализации первого подхода является система аутентификации и распределения ключей Kerberos; она рассмотрена в гл. 13.

Остановимся подробнее на втором подходе.

При использовании для защищенного информационного обмена криптосистемы с симметричным секретным ключом два пользователя, желающие обменяться криптографически защищенной информацией, должны обладать общим секретным клю-

чом. Эти пользователи должны обменяться общим ключом по каналу связи безопасным образом. Если пользователи меняют ключ достаточно часто, то доставка ключа превращается в серьезную проблему.

Для решения этой проблемы возможно:

1) использование асимметричной криптосистемы с открытым ключом для защиты секретного ключа симметричной криптосистемы;

2) использование системы открытого распределения ключей Диффи — Хеллмана.

Реализация первого способа осуществляется в рамках комбинированной криптосистемы с симметричными и асимметричными ключами. При таком подходе симметричная криптосистема применяется для шифрования и передачи исходного открытого текста, а асимметричная криптосистема с открытым ключом применяется для шифрования, передачи и последующего расшифровывания только секретного ключа симметричной криптосистемы.

Второй способ основан на применении алгоритма открытого распределения ключей Диффи — Хеллмана, позволяющего пользователям обмениваться ключами по незащищенным каналам связи.

Метод распределения ключей Диффи — Хеллмана

У. Диффи и М. Хеллман изобрели метод *открытого распределения ключей* в 1976 г. Этот метод позволяет пользователям обмениваться ключами по незащищенным каналам связи. Его безопасность обусловлена трудностью вычисления дискретных логарифмов в конечном поле, в отличие от легкости решения прямой задачи дискретного возведения в степень в том же конечном поле.

Суть метода Диффи — Хеллмана заключается в следующем (рис. 5.9).

Пользователи A и B, участвующие в обмене информации, генерируют независимо друг от друга свои случайные секретные ключи k_A и k_B (ключи k_A и k_B — случайные большие целые числа, которые хранятся пользователями A и B в секрете).

Затем пользователь A вычисляет на основании своего секретного ключа k_A открытый ключ

$$K_A = g^{k_A} \pmod N,$$

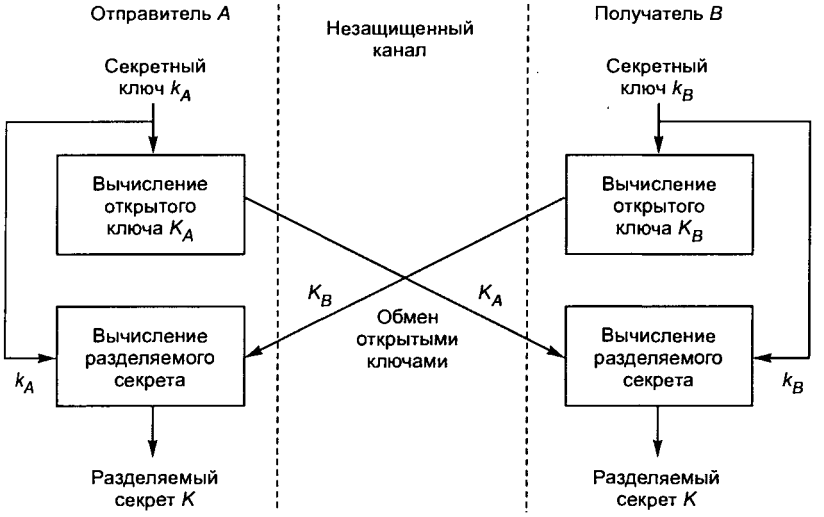


Рис. 5.9. Схема открытого распределения ключей Диффи — Хеллмана

одновременно пользователь B вычисляет на основании своего секретного ключа k_B открытый ключ

$$K_B = g^{k_B} \pmod{N},$$

где N и g — большие целые простые числа. Арифметические действия выполняются с приведением по модулю N [62]. Числа N и g могут не храниться в секрете. Как правило, эти значения являются общими для всех пользователей сети или системы.

Затем пользователи A и B обмениваются своими открытыми ключами K_A и K_B по незащищенному каналу и используют их для вычисления общего сессионного ключа K (разделяемого секрета):

пользователь A: $K = (K_B)^{k_A} \pmod{N} = (g^{k_B})^{k_A} \pmod{N}$;

пользователь B: $K' = (K_A)^{k_B} \pmod{N} = (g^{k_A})^{k_B} \pmod{N}$;

при этом $K = K'$, так как $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} \pmod{N}$.

Таким образом, результатом этих действий оказывается общий сессионный ключ, который является функцией обоих секретных ключей k_A и k_B.

Злоумышленник, перехвативший значения открытых ключей K_A и K_B, не может вычислить сессионный ключ K, потому что он не имеет соответствующих значений секретных ключей k_A и k_B.

Благодаря использованию однонаправленной функции, операция вычисления открытого ключа необратима, т. е. невозможно по значению открытого ключа абонента вычислить его секретный ключ.

Уникальность метода Диффи — Хеллмана заключается в том, что пара абонентов имеет возможность получить известное только им секретное число, передавая по открытой сети открытые ключи. После этого абоненты могут приступить к защите передаваемой информации уже известным проверенным способом — применяя симметричное шифрование с использованием полученного разделяемого секрета.

Схема Диффи — Хеллмана дает возможность шифровать данные при каждом сеансе связи на новых ключах. Это позволяет не хранить секреты на дискетах или других носителях. Не следует забывать, что любое хранение секретов повышает вероятность попадания их в руки конкурентов или противника.

На основе схемы Диффи — Хеллмана функционирует протокол управления криптоключами IKE (Internet Key Exchange), применяемыми при построении защищенных виртуальных сетей VPN на сетевом уровне.

Глава 6
КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования/расшифрования. В соответствии со стандартом шифрования ГОСТ 28147—89 под *шифром* понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования [10]. Существует множество разных криптографических алгоритмов. Назначение этих алгоритмов — защита информации. Защищать же информацию приходится от разных угроз и разными способами. Чтобы обеспечить надежную и адекватную защиту с помощью криптоалгоритма (КА), нужно понимать, какие бывают КА и какой тип алгоритма лучше приспособлен для решения конкретной задачи.

6.1. Классификация криптографических алгоритмов

Известны несколько классификаций криптографических алгоритмов [50]. Одна из них подразделяет КА в зависимости от числа ключей, применяемых в конкретном алгоритме:

- бесключевые КА — не используют в вычислениях никаких ключей;
- одноключевые КА — работают с одним ключевым параметром (секретным ключом);
- двухключевые КА — на различных стадиях работы в них применяются два ключевых параметра: секретный и открытый ключи.

Существуют более детальные классификации, одна из которых приведена на рис. 6.1.

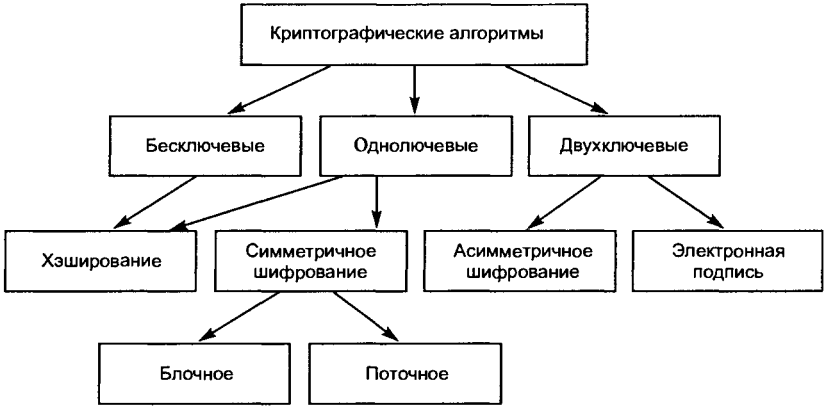


Рис. 6.1. Классификация криптоалгоритмов защиты информации

Охарактеризуем кратко основные типы КА.

Хэширование — это метод криптозащиты, представляющий собой контрольное преобразование информации: из данных неограниченного размера путем выполнения криптографических преобразований вычисляется хэш-значение фиксированной длины, однозначно соответствующее исходным данным.

Симметричное шифрование использует один и тот же ключ как для зашифровывания, так и для расшифровывания информации.

Симметричное шифрование подразделяется на два вида: *блочное* и *поточное*, хотя следует отметить, что в некоторых классификациях они не разделяются и считается, что поточное шифрование — это шифрование блоков единичной длины.

Блочное шифрование характеризуется тем, что информация предварительно разбивается на блоки фиксированной длины (например, 64 или 128 бит). При этом в различных КА или даже в разных режимах работы одного и того же алгоритма блоки могут шифроваться как независимо друг от друга, так и «со сцеплением», т. е. когда результат шифрования текущего блока данных зависит от значения предыдущего блока или от результата шифрования предыдущего блока.

Поточное шифрование применяется, прежде всего, тогда, когда информацию невозможно разбить на блоки — скажем, есть некий поток данных, каждый символ которых требуется зашифровать и отправить, не дожидаясь остальных данных, достаточ-

ных для формирования блока. Алгоритмы поточного шифрования шифруют данные побитно или посимвольно.

Асимметричное шифрование характеризуется применением двух типов ключей: открытого — для зашифровывания информации и секретного — для ее расшифровывания. Секретный и открытый ключи связаны между собой достаточно сложным соотношением.

Электронная цифровая подпись (ЭЦП) используется для надежного подтверждения целостности и авторства данных.

6.2. Симметричные алгоритмы шифрования

6.2.1. Основные понятия

В симметричных криптоалгоритмах для зашифровывания и расшифровывания сообщения используется один и тот же блок информации (ключ). Хотя алгоритм воздействия на передаваемые данные может быть известен посторонним лицам, но он зависит от секретного ключа, которым должны обладать только отправитель и получатель. Симметричные криптоалгоритмы выполняют преобразование небольшого блока данных (1 бит либо 32—128 бит) в зависимости от секретного ключа таким образом, что прочесть исходное сообщение можно только зная этот секретный ключ.

Симметричные криптосистемы позволяют на основе симметричных криптоалгоритмов кодировать и декодировать файлы произвольной длины.

Характерная особенность симметричных блочных криптоалгоритмов — преобразование блока входной информации фиксированной длины и получение результирующего блока того же объема, но недоступного для прочтения сторонним лицам, не владеющим ключом. Схему работы симметричного блочного шифра можно описать функциями

$$C = E_K(M) \text{ и } M = D_K(C),$$

где M — исходный (открытый) блок данных, C — зашифрованный блок данных.

Ключ K является параметром симметричного блочного криптоалгоритма и представляет собой блок двоичной информации

фиксированного размера. Исходный *M* и зашифрованный *C* блоки данных также имеют фиксированную разрядность, равную между собой, но необязательно равную длине ключа *K*.

Блочные шифры являются той основой, на которой реализованы практически все симметричные криптосистемы. Практически все алгоритмы используют для преобразований определенный набор обратимых математических преобразований.

Методика создания цепочек из зашифрованных блочными алгоритмами байтов позволяет шифровать ими пакеты информации неограниченной длины. Отсутствие статистической корреляции между битами выходного потока блочного шифра используется для вычисления контрольных сумм пакетов данных и в хэшировании паролей. На сегодняшний день разработано достаточно много стойких блочных шифров.

Криптоалгоритм считается идеально стойким, если для прочтения зашифрованного блока данных необходим перебор всех возможных ключей до тех пор, пока расшифрованное сообщение не окажется осмысленным. В общем случае стойкость блочного шифра зависит только от длины ключа и возрастает экспоненциально с ее ростом. Идеально стойкие криптоалгоритмы должны удовлетворять еще одному важному требованию. Ключ, которым произведено это преобразование, при известных исходном и зашифрованном значениях блока можно узнать только путем полного перебора его значений.

6.2.2. Блочные алгоритмы шифрования данных

Алгоритм шифрования данных DES (Data Encryption Standard) был опубликован в 1977 г. и остается пока распространенным блочным симметричным алгоритмом, используемым в системах защиты коммерческой информации.

Алгоритм DES построен в соответствии с методологией сети Фейстеля и состоит из чередующейся последовательности перестановок и подстановок. Алгоритм DES осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (остальные 8 — проверочные биты для контроля на четность).

Процесс шифрования заключается в начальной перестановке битов 64-битового блока, 16 циклах (раундах) шифрования и, наконец, в конечной перестановке битов (рис. 6.2).

Рис. 6.2. Обобщенная схема шифрования в алгоритме DES

Расшифровывание в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности.

Основные достоинства алгоритма DES:

- используется только один ключ длиной 56 бит;
- относительная простота алгоритма обеспечивает высокую скорость обработки;
- зашифровав сообщение с помощью одного пакета программ, для расшифровки можно использовать любой другой пакет программ, соответствующий алгоритму DES;
- криптостойкость алгоритма вполне достаточна для обеспечения информационной безопасности большинства коммерческих приложений.

Современная микропроцессорная техника позволяет за достаточно приемлемое время взламывать симметричные блочные шифры с длиной ключа 40 бит. Для такого взламывания используется метод полного перебора — тотального опробования всех возможных значений ключа (метод «грубой силы»). До недавнего времени DES считался относительно безопасным алгоритмом шифрования.

Существует много способов комбинирования блочных алгоритмов для получения новых более стойких алгоритмов. Одним из таких способов является *многократное шифрование* — исполь-

зование блочного алгоритма несколько раз с разными ключами для шифрования одного и того же блока открытого текста. При трехкратном шифровании можно применить три различных ключа.

Алгоритм 3-DES (Triple DES — тройной DES) используется в ситуациях, когда надежность алгоритма DES считается недостаточной.

Сегодня все шире используются два современных криптостойких алгоритма шифрования: отечественный стандарт шифрования ГОСТ 28147—89 и новый криптостандарт США — AES (Advanced Encryption Standard).

Стандарт шифрования ГОСТ 28147—89 предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации. Алгоритм шифрования данных, определяемый ГОСТ 28147—89, представляет собой 64-битовый блочный алгоритм с 256-битовым ключом.

Данные, подлежащие зашифрованию, разбивают на 64-разрядные блоки. Эти блоки разбиваются на два субблока N_1 и N_2 по 32 бит (рис. 6.3). Субблок N_1 обрабатывается определенным образом, после чего его значение складывается со значением субблока N_2 (сложение выполняется по модулю 2, т. е. применяется логическая операция XOR — «исключающее или»), а затем

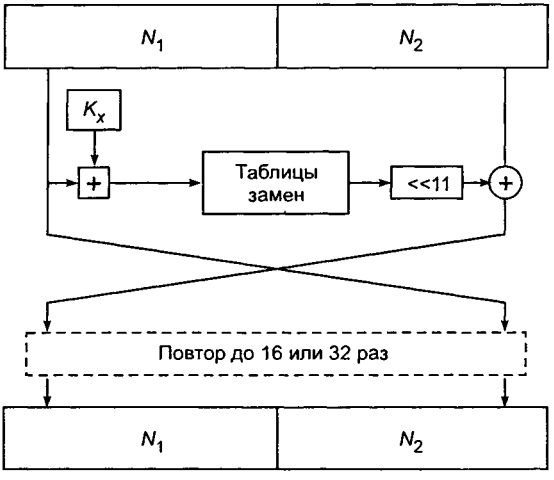


Рис. 6.3. Схема алгоритма ГОСТ 28147—89

субблоки меняются местами. Данное преобразование выполняется определенное число раз («раундов») — 16 или 32, в зависимости от режима работы алгоритма.

В каждом раунде выполняются две операции.

Первая операция — наложение ключа. Содержимое субблока N_1 складывается по модулю 2^{32} с 32-битовой частью ключа K_x. Полный ключ шифрования представляется в виде конкатенации 32-битовых подключей: K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7. В процессе шифрования используется один из этих подключей — в зависимости от номера раунда и режима работы алгоритма.

Вторая операция — табличная замена. После наложения ключа субблок N_1 разбивается на 8 частей по 4 бит, значение каждой из которых заменяется в соответствии с таблицей замены для данной части субблока. Затем выполняется побитовый циклический сдвиг субблока влево на 11 бит.

Табличные замены. Блок подстановки *S*-box (Substitution box) часто используются в современных алгоритмах шифрования, поэтому стоит пояснить, как организуется подобная операция.

Блок подстановки *S*-box состоит из восьми узлов замены (*S*-блоков замены) S_1, S_2, ..., S_8 с памятью 64 бит каждый. Поступающий на блок подстановки *S* 32-битовый вектор разбивают на 8 последовательно идущих 4-битовых векторов, каждый из которых преобразуется в 4-битовый вектор соответствующим узлом замены. Каждый узел замены можно представить в виде таблицы-перестановки 16 4-битовых двоичных чисел в диапазоне 0000...1111. Входной вектор указывает адрес строки в таблице, а число в этой строке является выходным вектором. Затем 4-битовые выходные векторы последовательно объединяют в 32-битовый вектор. Узлы замены (таблицы-перестановки) представляют собой ключевые элементы, которые являются общими для сети ЭВМ и редко изменяются. Эти узлы замены должны сохраняться в секрете.

Алгоритм, определяемый ГОСТ 28147—89, предусматривает четыре режима работы: *простой замены*, *гаммирования*, *гаммирования с обратной связью* и *генерации имитоприставок*. В них используется одно и то же описанное выше шифрующее преобразование, но, поскольку назначение режимов различно, осуществляется это преобразование в каждом из них по-разному.

В режиме *простой замены* для зашифровывания каждого 64-битового блока информации выполняются 32 описанных

выше раунда. При этом 32-битовые подключи используются в следующей последовательности:

K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1 и т. д. — в раундах с 1-го по 24-й;

K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0 — в раундах с 25-го по 32-й.

Расшифровывание в данном режиме проводится точно так же, но с несколько другой последовательностью применения подключей:

K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7 — в раундах с 1-го по 8-й;

K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0, K_7, K_6 и т. д. — в раундах с 9-го по 32-й.

Все блоки шифруются независимо друг от друга, т. е. результат зашифровывания каждого блока зависит только от его содержимого (соответствующего блока исходного текста). При наличии нескольких одинаковых блоков исходного (открытого) текста соответствующие им блоки шифртекста тоже будут одинаковы, что дает дополнительную полезную информацию для пытающегося вскрыть шифр криптоаналитика. Поэтому данный режим применяется в основном для шифрования самих ключей шифрования (очень часто реализуются многоключевые схемы, в которых по ряду соображений ключи шифруются друг на друге). Для шифрования собственно информации предназначены два других режима работы — гаммирования и гаммирования с обратной связью.

В *режиме гаммирования* каждый блок открытого текста побитно складывается по модулю 2 с блоком гаммы шифра размером 64 бит. *Гамма шифра* — это специальная последовательность, которая получается в результате определенных операций с регистрами N_1 и N_2 (рис. 6.9):

1. В регистры N_1 и N_2 записывается их начальное заполнение — 64-битовая величина, называемая синхропосылкой.

2. Выполняется зашифровывание содержимого регистров N_1 и N_2 (в данном случае — синхропосылки) в режиме простой замены.

3. Содержимое регистра N_1 складывается по модулю $(2^{32} - 1)$ с константой $C_1 = 2^{24} + 2^{16} + 2^8 + 2^4$, а результат сложения записывается в регистр N_1.

4. Содержимое регистра N_2 складывается по модулю 232 с константой $C_2 = 2^{24} + 2^{16} + 2^8 + 1$, а результат сложения записывается в регистр N_2.

5. Содержимое регистров N_1 и N_2 подается на выход в качестве 64-битового блока гаммы шифра (в данном случае N_1 и N_2 образуют первый блок гаммы).

Если необходим следующий блок гаммы (т. е. необходимо продолжить зашифровывание или расшифровывание), выполняется возврат к операции 2.

Для расшифровывания гамма вырабатывается аналогичным образом, а затем к битам зашифрованного текста и гаммы снова применяется операция XOR. Поскольку эта операция обратима, в случае правильно выработанной гаммы получается исходный текст (табл. 6.1).

Таблица 6.1. **Зашифровывание и расшифровывание в режиме гаммирования**

	Операция	Результат
Исходный текст		100100
Гамма	XOR	111000
Шифртекст	=	011100
Гамма	XOR	111000
Исходный текст	=	100100

Для выработки нужной для расшифровки гаммы шифра у пользователя, расшифровывающего криптограмму, должен быть тот же ключ и то же значение синхропосылки, которые применялись при зашифровывании информации. В противном случае получить исходный текст из зашифрованного не удастся.

В большинстве реализаций алгоритма ГОСТ 28147—89 синхропосылка не секретна, однако есть системы, где синхропосылка такой же секретный элемент, как и ключ шифрования. Для таких систем эффективная длина ключа алгоритма (256 бит) увеличивается еще на 64 бит секретной синхропосылки, которую также можно рассматривать как ключевой элемент.

В *режиме гаммирования с обратной связью* для заполнения регистров N_1 и N_2, начиная со 2-го блока, используется не предыдущий блок гаммы, а результат зашифрования предыдущего блока открытого текста (рис. 6.4). Первый же блок в данном режиме генерируется полностью аналогично предыдущему.

Рассматривая режим *генерации имитовставок*, следует определить понятие предмета генерации. *Имитовставка* — это криптографическая контрольная сумма, вычисляемая с исполь-

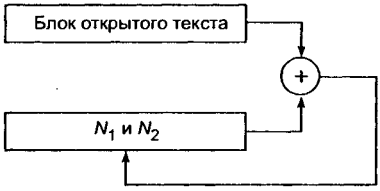


Рис. 6.4. Выработка гаммы шифра в режиме гаммирования с обратной связью

зованием ключа шифрования и предназначенная для проверки целостности сообщений. При генерации имитоприставки выполняются следующие операции: первый 64-битовый блок массива информации, для которого вычисляется имитоприставка, записывается в регистры N_1 и N_2 и зашифровывается в сокращенном режиме простой замены (выполняются первые 16 раундов из 32). Полученный результат суммируется по модулю 2 со следующим блоком информации с сохранением результата в N_1 и N_2.

Цикл повторяется до последнего блока информации. Получившееся в результате этих преобразований 64-битовое содержимое регистров N_1 и N_2 или его часть и называется имитоприставкой. Размер имитоприставки выбирается, исходя из требуемой достоверности сообщений: при длине имитоприставки r бит вероятность, что изменение сообщения останется незамеченным, равна 2^{-r}.

Чаще всего используется 32-битовая имитоприставка, т. е. половина содержимого регистров. Этого достаточно, поскольку, как любая контрольная сумма, имитоприставка предназначена прежде всего для защиты от случайных искажений информации. Для защиты же от преднамеренной модификации данных применяются другие криптографические методы — в первую очередь электронная цифровая подпись.

При обмене информацией имитоприставка служит своего рода дополнительным средством контроля. Она вычисляется для открытого текста при зашифровывании какой-либо информации и посылается вместе с шифртекстом. После расшифровывания вычисляется новое значение имитоприставки, которое сравнивается с присланной. Если значения не совпадают, значит шифртекст был искажен при передаче или при расшифровывании использовались неверные ключи. Особенно полезна имитоприставка для проверки правильности расшифровывания ключевой информации при использовании многоключевых схем.

Алгоритм ГОСТ 28147—89 является очень стойким алгоритмом — в настоящее время для его раскрытия не предложено более эффективных методов, чем упомянутый выше метод «грубой силы». Его высокая стойкость достигается в первую очередь за счет большой длины ключа — 256 бит. При использовании секретной синхропосылки эффективная длина ключа увеличивается до 320 бит, а засекречивание таблицы замен прибавляет дополнительные биты. Кроме того, криптостойкость зависит от количества раундов преобразований, которых по ГОСТ 28147—89 должно быть 32 (полный эффект рассеивания входных данных достигается уже после 8 раундов).

Стандарт шифрования AES. В 1997 г. Американский институт стандартизации NIST (National Institute of Standards & Technology) объявил конкурс на новый стандарт симметричного криптоалгоритма, названного AES (Advanced Encryption Standard). К его разработке были подключены самые крупные центры криптологии всего мира. Победитель этого соревнования фактически становился мировым криптостандартом на ближайшие 10—20 лет.

К криптоалгоритмам — кандидатам на новый стандарт AES — были предъявлены следующие требования:

- алгоритм должен быть симметричным;
- алгоритм должен быть блочным шифром;
- алгоритм должен иметь длину блока 128 бит и поддерживать три длины ключа: 128, 192 и 256 бит.

Дополнительно разработчикам криптоалгоритмов рекомендовалось:

- использовать операции, легко реализуемые как аппаратно (в микрочипах), так и программно (на персональных компьютерах и серверах);
- ориентироваться на 32-разрядные процессоры;
- не усложнять без необходимости структуру шифра, для того чтобы все заинтересованные стороны были в состоянии самостоятельно провести независимый криптоанализ алгоритма и убедиться, что в нем не заложено каких-либо недокументированных возможностей.

Итоги конкурса были подведены в октябре 2000 г. — победителем был объявлен алгоритм Rijndael, разработанный двумя криптографами из Бельгии, Винсентом Риджменом (Vincent Rijmen) и Джоан Даймен (Joan Daemen). Алгоритм Rijndael стал новым стандартом шифрования данных AES [91, 92].

Алгоритм AES не похож на большинство известных алгоритмов симметричного шифрования, структура которых носит название «сеть Фейстеля» и аналогична российскому ГОСТ 28147—89. В отличие от отечественного стандарта шифрования, алгоритм AES представляет каждый блок обрабатываемых данных в виде двухмерного байтового массива размером 4 × 4, 4 × 6 или 4 × 8 в зависимости от установленной длины блока (допускается использование нескольких фиксированных размеров шифруемого блока информации). Далее на соответствующих этапах производятся преобразования либо над независимыми столбцами, либо над независимыми строками, либо вообще над отдельными байтами.

Алгоритм AES состоит из определенного количества раундов (от 10 до 14 — это зависит от размера блока и длины ключа) и выполняет четыре преобразования:

BS (ByteSub) — табличная замена каждого байта массива (рис. 6.5);

SR (ShiftRow) — сдвиг строк массива (рис. 6.6). При этой операции первая строка остается без изменений, а остальные циклически побайтно сдвигаются влево на фиксированное число байт, зависящее от размера массива. Например, для массива размером 4 × 4 строки 2, 3 и 4 сдвигаются соответственно на 1, 2 и 3 байта;

MC (MixColumn) — операция над независимыми столбцами массива (рис. 6.7), когда каждый столбец по определенному правилу умножается на фиксированную матрицу $c(x)$;

AK (AddRoundKey) — добавление ключа. Каждый бит массива складывается по модулю 2 с соответствующим битом ключа раунда, который в свою очередь определенным образом вычисляется из ключа шифрования (рис. 6.8).

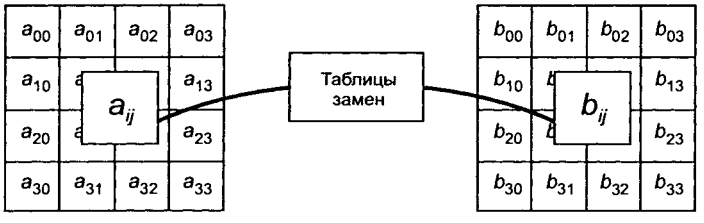


Рис. 6.5. Преобразование BS (ByteSub) использует таблицу замен (подстановок) для обработки каждого байта массива State

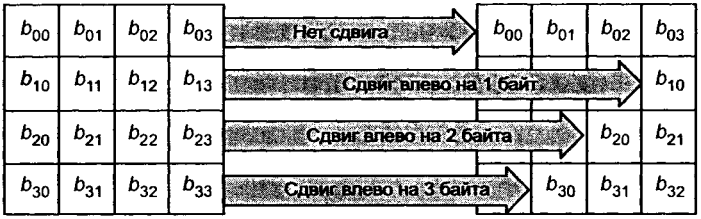


Рис. 6.6. Преобразование SR (ShiftRow) циклически сдвигает три последних строки в массиве State

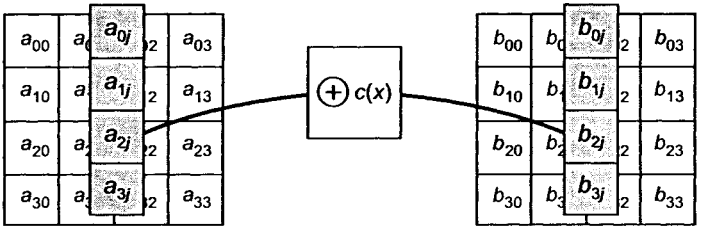


Рис. 6.7. Преобразование MC (MixColumn) поочередно обрабатывает столбцы массива State

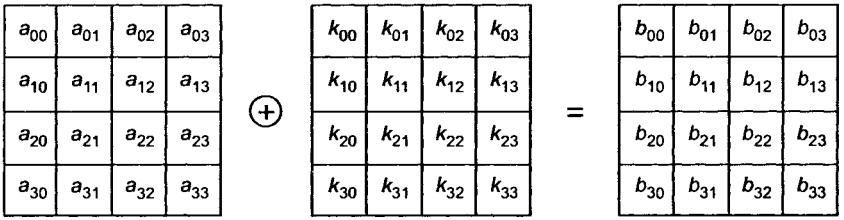


Рис. 6.8. Преобразование AK (AddRoundKey) производит сложение XOR каждого столбца массива State со словом из ключевого набора

Эти преобразования воздействуют на массив State, который адресуется с помощью указателя 'state'. Преобразование AddRoundKey использует дополнительный указатель для адресации ключа раунда Round Key.

Преобразование BS (ByteSub) является нелинейной байтовой подстановкой, которая воздействует независимо на каждый байт массива State, используя таблицу замен (подстановок) *S*-box.

В каждом раунде (с некоторыми исключениями) над шифруемыми данными поочередно выполняются перечисленные

преобразования (рис. 6.9). Исключения касаются первого и последнего раундов: перед первым раундом дополнительно выполняется операция AK, а в последнем раунде отсутствует MC.

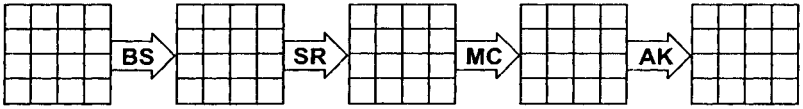


Рис. 6.9. Раунд алгоритма AES

В результате последовательность операций при зашифровывании выглядит так:

AK, {BS, SR, MC, AK} (повторяется $R-1$ раз), BS, SR, AK.

Количество раундов шифрования R в алгоритме AES переменное (10, 12 или 14 раундов) и зависит от размеров блока и ключа шифрования (для ключа также предусмотрено несколько фиксированных размеров).

Расшифровывание выполняется с помощью следующих обратных операций. Выполняется обращение таблицы и табличная замена на инверсной таблице (относительно применяемой при зашифровывании). Обратная операция к SR — это циклический сдвиг строк вправо, а не влево. Обратная операция для MC — умножение по тем же правилам на другую матрицу $d(x)$, удовлетворяющую условию $c(x) \cdot d(x) = 1$. Добавление ключа AK является обратным самому себе, поскольку в нем используется только операция XOR. Эти обратные операции применяются при расшифровании в последовательности, обратной той, что использовалась при зашифровании.

Все преобразования в шифре AES имеют строгое математическое обоснование. Сама структура и последовательность операций позволяют выполнять данный алгоритм эффективно как на 8-битных так и на 32-битных процессорах. В структуре алгоритма заложена возможность параллельного исполнения некоторых операций, что может поднять скорость шифрования на многопроцессорных рабочих станциях в 4 раза.

Алгоритм AES стал новым стандартом шифрования данных благодаря ряду преимуществ перед другими алгоритмами. Прежде всего он обеспечивает высокую скорость шифрования на всех платформах: как при программной, так и при аппаратной реализации. Кроме того, требования к ресурсам для его работы мини-

мальны, что важно при его использовании в устройствах, обладающих ограниченными вычислительными возможностями.

Недостатком алгоритма AES можно считать лишь его нетрадиционную схему. Дело в том, что свойства алгоритмов, основанных на «сети Фейстеля», хорошо исследованы, а AES, в отличие от них, может содержать скрытые уязвимости, которые могут обнаружиться только по прошествии какого-то времени с момента начала его широкого распространения.

Для шифрования данных применяются и другие симметричные блочные криптоалгоритмы.

Основные режимы работы блочного симметричного алгоритма

Большинство блочных симметричных криптоалгоритмов непосредственно преобразуют 64-битовый входной открытый текст в 64-битовый выходной шифрованный текст, однако данные редко ограничиваются 64 разрядами.

Чтобы воспользоваться блочным симметричным алгоритмом для решения разнообразных криптографических задач, разработаны четыре рабочих режима:

- электронная кодовая книга ECB (Electronic Code Book);
- сцепление блоков шифра CBC (Cipher Block Chaining);
- обратная связь по шифртексту CFB (Cipher Feed Back);
- обратная связь по выходу OFB (Output Feed Back).

Эти рабочие режимы первоначально были разработаны для блочного алгоритма DES, но в любом из этих режимов могут работать и другие блочные криптоалгоритмы.

6.3. Асимметричные криптоалгоритмы

Всего за 30 лет асимметричная криптография превратилась в одно из основных направлений криптологии и используется в ИТ так же часто, как и симметричные криптосистемы.

6.3.1. Алгоритм шифрования RSA

Криптоалгоритм RSA предложили в 1978 г. три автора: Р. Райвест (Rivest), А. Шамир (Shamir) и А. Адлеман (Adleman). Алгоритм получил свое название по первым буквам фамилий его

авторов. Он стал первым алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи [62].

Надежность алгоритма RSA основывается на трудности факторизации больших чисел и трудности вычисления дискретных логарифмов в конечном поле.

В алгоритме RSA открытый ключ K_B, секретный ключ k_B, сообщение M и криптограмма C принадлежат множеству целых чисел

$$Z_N = \{0, 1, 2, ..., N-1\},$$

где N — модуль:

$$N = PQ,$$

а P и Q — случайные большие простые числа. Для обеспечения максимальной безопасности выбирают P и Q равной длины и хранят в секрете.

Множество Z_N с операциями сложения и умножения по модулю N образует арифметику по модулю N.

Открытый ключ K_B выбирают случайным образом так, чтобы выполнялись условия:

$$1 < K_B \le \varphi(N), \text{ НОД } (K_B, \varphi(N)) = 1;$$

$$\varphi(N) = (P-1)(Q-1),$$

где $\varphi(N)$ — функция Эйлера.

Функция Эйлера $\varphi(N)$ указывает количество положительных целых чисел в интервале от 1 до N, которые взаимно просты с N.

Второе из указанных выше условий означает, что открытый ключ K_B и функция Эйлера $\varphi(N)$ должны быть взаимно простыми.

Далее, используя расширенный алгоритм Евклида, вычисляют секретный ключ k_B, такой, что

$$k_B \cdot K_B \equiv 1 \pmod{\varphi(N)}$$

или

$$k_B = K_B^{-1} \pmod{(P-1)(Q-1)}.$$

Это можно осуществить, так как получатель B знает пару простых чисел (P, Q) и может легко найти $\varphi(N)$. Заметим, что k_B и N должны быть взаимно простыми.

Открытый ключ K_B используют для шифрования данных, а секретный ключ k_B — для расшифровывания.

Процедура шифрования определяет криптограмму C через пару (K_B, M) в соответствии со следующей формулой:

$$C = E_{K_B}(M) = M^{K_B} (\text{mod } N).$$

В качестве алгоритма быстрого вычисления значения C используют ряд последовательных возведений в квадрат целого M и умножений на M с приведением по модулю N.

Расшифровывание криптограммы C выполняют, используя пару (k_B, C) по следующей формуле:

$$M = D_{k_B}(C) = C^{k_B} (\text{mod } N).$$

Криптоалгоритм RSA всесторонне исследован и признан стойким при достаточной длине ключей. В настоящее время длина ключа — 1024 бита — считается приемлемым вариантом. Некоторые авторы утверждают, что с ростом мощности процессоров криптоалгоритм RSA потеряет стойкость к атаке полного перебора. Однако увеличение мощности процессоров позволит применить более длинные ключи, что повышает стойкость RSA.

В асимметричной криптосистеме RSA количество используемых ключей связано с количеством абонентов линейной зависимостью (в системе из N пользователей используются $2N$ ключей), а не квадратичной, как в симметричных системах.

Следует отметить, что быстродействие RSA существенно ниже быстродействия DES, а программная и аппаратная реализация криптоалгоритма RSA гораздо сложнее, чем DES. Поэтому криптосистема RSA, как правило, используется при передаче небольшого объема сообщений.

6.3.2. Алгоритмы цифровой подписи

Стандарт цифровой подписи ГОСТ Р 34.10—94 — первый отечественный стандарт цифровой подписи — вступил в действие с начала 1995 г. В нем используются следующие параметры:

p — большое простое число длиной 509—512 бит либо 1020—1024 бит;

q — простой сомножитель числа $(p-1)$, имеющий длину 254—256 бит;

a — любое число, меньшее $(p-1)$, причем такое, что $a^q \bmod p = 1$;

x — некоторое число, меньшее q;

$y = a^x \bmod p$.

Кроме того, этот алгоритм использует однонаправленную хэш-функцию $H(x)$. ГОСТ Р 34.11—94 определяет хэш-функцию, основанную на использовании стандартного симметричного алгоритма ГОСТ 28147—89.

Первые три параметра — p, q и a — являются открытыми и могут быть общими для всех пользователей сети. Число x — секретный ключ, число y — открытый ключ.

Чтобы подписать некоторое сообщение m, а затем проверить подпись, выполняются следующие шаги.

1. Пользователь A генерирует случайное число k, причем $k < q$.

2. Пользователь A вычисляет значения:

$$r = (a^k \bmod p) \bmod q;$$

$$s = (x \cdot r + k(H(m))) \bmod q.$$

Если $H(m) \bmod q = 0$, то значение $H(m) \bmod q$ принимают равным единице. Если $r = 0$, то выбирают другое значение k и начинают снова.

Цифровая подпись представляет собой два числа:

$$r \bmod 2^{256} \quad \text{и} \quad s \bmod 2^{256}.$$

Пользователь A отправляет эти числа пользователю B.

3. Пользователь B проверяет полученную подпись, вычисляя:

$$v = H(m)^{q-2} \bmod q;$$

$$z_1 = (s \cdot v) \bmod q;$$

$$z_2 = ((q - r) \cdot v) \bmod q;$$

$$u = ((a^{z_1} \cdot y^{z_2}) \bmod p) \bmod q.$$

Если $u = r$, то подпись считается верной.

Различие между этим алгоритмом и алгоритмом DSA заключается в том, что в DSA

$$s = (k^{-1}(x \cdot r + (H(m))))\bmod q,$$

что приводит к другому уравнению верификации.

Следует также отметить, что в отечественном стандарте ЭЦП параметр q имеет длину 256 бит. Западных криптографов вполне устраивает q длиной примерно 160 бит. Различие в значениях параметра q является стремлением разработчиков отечественного стандарта к получению более безопасной подписи.

Новый отечественный стандарт цифровой подписи ГОСТ Р 34.10—2001 был принят в 2001 г. Его принципиальное отличие от предыдущего ГОСТ Р 34.10—94 состоит в том, что все вычисления при генерации и проверке ЭЦП в новом алгоритме производятся в группе точек эллиптической кривой, определенной над конечным полем F_p. Принадлежность точки (пары чисел x и y) к данной группе определяется следующим соотношением:

$$y^2 \equiv x^3 + ax + b \bmod p,$$

где модуль системы p является простым числом, большим 3, а коэффициенты a и b являются константами, удовлетворяющими следующим соотношениям:

$$a < p,\ b < p;$$

$$4a^3 + 27b^2 \neq 0 \bmod p.$$

Дальнейшие математические подробности можно найти в [17, 62]. Следует отметить, что принципы вычислений по данному алгоритму аналогичны применяемым в ГОСТ Р 34.10—94. Сначала генерируется случайное число x, с его помощью вычисляется r-часть ЭЦП, затем вычисляется s-часть ЭЦП из r-части, значения x, значения секретного ключа и хэш-значения подписываемых данных.

При проверке же подписи аналогичным образом проверяется соответствие определенным соотношениям r, s, открытого ключа и хэш-значения информации, подпись которой проверяется. Подпись считается неверной, если соотношения не соблюдаются.

В перспективе криптосистемы на основе эллиптических кривых, вероятно, вытеснят существующие алгоритмы ЭЦП, асим-

метричного шифрования и выработки ключей парной связи (ключ для шифрования информации между двумя конкретными пользователями вычисляется из секретного ключа отправителя информации и открытого ключа получателя). Алгоритмы на базе эллиптических кривых позволяют заметно сократить время вычислений без потерь криптостойкости или соответственно увеличить уровень защиты при тех же временных затратах.

Отечественный стандарт хэширования ГОСТ Р 34.11—94

Отечественным стандартом генерирования хэш-функции является алгоритм ГОСТ Р 34.11—94. Этот стандарт является обязательным для применения в качестве алгоритма хэширования в государственных организациях РФ и ряде коммерческих организаций. Коротко данный алгоритм хэширования можно описать следующим образом (рис. 6.10) [12].

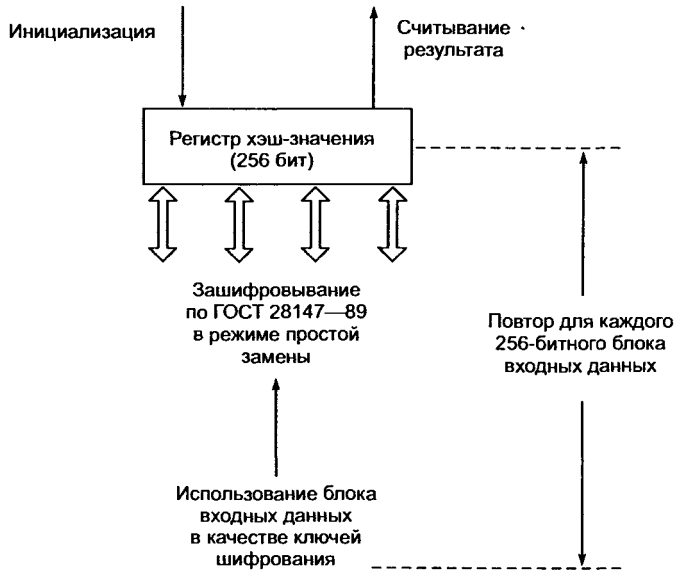


Рис. 6.10. Хэширование по алгоритму ГОСТ Р 34.11—94

Шаг 1. Инициализация регистра хэш-значения. Если длина сообщения не превышает 256 бит — переход к шагу 3, если превышает — переход к шагу 2.

Шаг 2. Итеративное вычисление хэш-значения блоков хэшируемых данных по 256 бит с использованием хранящегося в регистре хэш-значения предыдущего блока. Вычисление включает в себя следующие действия:

- генерацию ключей шифрования на основе блока хэшируемых данных;
- зашифровывание хранящегося в регистре хэш-значения в виде четырех блоков по 64 бита по алгоритму ГОСТ 28147—89 в режиме простой замены;
- перемешивание результата.

Вычисление производится до тех пор, пока длина необработанных входных данных не станет меньше или равной 256 бит. В этом случае — переход к шагу 3.

Шаг 3. Дополнение битовыми нулями необработанной части сообщения до 256 бит. Вычисление хэш-значения аналогично шагу 2. В результате в регистре оказывается искомое хэш-значение.

Глава 7
ТЕХНОЛОГИИ АУТЕНТИФИКАЦИИ

Применение открытых каналов передачи данных создает потенциальные возможности для действий злоумышленников (нарушителей). Поэтому одной из важных задач обеспечения информационной безопасности при взаимодействии пользователей является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны. Обычно для решения данной проблемы применяются специальные приемы, дающие возможность проверить подлинность проверяемой стороны.

7.1. Аутентификация, авторизация и администрирование действий пользователей

С каждым зарегистрированным в компьютерной системе субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов, именующие данный субъект. Эту информацию называют *идентификатором* субъекта. Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (законным) пользователем; остальные пользователи относятся к нелегальным пользователям. Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию и аутентификацию.

Идентификация (*Identification*) — процедура распознавания пользователя по его идентификатору (имени). Эта функция вы-

полняется, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация (*Authentication*) — процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы: можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (*Authorization*) — процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу его действия и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, то конфиденциальность и целостность информации в этой системе могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Администрирование (*Accounting*) — регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. Хотя эта учетная информация может быть использована для выписывания счета, с позиций безопасности она особенно важна для обнаружения, анализа инцидентов безопасности в сети и соответствующего реагирования на них. Записи в системном журнале, аудиторские проверки и ПО accounting — все это может быть использовано для обеспечения подотчетности пользователей, если что-либо случится при входе в сеть с их идентификатором.

Необходимый уровень аутентификации определяется требованиями безопасности, которые установлены в организации. Общедоступные Web-серверы могут разрешить анонимный или гостевой доступ к информации. Финансовые транзакции могут потребовать строгой аутентификации. Примером слабой формы аутентификации может служить использование IP-адреса для определения пользователя. Подмена (spoofing) IP-адреса может легко разрушить механизм аутентификации. Надежная аутентификация является тем ключевым фактором, который гарантирует, что только авторизованные пользователи получат доступ к контролируемой информации.

При защите каналов передачи данных должна выполняться *взаимная аутентификация субъектов*, т. е. взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи. Процедура подтверждения подлинности выполняется обычно в начале сеанса установления соединения абонентов. Термин «соединение» указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры — обеспечить уверенность, что соединение установлено с законным субъектом и вся информация дойдет до места назначения.

Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от предъявляемых субъектом сущностей процессы аутентификации могут быть разделены на основе:

- *знания* чего-либо. Примерами могут служить пароль, персональный идентификационный код PIN (Personal Identification Number), а также секретные и открытые ключи, знание которых демонстрируется в протоколах типа запрос—ответ;
- *обладания* чем-либо. Обычно это магнитные карты, смарт-карты, сертификаты и устройства *touch memory*;
- каких-либо неотъемлемых *характеристик*. Эта категория включает методы, базирующиеся на проверке биометрических характеристик пользователя (голоса, радужной оболочки и сетчатки глаза, отпечатков пальцев, геометрии ладони и др.). В данной категории не используются криптографические методы и средства. Аутентификация на основе биометрических характеристик применяется для контроля доступа в помещения или к какой-либо технике [9, 54].

Пароль — это то, что знает пользователь и другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

Персональный идентификационный номер PIN (Personal Identification Number) является испытанным способом аутентификации держателя пластиковой карты и смарт-карты. Секретное значение PIN-кода должно быть известно только держателю карты.

Динамический (одноразовый) пароль — это пароль, который после однократного применения никогда больше не используется. На практике обычно используется регулярно меняющееся значение, которое базируется на постоянном пароле или ключевой фразе.

Система запрос—ответ. Одна из сторон инициирует аутентификацию с помощью посылки другой стороне уникального и непредсказуемого значения «запрос», а другая сторона посылает ответ, вычисленный с помощью «запроса» и секрета. Так как обе стороны владеют одним секретом, то первая сторона может проверить правильность ответа второй стороны.

Сертификаты и цифровые подписи. Если для аутентификации используются сертификаты, то требуется применение цифровых подписей на этих сертификатах. Сертификаты выдаются ответственным лицом в организации пользователя, сервером сертификатов или внешней доверенной организацией. В рамках Интернета появились коммерческие инфраструктуры управления открытыми ключами PKI (Public Key Infrastructure) для распространения сертификатов открытых ключей. Пользователи могут получить сертификаты различных уровней.

Процессы аутентификации можно также классифицировать по уровню обеспечиваемой безопасности [9, 54]. В соответствии с этим процессы аутентификации разделяются на следующие типы:

- аутентификация, использующая пароли и PIN-коды;
- строгая аутентификация на основе использования криптографических методов и средств;
- биометрическая аутентификация пользователей.

С точки зрения безопасности каждый из перечисленных типов способствует решению своих специфических задач, поэтому процессы и протоколы аутентификации активно используются на практике.

Основные атаки на протоколы аутентификации:

- *маскарад* (*impersonation*). Пользователь выдает себя за другого с целью получения полномочий и возможности действий от лица другого пользователя;
- *подмена стороны* аутентификационного обмена (*interleaving attack*). Злоумышленник в ходе данной атаки участвует в процессе аутентификационного обмена между двумя сторонами с целью модификации проходящего через него трафика;
- *повторная передача* (*replay attack*) заключается в повторной передаче аутентификационных данных каким-либо пользователем;
- *принудительная задержка* (*forced delay*). Злоумышленник перехватывает некоторую информацию и передает ее спустя некоторое время;
- *атака с выборкой текста* (*chosen-text attack*). Злоумышленник перехватывает аутентификационный трафик и пытается получить информацию о долговременных криптографических ключах.

Для предотвращения таких атак при построении протоколов аутентификации применяются:

- использование механизмов типа «запрос—ответ», «отметка времени», случайных чисел, идентификаторов, цифровых подписей;
- привязка результата аутентификации к последующим действиям пользователей в рамках системы. Примером подобного подхода может служить осуществление в процессе аутентификации обмена секретными сеансовыми ключами, которые используются при дальнейшем взаимодействии пользователей;
- периодическое выполнение процедур аутентификации в рамках уже установленного сеанса связи и т. п.

Механизм «запрос—ответ» состоит в следующем. Если пользователь A хочет быть уверенным, что сообщения, получаемые им от пользователя B, не являются ложными, он включает в посылаемое для B сообщение непредсказуемый элемент — запрос X (например, некоторое случайное число). При ответе пользователь B должен выполнить над этим элементом некоторую операцию (например, вычислить некоторую функцию $f(X)$). Это невозможно осуществить заранее, так как пользователю B неизвестно, какое случайное число X придет в запросе. Получив

ответ с результатом действий *B*, пользователь *A* может быть уверен, что *B* — подлинный. Недостаток этого метода — возможность установления закономерности между запросом и ответом.

Механизм «отметка времени» подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети определяет, насколько «устарело» пришедшее сообщение, и решает не принимать его, поскольку оно может быть ложным.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

При использовании отметок времени возникает проблема *допустимого временного интервала задержки* для подтверждения подлинности сеанса: сообщение с «временным штемпелем» в принципе не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы.

При сравнении и выборе протоколов аутентификации необходимо учитывать следующие характеристики:

- наличие *взаимной аутентификации*. Это свойство отражает необходимость обоюдной аутентификации между сторонами аутентификационного обмена;
- *вычислительную эффективность*. Это количество операций, необходимых для выполнения протокола;
- *коммуникационную эффективность*. Данное свойство отражает количество сообщений и их длину, необходимую для осуществления аутентификации;
- *наличие третьей стороны*. Примером третьей стороны может служить доверенный сервер распределения симметричных ключей или сервер, реализующий дерево сертификатов для распределения открытых ключей;
- *гарантии безопасности*. Примером может служить применение шифрования и цифровой подписи [9, 54].

7.2. Методы аутентификации, использующие пароли и PIN-коды

Одной из распространенных схем аутентификации является *простая аутентификация*, которая основана на применении традиционных многоразовых паролей с одновременным согласованием средств его использования и обработки. Аутентификация

на основе многоразовых паролей — простой и наглядный пример использования разделяемой информации. Пока в большинстве защищенных виртуальных сетей VPN (Virtual Private Network) доступ клиента к серверу разрешается по паролю. Однако все чаще применяются более эффективные средства аутентификации, например программные и аппаратные системы аутентификации на основе одноразовых паролей, смарт-карт, PIN-кодов и цифровых сертификатов.

7.2.1. Аутентификация на основе многоразовых паролей

Базовый принцип «единого входа» предполагает достаточность одноразового прохождения пользователем процедуры аутентификации для доступа ко всем сетевым ресурсам. Поэтому в современных операционных системах предусматривается централизованная служба аутентификации, которая выполняется одним из серверов сети и использует для своей работы базу данных (БД). В этой БД хранятся учетные данные о пользователях сети, включающие идентификаторы и пароли пользователей, а также другую информацию [45].

Процедуру простой аутентификации пользователя в сети можно представить следующим образом. Пользователь при попытке логического входа в сеть набирает свои идентификатор и пароль. Эти данные поступают для обработки на сервер аутентификации. В БД, хранящейся на сервере аутентификации, по идентификатору пользователя находится соответствующая запись. Из нее извлекается пароль и сравнивается с тем паролем, который ввел пользователь. Если они совпали, то аутентификация прошла успешно — пользователь получает легальный статус и получает те права и ресурсы сети, которые определены для его статуса системой авторизации.

В схеме простой аутентификации (рис. 7.1) передача пароля и идентификатора пользователя может производиться следующими способами [9]:

- в незашифрованном виде; например, согласно протоколу парольной аутентификации PAP (Password Authentication Protocol) пароли передаются по линии связи в открытой незащищенной форме;

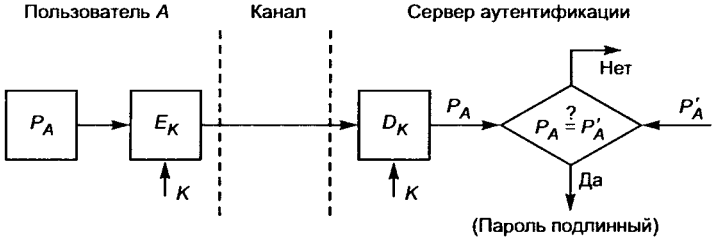


Рис. 7.1. Простая аутентификация с использованием пароля

- в защищенном виде; все передаваемые данные (идентификатор и пароль пользователя, случайное число и метки времени) защищены посредством шифрования или однонаправленной функции.

Очевидно, что вариант аутентификации с передачей пароля пользователя в незашифрованном виде не гарантирует даже минимального уровня безопасности, так как подвержен многочисленным атакам и легко компрометируется. Чтобы защитить пароль, его нужно зашифровать перед пересылкой по незащищенному каналу. Для этого в схему включены средства шифрования E_K и расшифровывания D_K, управляемые разделяемым секретным ключом K. Проверка подлинности пользователя основана на сравнении присланного пользователем пароля P_A и исходного значения P'_A, хранящегося на сервере аутентификации. Если значения P_A и P'_A совпадают, то пароль P_A считается подлинным, а пользователь A — законным.

Схемы организации простой аутентификации отличаются не только методами передачи паролей, но и видами их хранения и проверки. Наиболее распространенным способом является хранение паролей пользователей в открытом виде в системных файлах, причем на эти файлы устанавливаются атрибуты защиты от чтения и записи (например, при помощи описания соответствующих привилегий в списках контроля доступа ОС). Система сопоставляет введенный пользователем пароль с хранящейся в файле паролей записью. При этом способе не используются криптографические механизмы, такие как шифрование или однонаправленные функции. Очевидным недостатком этого способа является возможность получения злоумышленником в системе привилегий администратора, включая права доступа к системным файлам, и в частности, к файлу паролей.

Для обеспечения надежной защиты ОС пароль каждого пользователя должен быть известен только этому пользователю и никому другому, в том числе и администраторам системы. На первый взгляд то, что администратор знает пароль некоторого пользователя, не отражается негативно на безопасности системы, поскольку администратор, войдя в систему от имени обычного пользователя, получает права меньшие чем те, которые он получит, зайдя в систему от своего имени. Однако, входя в систему от имени другого пользователя, администратор получает возможность обходить систему аудита, а также совершать действия, компрометирующие этого пользователя, что недопустимо в защищенной системе. Таким образом, пароли пользователей не должны храниться в ОС в открытом виде.

С точки зрения безопасности предпочтительным является метод передачи и хранения паролей с использованием односторонних функций. Обычно для шифрования паролей в списке пользователей используют одну из известных криптографически стойких *хэш-функций*. В списке пользователей хранится не сам пароль, а *образ пароля*, являющийся результатом применения к паролю хэш-функции.

Однонаправленность хэш-функции не позволяет восстановить пароль по образу пароля, но позволяет, вычислив хэш-функцию, получить образ введенного пользователем пароля и таким образом проверить правильность введенного пароля. В простейшем случае в качестве хэш-функции используется результат шифрования некоторой константы на пароле.

Например, односторонняя функция $h(\cdot)$ может быть определена следующим образом:

$$h(P) = E_P(ID),$$

где P — пароль пользователя; ID — идентификатор пользователя; E_P — процедура шифрования, выполняемая с использованием пароля P в качестве ключа.

Такие функции удобны, если длина пароля и ключа одинаковы. В этом случае проверка подлинности пользователя A с помощью пароля P_A состоит из пересылки серверу аутентификации отображения $h(P_A)$ и сравнения его с предварительно вычисленным и хранимым в БД сервера аутентификации эквивалентом $h'(P_A)$ (рис. 7.2). Если отображения $h(P_A)$ и $h'(P_A)$ равны, то считается, что пользователь успешно прошел аутентификацию.

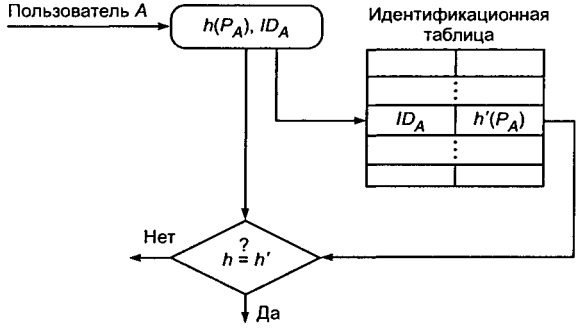


Рис. 7.2. Использование односторонней функции для проверки пароля

На практике пароли состоят лишь из нескольких символов, чтобы дать возможность пользователям запомнить их. Короткие пароли уязвимы к атаке полного перебора всех вариантов. Для того чтобы предотвратить такую атаку, функцию $h(P)$ можно определить иначе, например в виде:

$$h(P) = E_{P \oplus K}(ID),$$

где K и ID — соответственно ключ и идентификатор отправителя.

Различают две формы представления объектов, аутентифицирующих пользователя:

- внешний аутентифицирующий объект, не принадлежащий системе;
- внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта.

Внешние объекты могут быть представлены на различных носителях информации: пластиковых картах, смарт-картах, гибких магнитных дисках и т. п. Естественно, что внешняя и внутренняя формы представления аутентифицирующего объекта должны быть семантически тождественны.

Системы простой аутентификации на основе многоразовых паролей имеют пониженную стойкость, поскольку выбор аутентифицирующей информации происходит из относительно небольшого числа слов. Срок действия многоразового пароля должен быть определен в политике безопасности организации. Пароли должны регулярно изменяться, быть трудными для угадывания и не присутствовать в словаре.

В гл. 13 рассматриваются: протокол аутентификации по многоразовому паролю PAP (Password Authentication Protocol), про-

токол аутентификации на основе процедуры запрос—отклик CHAP (Challenge-Handshake Authentication Protocol), а также протоколы централизованного контроля доступа к сети удаленных пользователей TACACS (Terminal Access Controller Access Control System), TACACS+ и RADIUS (Remote Authentication Dial-In User Service).

7.2.2. Аутентификация на основе одноразовых паролей

Схемы аутентификации, основанные на традиционных многоразовых паролях, не обладают достаточной безопасностью. Такие пароли можно перехватить, разгадать, подсмотреть или просто украсть. Более надежными являются процедуры аутентификации на основе одноразовых паролей.

Суть схемы одноразовых паролей — использование различных паролей при каждом новом запросе на предоставление доступа. Одноразовый динамический пароль действителен только для одного входа в систему, и затем его действие истекает. Даже если его перехватили, он будет бесполезен. Динамический механизм задания пароля — один из лучших способов защиты процесса аутентификации от угроз извне. Обычно системы аутентификации с одноразовыми паролями используются для проверки удаленных пользователей.

Генерация одноразовых паролей может осуществляться аппаратным или программным способом. Некоторые аппаратные средства доступа на основе одноразовых паролей реализуются в виде миниатюрных устройств со встроенным микропроцессором, внешне похожих на платежные пластиковые карточки. Такие карты, обычно называемые ключами, могут иметь клавиатуру и небольшое дисплейное окно.

В качестве примера рассмотрим технологию аутентификации SecurID на основе одноразовых паролей с использованием аппаратных ключей и механизма временно́й синхронизации. Эта технология разработана компанией Security Dynamics и реализована в коммуникационных серверах ряда компаний, в частности в серверах компании Cisco Systems и др.

Схема аутентификации с использованием временно́й синхронизации базируется на алгоритме генерации случайных чисел через определенный интервал времени. Этот интервал устанав-

ливается и может быть изменен администратором сети. Схема аутентификации использует два параметра:

- секретный ключ, представляющий собой уникальное 64-битное число, назначаемое каждому пользователю и хранящееся в БД аутентификационного сервера и в аппаратном ключе пользователя;
- значение текущего времени.

Когда удаленный пользователь делает попытку логического входа в сеть, ему предлагается ввести его персональный идентификационный номер PIN, состоящий из четырех десятичных цифр, и шесть цифр случайного числа, отображаемого в этот момент на дисплее аппаратного ключа. Используя введенный пользователем PIN-код, сервер извлекает из БД секретный ключ пользователя и выполняет алгоритм генерации случайного числа, используя в качестве параметров извлеченный секретный ключ и значение текущего времени. Затем сервер проверяет, совпадают ли сгенерированное число и число, введенное пользователем. Если эти числа совпадают, то сервер разрешает пользователю осуществить логический вход в систему.

При использовании этой схемы аутентификации требуется жесткая временна́я синхронизация аппаратного ключа и сервера. Со схемой аутентификации, основанной на временной синхронизации, связана еще одна проблема. Генерируемое аппаратным ключом случайное число является достоверным паролем в течение небольшого конечного промежутка времени. Поэтому возможна кратковременная ситуация, когда можно перехватить PIN-код и случайное число, чтобы использовать их для доступа в сеть. Это — уязвимое место схемы.

Одним из наиболее распространенных протоколов аутентификации на основе одноразовых паролей является стандартизованный в Интернете протокол S/Key (RFC 1760). Этот протокол реализован во многих системах, требующих проверки подлинности удаленных пользователей, в частности в системе TACACS+ компании Cisco. Протокол S/Key подробно рассматривается в гл. 13.

7.2.3. Аутентификация на основе PIN-кода

Наиболее распространенным методом аутентификации держателя пластиковой карты и смарт-карты является ввод секретного числа, которое обычно называют *PIN-кодом* (*Personal Iden-*

tification Number — персональный идентификационный код) или иногда CHV (CardHolder Verification). Защита PIN-кода карты является критичной для безопасности всей системы. Карты могут быть потеряны, украдены или подделаны. В таких случаях единственной контрмерой против несанкционированного доступа остается секретное значение PIN-кода. Вот почему открытая форма PIN должна быть известна только законному держателю карты. Очевидно, значение PIN нужно держать в секрете в течение всего срока действия карты.

Длина PIN-кода должна быть достаточно большой, чтобы минимизировать вероятность определения правильного PIN-кода методом проб и ошибок. С другой стороны, длина PIN-кода должна быть достаточно короткой, чтобы дать возможность держателям карт запомнить его значение. Согласно рекомендации стандарта ISO 9564-1, PIN-код должен содержать от 4 до 12 буквенно-цифровых символов. Однако в большинстве случаев ввод нецифровых символов технически невозможен, поскольку доступна только цифровая клавиатура. Поэтому обычно PIN-код представляет собой четырехразрядное число, каждая цифра которого может принимать значение от 0 до 9.

PIN-код вводится с помощью клавиатуры терминала или компьютера и затем отправляется на смарт-карту. Смарт-карта сравнивает полученное значение PIN-кода с эталонным значением, хранимым в карте, и отправляет результат сравнения на терминал. Ввод PIN-кода относится к мерам безопасности, особенно для финансовых транзакций, и, следовательно, требования к клавиатуре часто определяются в прикладной области. PIN-клавиатуры имеют все признаки модуля безопасности и шифруют PIN-код сразу при его вводе. Это обеспечивает надежную защиту от проникновения в клавиатуру для перехвата PIN-кода во время ввода.

При идентификации клиента по значению PIN-кода и предъявленной карте используются два основных способа проверки PIN-кода: неалгоритмический и алгоритмический [29].

Неалгоритмический способ проверки PIN-кода не требует применения специальных алгоритмов. Проверка PIN-кода осуществляется путем непосредственного сравнения введенного клиентом PIN-кода со значениями, хранимыми в БД. Обычно БД со значениями PIN-кодов клиентов шифруется методом прозрачного шифрования, чтобы повысить ее защищенность, не усложняя процесса сравнения.

Алгоритмический способ проверки PIN-кода заключается в том, что введенный клиентом PIN-код преобразуют по определенному алгоритму с использованием секретного ключа и затем сравнивают со значением PIN-кода, хранящимся в определенной форме на карте. Достоинства этого метода проверки:

- отсутствие копии PIN-кода на главном компьютере исключает его раскрытие обслуживающим персоналом;
- отсутствие передачи PIN-кода между банкоматом или кассиром-автоматом и главным компьютером банка исключает его перехват злоумышленником или навязывание результатов сравнения;
- упрощение работы по созданию программного обеспечения системы, так как уже нет необходимости действий в реальном масштабе времени.

7.3. Строгая аутентификация

7.3.1. Основные понятия

Идея строгой аутентификации, реализуемая в криптографических протоколах, заключается в следующем. Проверяемая (доказывающая) сторона доказывает свою подлинность проверяющей стороне, демонстрируя знание некоторого секрета [54, 62]. Например, этот секрет может быть предварительно распределен безопасным способом между сторонами аутентификационного обмена. Доказательство знания секрета осуществляется с помощью последовательности запросов и ответов с использованием криптографических методов и средств.

Существенным является факт, что доказывающая сторона демонстрирует только знание секрета, но сам секрет в ходе аутентификационного обмена не раскрывается. Это обеспечивается посредством ответов доказывающей стороны на различные запросы проверяющей стороны. При этом результирующий запрос зависит только от пользовательского секрета и начального запроса, который обычно представляет произвольно выбранное в начале протокола большое число.

В большинстве случаев строгая аутентификация заключается в том, что каждый пользователь аутентифицируется по признаку владения своим секретным ключом. Иначе говоря, пользователь

имеет возможность определить, владеет ли его партнер по связи надлежащим секретным ключом и может ли он использовать этот ключ для подтверждения того, что он действительно является подлинным партнером по информационному обмену.

В соответствии с рекомендациями стандарта X.509 различают процедуры строгой аутентификации следующих типов:

- односторонняя аутентификация;
- двусторонняя аутентификация;
- трехсторонняя аутентификация.

Односторонняя аутентификация предусматривает обмен информацией только в одном направлении.

Двусторонняя аутентификация по сравнению с односторонней содержит дополнительный ответ проверяющей стороны доказывающей стороне, который должен убедить ее, что связь устанавливается именно с той стороной, которой были предназначены аутентификационные данные;

Трехсторонняя аутентификация содержит дополнительную передачу данных от доказывающей стороны проверяющей. Этот подход позволяет отказаться от использования меток времени при проведении аутентификации.

Следует отметить, что данная классификация достаточно условна. На практике набор используемых приемов и средств зависит непосредственно от конкретных условий реализации процесса аутентификации. Необходимо учитывать, что проведение строгой аутентификации требует обязательного согласования сторонами используемых криптографических алгоритмов и дополнительных параметров [9, 54].

Прежде чем перейти к рассмотрению конкретных вариантов протоколов строгой аутентификации, следует остановиться на назначении и возможностях так называемых одноразовых параметров, используемых в протоколах аутентификации. Одноразовые параметры иногда называют также *nonces* — это величина, используемая для одной и той же цели не более одного раза. Среди используемых на сегодняшний день одноразовых параметров следует выделить: случайные числа, метки времени и номера последовательностей.

Одноразовые параметры позволяют избежать повтора передачи, подмены стороны аутентификационного обмена и атаки с выбором открытого текста. С их помощью можно обеспечить уникальность, однозначность и временные гарантии передаваe-

мых сообщений. Различные типы одноразовых параметров могут употребляться как отдельно, так и дополнять друг друга.

Следует отметить, что одноразовые параметры широко используются и в других вариантах криптографических протоколов (например, в протоколах распределения ключевой информации).

В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации делятся на протоколы, основанные:

- на симметричных алгоритмах шифрования;
- однонаправленных ключевых хэш-функциях;
- асимметричных алгоритмах шифрования;
- алгоритмах электронной цифровой подписи.

7.3.2. Строгая аутентификация, основанная на симметричных алгоритмах

Для работы протоколов аутентификации, построенных на основе симметричных алгоритмов, необходимо, чтобы проверяющий и доказывающий с самого начала имели один и тот же секретный ключ. Для закрытых систем с небольшим количеством пользователей каждая пара пользователей может заранее разделить его между собой. В больших распределенных системах, применяющих технологию симметричного шифрования, часто используются протоколы аутентификации с участием доверенного сервера, с которым каждая сторона разделяет знание ключа. Такой сервер распределяет сеансовые ключи для каждой пары пользователей всякий раз, когда один из них запрашивает аутентификацию другого. Кажущаяся простота данного подхода является обманчивой, на самом деле разработка протоколов аутентификации этого типа является сложной и с точки зрения безопасности не очевидной.

Протоколы аутентификации с симметричными алгоритмами шифрования

Ниже приводятся три примера протоколов аутентификации, специфицированных в ISO/IEC 9798-2. Эти протоколы предполагают предварительное распределение разделяемых секретных ключей [54, 62].

Рассмотрим следующие варианты аутентификации:

- односторонняя аутентификация с использованием меток времени;
- односторонняя аутентификация с использованием случайных чисел;
- двусторонняя аутентификация.

В каждом из этих случаев пользователь доказывает свою подлинность, демонстрируя знание секретного ключа, так как производит расшифровывание запросов с помощью этого секретного ключа.

При использовании в процессе аутентификации симметричного шифрования необходимо также реализовать механизмы обеспечения целостности передаваемых данных на основе общепринятых способов.

Введем следующие обозначения:

r_A — случайное число, сгенерированное участником A;

r_B — случайное число, сгенерированное участником B;

t_A — метка времени, сгенерированная участником A;

E_K — симметричное шифрование на ключе K (ключ K должен быть предварительно распределен между A и B).

1. Односторонняя аутентификация, основанная на метках времени:

$$A \rightarrow B\colon E_K(t_A, B). \qquad (1)$$

После получения и расшифровывания данного сообщения участник B убеждается в том, что метка времени t_A действительна и идентификатор B, указанный в сообщении, совпадает с его собственным. Предотвращение повторной передачи данного сообщения основывается на том, что без знания ключа невозможно изменить метку времени t_A и идентификатор B.

2. Односторонняя аутентификация, основанная на использовании случайных чисел:

$$A \leftarrow B\colon r_B; \qquad (1)$$

$$A \rightarrow B\colon E_K(r_B, B). \qquad (2)$$

Участник B отправляет участнику A случайное число r_B. Участник A шифрует сообщение, состоящее из полученного числа r_B и идентификатора B, и отправляет зашифрованное сообщение участнику B. Участник B расшифровывает полученное сообщение и сравнивает случайное число, содержащееся в сообщении,

с тем, которое он послал участнику *A*. Дополнительно он проверяет имя, указанное в сообщении.

3. Двусторонняя аутентификация, использующая случайные значения:

$$A \leftarrow B\text{: } r_B; \quad (1)$$

$$A \rightarrow B\text{: } E_K(r_A, r_B, B); \quad (2)$$

$$A \leftarrow B\text{: } E_K(r_A, r_B); \quad (3)$$

При получении сообщения (2) участник *B* выполняет те же проверки, что и в предыдущем протоколе, и дополнительно расшифровывает случайное число r_A для включения его в сообщение (3) для участника *A*. Сообщение (3), полученное участником *A*, позволяет ему убедиться на основе проверки значений r_A и r_B, что он имеет дело именно с участником *B*.

Широко известными представителями протоколов, обеспечивающих аутентификацию пользователей с привлечением в процессе аутентификации третьей стороны, являются протокол распределения секретных ключей Нидхэма и Шредера и протокол Kerberos.

Протоколы, основанные на использовании однонаправленных ключевых хэш-функций

Протоколы, представленные выше, могут быть модифицированы путем замены симметричного шифрования на шифрование с помощью односторонней ключевой хэш-функции [45, 62]. Это бывает необходимо, если алгоритмы блочного шифрования недоступны или не отвечают предъявляемым требованиям (например, в случае экспортных ограничений).

Своеобразие шифрования с помощью односторонней хэш-функции заключается в том, что оно по существу является односторонним, т. е. не сопровождается обратным преобразованием — расшифровыванием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования [45].

Односторонняя хэш-функция $h_K(\cdot)$ с параметром-ключом *K*, примененная к шифруемым данным *M*, дает в результате хэш-значение *m* (дайджест), состоящее из фиксированного небольшого числа байт (рис. 7.3). Дайджест $m = h_K(M)$ передается

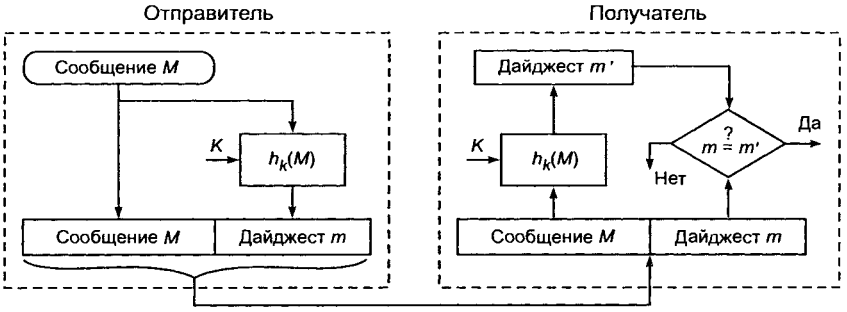


Рис. 7.3. Применение для аутентификации односторонней хэш-функции с параметром-ключом

получателю вместе с исходным сообщением *M*. Получатель сообщения, зная, какая односторонняя хэш-функция была применена для получения дайджеста, заново вычисляет ее, используя расшифрованное сообщение *M*. Если значения полученного дайджеста *m* и вычисленного дайджеста *m'* совпадают, значит содержимое сообщения *M* не было подвергнуто никаким изменениям.

Знание дайджеста не дает возможности восстановить исходное сообщение, но позволяет проверить целостность данных. Дайджест можно рассматривать как своего рода контрольную сумму для исходного сообщения. Однако между дайджестом и обычной контрольной суммой имеется и существенное различие. Контрольную сумму используют как средство проверки целостности передаваемых сообщений по ненадежным линиям связи. Это средство проверки не рассчитано на борьбу со злоумышленниками, которым в такой ситуации ничто не мешает подменить сообщение, добавив к нему новое значение контрольной суммы. Получатель в таком случае не заметит никакой подмены.

В отличие от обычной контрольной суммы при вычислении дайджеста применяются секретные ключи. В случае, если для получения дайджеста используется односторонняя хэш-функция с параметром-ключом *K*, который известен только отправителю и получателю, любая модификация исходного сообщения будет немедленно обнаружена.

На рис. 7.4 показан другой вариант использования односторонней хэш-функции для проверки целостности данных. В этом случае односторонняя хэш-функция $h(\cdot)$ не имеет параметра-ключа, но применяется не просто к сообщению *M*, а к сообщению, дополненному секретным ключом *K*, т. е. отправитель

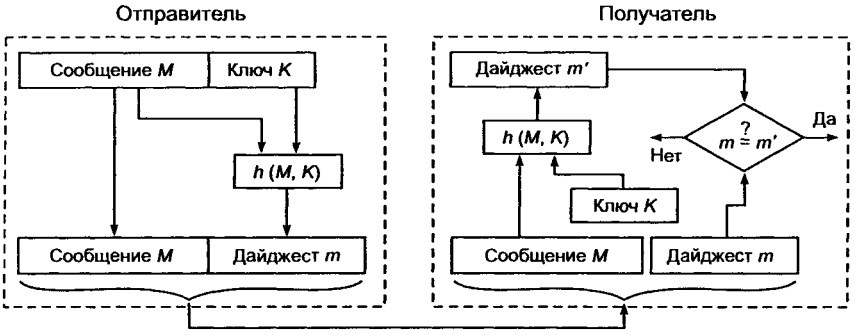


Рис. 7.4. Применение односторонней хэш-функции к сообщению, дополненному секретным ключом K

вычисляет дайджест $m = h(M, K)$. Получатель, извлекая исходное сообщение M, также дополняет его тем же известным ему секретным ключом K, после чего применяет к полученным данным одностороннюю хэш-функцию $h(\cdot)$. Результат вычислений — дайджест m' — сравнивается с полученным по сети дайджестом m.

При использовании односторонних функций шифрования в рассмотренные выше протоколы необходимо внести следующие изменения:

- функция симметричного шифрования E_K заменяется функцией h_K;
- проверяющий вместо установления факта совпадения полей в расшифрованных сообщениях с предполагаемыми значениями вычисляет значение однонаправленной функции и сравнивает его с полученным от другого участника обмена информацией;
- для обеспечения независимого вычисления значения однонаправленной функции получателем сообщения в протоколе 1 метка времени t_A должна передаваться дополнительно в открытом виде, а в сообщении (2) протокола 3 случайное число r_A должно передаваться дополнительно в открытом виде.

Модифицированный вариант протокола 3 с учетом сформулированных изменений имеет следующую структуру:

$$A \leftarrow B\colon r_B; \tag{1}$$

$$A \rightarrow B\colon r_A,\ h_K(r_A, r_B, B); \tag{2}$$

$$A \leftarrow B\colon h_K(r_A, r_B, A). \tag{3}$$

Заметим, что в сообщение (3) протокола включено поле A. Результирующий протокол обеспечивает взаимную аутентификацию и известен как протокол SKID 3 [54, 62].

7.3.3. Строгая аутентификация, основанная на асимметричных алгоритмах

В протоколах строгой аутентификации могут быть использованы асимметричные алгоритмы с открытыми ключами. В этом случае доказывающий может продемонстрировать знание секретного ключа одним из следующих способов:

- расшифровать запрос, зашифрованный на открытом ключе;
- поставить свою цифровую подпись на запросе [54, 62].

Пара ключей, необходимая для аутентификации, не должна использоваться для других целей (например, для шифрования) по соображениям безопасности. Важно отметить, что выбранная система с открытым ключом должна быть устойчивой к атакам с выборкой шифрованного текста даже в том случае, если нарушитель пытается получить критичную информацию, выдавая себя за проверяющего и действуя от его имени.

Аутентификация с использованием асимметричных алгоритмов шифрования

В качестве примера протокола, построенного на использовании асимметричного алгоритма шифрования, можно привести следующий протокол аутентификации:

$$A \leftarrow B\colon h(r),\ B,\ P_A(r,\ B); \qquad (1)$$

$$A \rightarrow B\colon r. \qquad (2)$$

Участник B выбирает случайным образом r и вычисляет значение $x = h(r)$ (значение x демонстрирует знание r без раскрытия самого значения r), далее он вычисляет значение $e = P_A(r, B)$. Под P_A подразумевается алгоритм асимметричного шифрования (например, RSA), а под $h(\cdot)$ — хэш-функция. Участник B отправляет сообщение (1) участнику A. Участник A расшифровывает $e = P_A(r, B)$ и получает значения r_1 и B_1, а также вычисляет

$x_1 = h(r_1)$. После этого производится ряд сравнений, доказывающих, что $x = x_1$ и что полученный идентификатор B_1 действительно указывает на участника *B*. В случае успешного проведения сравнения участник *A* посылает *r*. Получив его, участник *B* проверяет, то ли это значение, которое он отправил в сообщении (1).

В качестве другого примера приведем модифицированный протокол Нидхэма и Шредера, основанный на асимметричном шифровании (достаточно подробно он описан в разделе, посвященном распределению ключевой информации, поскольку основной вариант протокола используется для аутентификационного обмена ключевой информации).

Рассматривая вариант протокола Нидхэма и Шредера, используемый только для аутентификации, будем подразумевать под P_B алгоритм шифрования открытым ключом участника *B*. Протокол имеет следующую структуру:

$$A \rightarrow B\text{: } P_B(r_1, A); \quad (1)$$

$$A \leftarrow B\text{: } P_A(r_2, r_1); \quad (2)$$

$$A \leftarrow B\text{: } r_2. \quad (3)$$

Аутентификация, основанная на использовании цифровой подписи

В рекомендациях стандарта X.509 специфицирована схема аутентификации, основанная на использовании цифровой подписи, меток времени и случайных чисел.

Для описания этой схемы аутентификации введем следующие обозначения:

t_A, r_A и r_B — временная метка и случайные числа соответственно;

S_A — подпись, сгенерированная участником *A*;

S_B — подпись, сгенерированная участником *B*;

cert_A — сертификат открытого ключа участника *A*;

cert_B — сертификат открытого ключа участника *B*.

Если участники имеют аутентичные открытые ключи, полученные друг от друга, то можно не пользоваться сертификатами, в противном случае они служат для подтверждения подлинности открытых ключей.

В качестве примеров приведем следующие протоколы аутентификации.

1. Односторонняя аутентификация с применением меток времени:

$$A \rightarrow B\text{: } \mathrm{cert}_A,\ t_A,\ B,\ S_A(t_A,\ B). \qquad (1)$$

После принятия данного сообщения участник B проверяет правильность метки времени t_A, полученный идентификатор B и, используя открытый ключ из сертификата cert_A, корректность цифровой подписи $S_A(t_A,\ B)$.

2. Односторонняя аутентификация с использованием случайных чисел:

$$A \leftarrow B\text{: } r_B; \qquad (1)$$

$$A \rightarrow B\text{: } \mathrm{cert}_A,\ r_A,\ B,\ S_A(r_A,\ r_B,\ B). \qquad (2)$$

Участник B, получив сообщение от участника A, убеждается, что именно он является адресатом сообщения; используя открытый ключ участника A, взятый из сертификата cert_A, проверяет корректность подписи $S_A(r_A,\ r_B,\ B)$ под числом r_A, полученным в открытом виде, числом r_B, которое было отослано в сообщении (1), и его идентификатором B. Подписанное случайное число r_A используется для предотвращения атак с выборкой открытого текста.

3. Двусторонняя аутентификация с использованием случайных чисел:

$$A \leftarrow B\text{: } r_B; \qquad (1)$$

$$A \rightarrow B\text{: } \mathrm{cert}_A,\ r_A,\ B,\ S_A(r_A,\ r_B,\ B); \qquad (2)$$

$$A \leftarrow B\text{: } \mathrm{cert}_B,\ A,\ S_B(r_A,\ r_B,\ A). \qquad (3)$$

В данном протоколе обработка сообщений (1) и (2) выполняется так же, как и в предыдущем протоколе, а сообщение (3) обрабатывается аналогично сообщению (2).

7.4. Биометрическая аутентификация пользователя

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, персональный идентифика-

тор, секретный ключ и т. п.). В последнее время все большее распространение получает *биометрическая аутентификация пользователя*, позволяющая уверенно аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

Основные достоинства биометрических методов:

- высокая степень достоверности аутентификации по биометрическим признакам (из-за их уникальности);
- неотделимость биометрических признаков от дееспособной личности;
- трудность фальсификации биометрических признаков.

Активно используются следующие биометрические признаки:

- отпечатки пальцев;
- геометрическая форма кисти руки;
- форма и размеры лица;
- особенности голоса;
- узор радужной оболочки и сетчатки глаз.

Рассмотрим типичную схему функционирования биометрической подсистемы аутентификации. При регистрации в системе пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой как контрольный «образ» (биометрическая подпись) законного пользователя. Этот образ пользователя хранится системой в электронной форме и используется для проверки идентичности каждого, кто выдает себя за соответствующего законного пользователя. В зависимости от совпадения или несовпадения совокупности предъявленных признаков с зарегистрированными в контрольном образе предъявивший их признается законным пользователем (при совпадении) или незаконным (при несовпадении).

С точки зрения потребителя, эффективность биометрической аутентификационной системы характеризуется двумя параметрами:

- коэффициентом ошибочных отказов FRR (false-reject rate);
- коэффициентом ошибочных подтверждений FAR (false-alarm rate).

Ошибочный отказ возникает, когда система не подтверждает личность законного пользователя (типичные значения FRR — порядка одной ошибки на 100). *Ошибочное подтверждение* происходит в случае подтверждения личности незаконного пользователя (типичные значения FAR — порядка одной ошибки

на 10 000). Эти коэффициенты связаны друг с другом: каждому коэффициенту ошибочных отказов соответствует определенный коэффициент ошибочных подтверждений.

В совершенной биометрической системе оба параметра ошибки должны быть равны нулю. К сожалению, биометрические системы тоже не идеальны. Обычно системные параметры настраивают так, чтобы добиться требуемого коэффициента ошибочных подтверждений, что определяет соответствующий коэффициент ошибочных отказов.

К настоящему времени разработаны и продолжают совершенствоваться технологии аутентификации по отпечаткам пальцев, радужной оболочке глаза, по форме кисти руки и ладони, по форме и размеру лица, по голосу и «клавиатурному почерку».

Чаще всего биометрические системы используют в качестве параметра идентификации отпечатки пальцев (дактилоскопические системы аутентификации). Такие системы просты и удобны, обладают высокой надежностью аутентификации.

Дактилоскопические системы аутентификации. Одна из основных причин широкого распространения таких систем — наличие больших банков данных отпечатков пальцев. Пользователями подобных систем главным образом являются полиция, различные государственные и некоторые банковские организации.

В общем случае биометрическая технология распознавания отпечатков пальцев заменяет защиту доступа с использованием пароля. Большинство систем используют отпечаток одного пальца.

Основными элементами дактилоскопической системы аутентификации являются:

- сканер;
- ПО идентификации, формирующее идентификатор пользователя;
- ПО аутентификации, производящее сравнение отсканированного отпечатка пальца с имеющимися в БД «паспортами» пользователей.

Дактилоскопическая система аутентификации работает следующим образом. Сначала проходит регистрация пользователя. Как правило, производится несколько вариантов сканирования в разных положениях пальца на сканере. Понятно, что образцы будут немного отличаться, и поэтому требуется сформировать некоторый обобщенный образец — «паспорт». Результаты запоминаются в БД аутентификации. При аутентификации произво-

дится сравнение отсканированного отпечатка пальца с «паспортами», хранящимися в БД.

Задача формирования «паспорта» и задача распознавания предъявляемого образца — это задачи распознавания образов. Для их решения используются различные алгоритмы, являющиеся ноу-хау фирм-производителей подобных устройств.

Сканеры отпечатков пальцев. Многие производители все чаще переходят от дактилоскопического оборудования на базе оптики к продуктам, основанным на интегральных схемах. Последние имеют значительно меньшие размеры, чем оптические считыватели, и поэтому их проще реализовать в широком спектре периферийных устройств.

Некоторые производители комбинируют биометрические системы со смарт-картами и картами-ключами. Например, в биометрической идентификационной смарт-карте Authentic реализован следующий подход. Образец отпечатка пальца пользователя запоминается в памяти карты в процессе внесения в списки идентификаторов пользователей, устанавливая соответствие между образцом и личным ключом шифрования. Затем, когда пользователь вводит смарт-карту в считыватель и прикладывает палец к сенсору, ключ удостоверяет его личность. Комбинация биометрических устройств и смарт-карт является удачным решением, повышающим надежность процессов аутентификации и авторизации.

Небольшой размер и невысокая цена датчиков отпечатков пальцев на базе интегральных схем превращает их в идеальный интерфейс для систем защиты. Их можно встроить в брелок для ключей, и пользователи получат универсальный ключ, который обеспечит защищенный доступ ко всему, начиная от компьютеров до входных дверей, дверей автомобилей и банкоматов.

Системы аутентификации по форме ладони используют сканеры формы ладони, обычно устанавливаемые на стенах. Следует отметить, что подавляющее большинство пользователей предпочитают системы этого типа.

Устройства считывания формы ладони создают объемное изображение ладони, измеряя длину пальцев, толщину и площадь поверхности ладони. Например, продукты компании Recognition Systems выполняют более 90 измерений, которые преобразуются в 9-разрядный образец для дальнейших сравнений. Этот образец может быть сохранен локально, на индивидуальном сканере ладони либо в централизованной БД.

По уровню доходов устройства сканирования формы ладони, занимают 2-е место среди биометрических устройств, но редко применяются в сетевой среде из-за высокой стоимости и размера. Однако сканеры формы ладони хорошо подходят для вычислительных сред со строгим режимом безопасности и напряженным трафиком, включая серверные комнаты. Они достаточно точны и обладают довольно низким коэффициентом ошибочного отказа FRR.

Системы аутентификации по лицу и голосу наиболее доступны из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства. Системы данного класса применяются при удаленной идентификации субъекта доступа в телекоммуникационных сетях.

Технология сканирования черт лица подходит для тех приложений, где прочие биометрические технологии непригодны. В этом случае для идентификации и верификации личности используются особенности глаз, носа и губ. Производители устройств распознавания черт лица применяют собственные математические алгоритмы для идентификации пользователей

Исследования, проводимые компанией International Biometric Group, говорят о том, что сотрудники многих организаций не доверяют устройствам распознавания по чертам лица. Кроме того, по данным этой компании, сканирование черт лица — единственный метод биометрической аутентификации, который не требует согласия на выполнение проверки (и может осуществляться скрытой камерой), а потому имеет негативный для пользователей подтекст.

Следует отметить, что технологии распознавания черт лица требуют дальнейшего совершенствования. Большая часть алгоритмов распознавания черт лица чувствительна к колебаниям в освещении, вызванным изменением интенсивности солнечного света в течение дня. Изменение положения лица также может повлиять на узнаваемость. Различие в положении в 15 % между запрашиваемым изображением и изображением, которое находится в БД, напрямую сказывается на эффективности: при различии в 45° распознавание становится неэффективным.

Системы аутентификации по голосу экономически выгодны по тем же причинам, что и системы распознавания по чертам лица. В частности, их можно устанавливать с оборудованием (например, микрофонами), поставляемым в стандартной комплектации со многими ПК.

Системы аутентификации по голосу при записи образца и в процессе последующей идентификации опираются на такие особенности голоса, как высота, модуляция и частота звука. Эти показатели определяются физическими характеристиками голосового тракта и уникальны для каждого человека. Распознавание голоса применяется вместо набора номера в определенных системах Sprint. Технология распознавания голоса отличается от распознавания речи: последняя интерпретирует то, что говорит абонент, а технология распознавания голоса абонента подтверждает личность говорящего.

Поскольку голос можно просто записать на пленку или другие носители, некоторые производители встраивают в свои продукты операцию запроса отклика. Эта функция предлагает пользователю при входе ответить на предварительно подготовленный и регулярно меняющийся запрос, например такой: «Повторите числа 0, 1, 3».

Оборудование аутентификации по голосу более пригодно для интеграции в приложения телефонии, чем для входа в сеть. Обычно оно позволяет абонентам получить доступ в финансовые или прочие системы посредством телефонной связи.

Технологии распознавания говорящего имеют некоторые ограничения. Различные люди могут говорить похожими голосами, а голос любого человека может меняться со временем в зависимости от самочувствия, эмоционального состояния и возраста. Более того, разница в модификации телефонных аппаратов и качество телефонных соединений могут серьезно усложнить распознавание.

Поскольку голос сам по себе не обеспечивает достаточной точности, распознавание по голосу следует сочетать с другими биометриками, такими как распознавание черт лица или отпечатков пальцев.

Системы аутентификации по узору радужной оболочки и сетчатки глаз могут быть разделены на два класса:

- использующие рисунок радужной оболочки глаза;
- использующие рисунок кровеносных сосудов сетчатки глаза.

Сетчатка человеческого глаза представляет собой уникальный объект для аутентификации. Рисунок кровеносных сосудов глазного дна отличается даже у близнецов. Поскольку вероятность повторения параметров радужной оболочки и сетчатки глаза имеет порядок 10^{-78}, такие системы являются наиболее на-

дежными среди всех биометрических систем и применяются там, где требуется высокий уровень безопасности (например, в режимных зонах военных и оборонных объектов).

Биометрический подход позволяет упростить процесс выяснения «кто есть кто». При использовании дактилоскопических сканеров и устройств распознавания голоса для входа в сети сотрудники избавляются от необходимости запоминать сложные пароли. Ряд компаний интегрируют биометрические возможности в системы однократной аутентификации SSO (Single Sign-On) масштаба предприятия. Подобная консолидация позволяет сетевым администраторам заменить службы однократной аутентификации паролей биометрическими технологиями.

Биометрическая аутентификация пользователя может быть использована при *шифровании* в виде модулей блокировки доступа к секретному ключу, который позволяет воспользоваться этой информацией только истинному владельцу частного ключа. Владелец может затем применять свой секретный ключ для шифрования информации, передаваемой по частным сетям или по Internet. Ахиллесовой пятой многих систем шифрования является проблема безопасного хранения самого криптографического секретного ключа. Зачастую доступ к ключу длиной 128 разрядов (или даже больше) защищен лишь паролем из 6 символов, т. е. 48 разрядов. Отпечатки пальцев обеспечивают намного более высокий уровень защиты и, в отличие от пароля, их невозможно забыть.

Часть 3
ТЕХНОЛОГИИ ЗАЩИТЫ МЕЖСЕТЕВОГО ОБМЕНА ДАННЫМИ

Развитие глобальных компьютерных сетей, появление новых перспективных информационных технологий (ИТ) привлекают все большее внимание. Глобальные сети применяются для передачи коммерческой информации различного уровня конфиденциальности, например для связи головной штаб-квартиры организации с удаленными офисами или создания Web-сайтов организации с размещенной на них рекламой и деловыми предложениями. Многие организации принимают решение о подключении своих локальных и корпоративных сетей к открытой глобальной сети.

Однако подключение к открытой глобальной сети может иметь и негативные последствия, поскольку появляются угрозы неправомерного вторжения из внешней сети во внутреннюю сеть. Такое вторжение может выполняться как с целью несанкционированного использования ресурсов внутренней сети, например хищения информации, так и с целью нарушения ее работоспособности. Количество уязвимостей сетевых ОС, прикладных программ и возможных атак на КИС постоянно растет. Без соответствующих средств защиты вероятность успешной реализации таких угроз является достаточно высокой.

Ежегодные потери, обусловленные недостаточным уровнем защищенности компьютерных сетей организаций, оцениваются миллиардами долларов. Поэтому при подключении к Internet локальной или корпоративной сети необходимо позаботиться об обеспечении информационной безопасности этой сети.

Проблема защиты от несанкционированных действий при взаимодействии с внешними сетями может быть успешно решена только на основе комплексной защиты корпоративных компьютерных сетей. К базовым средствам многоуровневой защиты межсетевого обмена данными относятся защищенные ОС, МЭ, виртуальные защищенные сети VPN, протоколы защиты на канальном, транспортном и сетевом (протокол IPSec) уровнях.

Глава 8
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ

8.1. Проблемы обеспечения безопасности ОС

Большинство программных средств защиты информации являются прикладными программами. Для их выполнения требуется поддержка ОС. Окружение, в котором функционирует ОС, называется *доверенной вычислительной базой* (ДВБ). ДВБ включает в себя полный набор элементов, обеспечивающих информационную безопасность: ОС, программы, сетевое оборудование, средства физической защиты и даже организационные процедуры. Краеугольным камнем этой пирамиды является защищенная ОС.

8.1.1. Угрозы безопасности ОС

Организация эффективной и надежной защиты ОС невозможна без предварительного анализа возможных угроз ее безопасности. Угрозы безопасности ОС существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается в системе, и т. д. Например, если ОС используется для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом (НСД) к файлам. Если же ОС используется как платформа провайдера Internet-услуг, очень опасны атаки на сетевое программное обеспечение ОС.

Угрозы безопасности ОС можно классифицировать по различным аспектам их реализации [56].

1. По *цели атаки*:
   - несанкционированное чтение информации;
   - несанкционированное изменение информации;
   - несанкционированное уничтожение информации;
   - полное или частичное разрушение ОС.
2. По *принципу воздействия на операционную систему*:
   - использование известных (легальных) каналов получения информации; например угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно, т. е. разрешен доступ пользователю, которому согласно политике безопасности доступ должен быть запрещен;
   - использование скрытых каналов получения информации; например угроза использования злоумышленником недокументированных возможностей ОС;
   - создание новых каналов получения информации с помощью программных закладок.
3. По *типу используемой злоумышленником уязвимости защиты*:
   - неадекватная политика безопасности, в том числе и ошибки администратора системы;
   - ошибки и недокументированные возможности программного обеспечения ОС, в том числе и так называемые *люки* — случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты;
   - ранее внедренная программная закладка.
4. По *характеру воздействия на операционную систему*:
   - активное воздействие — несанкционированные действия злоумышленника в системе;
   - пассивное воздействие — несанкционированное наблюдение злоумышленника за процессами, происходящими в системе.

Угрозы безопасности ОС можно также классифицировать по таким признакам, как: способ действий злоумышленника, используемые средства атаки, объект атаки, способ воздействия на объект атаки, состояние атакуемого объекта ОС на момент атаки.

ОС может подвергнуться следующим типичным атакам:

- *сканированию файловой системы.* Злоумышленник просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В ре-

зультате злоумышленник получает доступ к информации, который должен быть ему запрещен;

- *подбору пароля.* Существуют несколько методов подбора паролей пользователей:
  - тотальный перебор;
  - тотальный перебор, оптимизированный по статистике встречаемости символов или с помощью словарей;
  - подбор пароля с использованием знаний о пользователе (его имени, фамилии, даты рождения, номера телефона и т. д.);
- *краже ключевой информации.* Злоумышленник может подсмотреть пароль, набираемый пользователем, или восстановить набираемый пользователем пароль по движениям его рук на клавиатуре. Носитель с ключевой информацией (смарт-карта, Touch Memory и т. д.) может быть просто украден;
- *сборке мусора.* Во многих ОС информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый *мусор*). Злоумышленник восстанавливает эту информацию, просматривает ее и копирует интересующие его фрагменты;
- *превышению полномочий.* Злоумышленник, используя ошибки в программном обеспечении ОС или политике безопасности, получает полномочия, превышающие те, которые ему предоставлены в соответствии с политикой безопасности. Обычно это достигается путем запуска программы от имени другого пользователя;
- *программным закладкам.* Программные закладки, внедряемые в ОС, не имеют существенных отличий от других классов программных закладок;
- *жадным программам* — это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху ОС [56].

8.1.2. Понятие защищенной ОС

Операционную систему называют *защищенной,* если она предусматривает средства защиты от основных классов угроз. Защищенная ОС обязательно должна содержать средства разграниче-

ния доступа пользователей к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с ОС. Кроме того, защищенная ОС должна содержать средства противодействия случайному или преднамеренному выводу ОС из строя.

Если ОС предусматривает защиту не от всех основных классов угроз, а только от некоторых, такую ОС называют *частично защищенной* [56, 88].

Подходы к построению защищенных ОС

Существуют два основных подхода к созданию защищенных ОС — фрагментарный и комплексный. При *фрагментарном* подходе вначале организуется защита от одной угрозы, затем от другой и т. д. Примером фрагментарного подхода может служить ситуация, когда за основу берется незащищенная ОС (например, Windows 98), на нее устанавливаются антивирусный пакет, система шифрования, система регистрации действий пользователей и т. д.

При применении фрагментарного подхода подсистема защиты ОС представляет собой набор разрозненных программных продуктов, как правило, от разных производителей. Эти программные средства работают независимо друг от друга, при этом практически невозможно организовать их тесное взаимодействие. Кроме того, отдельные элементы такой подсистемы защиты могут некорректно работать в присутствии друг друга, что приводит к резкому снижению надежности системы.

При *комплексном* подходе защитные функции вносятся в ОС на этапе проектирования архитектуры ОС и являются ее неотъемлемой частью. Отдельные элементы подсистемы защиты, созданной на основе комплексного подхода, тесно взаимодействуют друг с другом при решении различных задач, связанных с организацией защиты информации, поэтому конфликты между ее отдельными компонентами практически невозможны. Подсистема защиты, созданная на основе комплексного подхода, может быть устроена так, что при фатальных сбоях в функционировании ее ключевых элементов она вызывает крах ОС, что не позволяет злоумышленнику отключать защитные функции системы. При фрагментарном подходе такая организация подсистемы защиты невозможна.

Как правило, подсистему защиты ОС, созданную на основе комплексного подхода, проектируют так, чтобы отдельные ее элементы были заменяемы. Соответствующие программные модули могут быть заменены другими модулями.

Административные меры защиты

Программно-аппаратные средства защиты ОС обязательно должны дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже надежная программно-аппаратная защита может давать сбои. Перечислим основные административные меры защиты.

1. *Постоянный контроль корректности функционирования ОС*, особенно ее подсистемы защиты. Такой контроль удобно организовать, если ОС поддерживает автоматическую регистрацию наиболее важных событий (*event logging*) в специальном журнале.

2. *Организация и поддержание адекватной политики безопасности.* Политика безопасности ОС должна постоянно корректироваться, оперативно реагируя на попытки злоумышленников преодолеть защиту ОС, а также на изменения в конфигурации ОС, установку и удаление прикладных программ.

3. *Инструктирование пользователей операционной системы* о необходимости соблюдения мер безопасности при работе с ОС и контроль за соблюдением этих мер.

4. *Регулярное создание и обновление резервных копий* программ и данных ОС.

5. *Постоянный контроль изменений в конфигурационных данных и политике безопасности ОС.* Информацию об этих изменениях целесообразно хранить на неэлектронных носителях информации, для того чтобы злоумышленнику, преодолевшему защиту ОС, было труднее замаскировать свои несанкционированные действия.

В конкретных ОС могут потребоваться и другие административные меры защиты информации [56].

Адекватная политика безопасности

Выбор и поддержание адекватной политики безопасности являются одной из наиболее важных задач администратора ОС. Если принятая в ОС политика безопасности неадекватна, то это

может привести к НСД злоумышленника к ресурсам системы и к снижению надежности функционирования ОС.

Известно утверждение: чем лучше защищена ОС, тем труднее с ней работать пользователям и администраторам. Это обусловлено следующими факторами:

- система защиты не всегда способна определить, является ли некоторое действие пользователя злонамеренным. Поэтому система защиты либо не пресекает некоторые виды НСД, либо запрещает некоторые вполне легальные действия пользователей. Чем выше защищенность системы, тем шире класс тех легальных действий пользователей, которые рассматриваются подсистемой защиты как несанкционированные;
- любая система, в которой предусмотрены функции защиты информации, требует от администраторов определенных усилий, направленных на поддержание адекватной политики безопасности. Чем больше в ОС защитных функций, тем больше времени и средств нужно тратить на поддержание защиты;
- подсистема защиты ОС, как и любой другой программный пакет, потребляет аппаратные ресурсы компьютера. Чем сложнее устроены защитные функции ОС, тем больше ресурсов компьютера (процессорного времени, оперативной памяти и др.) затрачивается на поддержание функционирования подсистемы защиты и тем меньше ресурсов остается на долю прикладных программ;
- поддержание слишком жесткой политики безопасности может негативно сказаться на надежности функционирования ОС. Чрезмерно жесткая политика безопасности может привести к трудно выявляемым ошибкам и сбоям в процессе функционирования ОС и даже к ее краху [56, 88].

Оптимальная адекватная политика безопасности — это такая политика безопасности, которая не только не позволяет злоумышленникам выполнять несанкционированные действия, но и не приводит к описанным выше негативным эффектам.

Адекватная политика безопасности определяется не только архитектурой ОС, но и ее конфигурацией, установленными прикладными программами и т. д. Формирование и поддержание адекватной политики безопасности ОС можно разделить на ряд этапов.

1. *Анализ угроз.* Администратор ОС рассматривает возможные угрозы безопасности данного экземпляра ОС. Среди возможных угроз выделяются наиболее опасные, защите от которых нужно уделять максимум средств.

2. *Формирование требований к политике безопасности.* Администратор определяет, какие средства и методы будут применяться для защиты от тех или иных угроз. Например, защиту от НСД к некоторому объекту ОС можно решать либо средствами разграничения доступа, либо криптографическими средствами, либо используя некоторую комбинацию этих средств.

3. *Формальное определение политики безопасности.* Администратор определяет, как конкретно должны выполняться требования, сформулированные на предыдущем этапе. Формулируются необходимые требования к конфигурации ОС, а также требования к конфигурации дополнительных пакетов защиты, если установка таких пакетов необходима. Результатом данного этапа является развернутый перечень настроек конфигурации ОС и дополнительных пакетов защиты с указанием того, в каких ситуациях, какие настройки должны быть установлены.

4. *Претворение в жизнь политики безопасности.* Задачей данного этапа является приведение конфигурации ОС и дополнительных пакетов защиты в соответствие с политикой безопасности, формально определенной на предыдущем этапе.

5. *Поддержание и коррекция политики безопасности.* В задачу администратора на данном этапе входит контроль соблюдения политики безопасности и внесение в нее необходимых изменений по мере появления изменений в функционировании ОС.

Специальных стандартов защищенности ОС не существует. Для оценки защищенности ОС используются стандарты, разработанные для компьютерных систем вообще. Как правило, сертификация ОС по некоторому классу защиты сопровождается составлением требований к адекватной политике безопасности, при безусловном выполнении которой защищенность конкретного экземпляра ОС будет соответствовать требованиям соответствующего класса защиты.

Определяя адекватную политику безопасности, администратор ОС должен в первую очередь ориентироваться на защиту ОС от конкретных угроз ее безопасности [56, 88].

8.2. Архитектура подсистемы защиты ОС

8.2.1. Основные функции подсистемы защиты ОС

Подсистема защиты ОС выполняет следующие основные функции.

1. Идентификация и аутентификация. Ни один пользователь не может начать работу с ОС, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.

2. Разграничение доступа. Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.

3. Аудит. ОС регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

4. *Управление политикой безопасности.* Политика безопасности должна постоянно поддерживаться в адекватном состоянии, т. е. должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в ОС.

5. Криптографические функции. Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.

6. Сетевые функции. Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе и задач, имеющих прямое отношение к защите информации.

Подсистема защиты обычно не представляет собой единый программный модуль. Как правило, каждая из перечисленных функций подсистемы защиты решается одним или несколькими программными модулями. Некоторые функции встраиваются непосредственно в ядро ОС. Между различными модулями подсистемы защиты должен существовать четко определенный ин-

терфейс, используемый при взаимодействии модулей для решения общих задач.

В таких ОС, как Windows XP, подсистема защиты четко выделяется в общей архитектуре ОС, в других, как UNIX, защитные функции распределены практически по всем элементам ОС. Однако любая ОС, удовлетворяющая стандарту защищенности, должна содержать подсистему защиты, выполняющую все вышеперечисленные функции. Обычно подсистема защиты ОС допускает расширение дополнительными программными модулями [56, 88].

8.2.2. Идентификация, аутентификация и авторизация субъектов доступа

В защищенной ОС любой пользователь (субъект доступа), перед тем как начать работу с системой, должен пройти идентификацию, аутентификацию и авторизацию. *Субъектом доступа* (или просто *субъектом*) называют любую сущность, способную инициировать выполнение операций над элементами ОС. В частности, пользователи являются субъектами доступа.

Идентификация субъекта доступа заключается в том, что субъект сообщает ОС *идентифицирующую информацию* о себе (имя, учетный номер и т. д.) и таким образом идентифицирует себя.

Для того чтобы установить, что пользователь именно тот, за кого себя выдает, в информационных системах предусмотрена процедура *аутентификации*, задача которой — предотвращение доступа к системе нежелательных лиц.

Аутентификация субъекта доступа заключается в том, что субъект предоставляет ОС помимо идентифицирующей информации еще и *аутентифицирующую информацию,* подтверждающую, что он действительно является тем субъектом доступа, к которому относится идентифицирующая информация (см. гл. 7).

Авторизация субъекта доступа происходит после успешной идентификации и аутентификации. При авторизации субъекта ОС выполняет действия, необходимые для того, чтобы субъект мог начать работу в системе. Например, авторизация пользователя в операционной системе UNIX включает в себя порождение процесса, являющегося операционной оболочкой, с которой в

дальнейшем будет работать пользователь. В ОС Windows NT авторизация пользователя включает в себя создание маркера доступа пользователя, создание рабочего стола и запуск на нем от имени авторизуемого пользователя процесса Userinit, инициализирующего индивидуальную программную среду пользователя. Авторизация субъекта не относится напрямую к подсистеме защиты ОС. В процессе авторизации решаются технические задачи, связанные с организацией начала работы в системе уже идентифицированного и аутентифицированного субъекта доступа.

С точки зрения обеспечения безопасности ОС процедуры идентификации и аутентификации являются весьма ответственными. Действительно, если злоумышленник сумел войти в систему от имени другого пользователя, он легко получает доступ ко всем объектам ОС, к которым имеет доступ этот пользователь. Если при этом подсистема аудита генерирует сообщения о событиях, потенциально опасных для безопасности ОС, то в журнал аудита записывается не имя злоумышленника, а имя пользователя, от имени которого злоумышленник работает в системе.

Методы идентификации и аутентификации с помощью имени и пароля, внешних носителей ключевой информации, биометрических характеристик пользователей подробно рассмотрены в гл. 7.

8.2.3. Разграничение доступа к объектам ОС

Основными понятиями процесса разграничения доступа к объектам ОС являются объект доступа, метод доступа к объекту и субъект доступа.

Объектом доступа (или просто *объектом*) называют любой элемент ОС, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен. Возможность доступа к объектам ОС определяется не только архитектурой ОС, но и текущей политикой безопасности. Под объектами доступа понимают как ресурсы оборудования (процессор, сегменты памяти, принтер, диски и ленты), так и программные ресурсы (файлы, программы, семафоры), т. е. все то, доступ к чему контролируется. Каждый объект имеет уникальное имя, отличающее его от других объектов в системе, и каждый из них может быть доступен через хорошо определенные и значимые операции.

Методом доступа к объекту называется операция, определенная для объекта. Тип операции зависит от объектов. Например, процессор может только выполнять команды, сегменты памяти могут быть записаны и прочитаны, считыватель магнитных карт может только читать, а для файлов могут быть определены методы доступа «чтение», «запись» и «добавление» (дописывание информации в конец файла).

Субъектом доступа называют любую сущность, способную инициировать выполнение операций над объектами (обращаться к объектам по некоторым методам доступа). Обычно полагают, что множество субъектов доступа и множество объектов доступа не пересекаются. Иногда к субъектам доступа относят процессы, выполняющиеся в системе. Однако логичнее считать субъектом доступа именно пользователя, от имени которого выполняется процесс. Естественно, под субъектом доступа подразумевают не физического пользователя, работающего с компьютером, а «логического» пользователя, от имени которого выполняются процессы ОС.

Таким образом, *объект доступа* — это то, к чему осуществляется доступ, *субъект доступа* — это тот, кто осуществляет доступ, и *метод доступа* — это то, как осуществляется доступ.

Для объекта доступа может быть определен *владелец* — субъект, которому принадлежит данный объект и который несет ответственность за конфиденциальность содержащейся в объекте информации, а также за целостность и доступность объекта.

Обычно владельцем объекта автоматически назначается субъект, создавший данный объект, в дальнейшем владелец объекта может быть изменен с использованием соответствующего метода доступа к объекту. На владельца, как правило, возлагается ответственность за корректное ограничение прав доступа к данному объекту других субъектов.

Правом доступа к объекту называют право на выполнение доступа к объекту по некоторому методу или группе методов. Например, если пользователь имеет возможность читать файл, говорят, что он имеет право на чтение этого файла. Говорят, что субъект имеет некоторую *привилегию,* если он имеет право на доступ по некоторому методу или группе методов ко всем объектам ОС, поддерживающим данный метод доступа.

Разграничением доступа субъектов к объектам является совокупность правил, определяющая для каждой тройки субъект—объект—метод, разрешен ли доступ данного субъекта к дан-

ному объекту по данному методу. При избирательном разграничении доступа возможность доступа определена однозначно для каждой тройки субъект—объект—метод, при полномочном разграничении доступа ситуация несколько сложнее.

Субъекта доступа называют *суперпользователем,* если он имеет возможность игнорировать правила разграничения доступа к объектам.

Правила разграничения доступа, действующие в ОС, устанавливаются администраторами системы при определении текущей политики безопасности. За соблюдением этих правил субъектами доступа следит *монитор ссылок* — часть подсистемы защиты ОС.

Правила разграничения доступа должны удовлетворять следующим требованиям.

1. Соответствовать аналогичным правилам, принятым в организации, в которой установлена ОС. Иными словами, если согласно правилам организации доступ пользователя к некоторой информации считается несанкционированным, этот доступ должен быть ему запрещен.

2. Не должны допускать разрушающие воздействия субъектов доступа на ОС, выражающиеся в несанкционированном изменении, удалении или другом воздействии на объекты, жизненно важные для нормальной работы ОС.

3. Любой объект доступа должен иметь владельца. Недопустимо присутствие *ничейных объектов* — объектов, не имеющих владельца.

4. Не допускать присутствия *недоступных объектов* — объектов, к которым не может обратиться ни один субъект доступа ни по одному методу доступа.

5. Не допускать утечки конфиденциальной информации.

Существуют две **основные модели разграничения доступа**:

- избирательное (дискреционное) разграничение доступа;
- полномочное (мандатное) разграничение доступа.

При *избирательном разграничении доступа* определенные операции над конкретным ресурсом запрещаются или разрешаются субъектам или группам субъектов. Большинство ОС реализуют именно избирательное разграничение доступа (discretionary access control).

Полномочное разграничение доступа заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уров-

нем допуска к информации. Иногда эту модель называют моделью многоуровневой безопасности, предназначенной для хранения секретов.

Избирательное разграничение доступа

Система правил *избирательного* разграничения доступа формулируется следующим образом.

1. Для любого объекта ОС существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой тройки субъект—объект—метод возможность доступа определена однозначно.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа.

Привилегированный пользователь не может игнорировать разграничение доступа к объектам. Например, в Windows NT администратор для обращения к чужому объекту (принадлежащему другому субъекту) должен сначала объявить себя владельцем этого объекта, использовав привилегию администратора объявлять себя владельцем любого объекта, затем дать себе необходимые права и только после этого может обратиться к объекту. Последнее требование введено для реализации механизма удаления потенциально недоступных объектов.

При создании объекта его владельцем назначается субъект, создавший данный объект. В дальнейшем субъект, обладающий необходимыми правами, может назначить объекту нового владельца. При этом субъект, изменяющий владельца объекта, может назначить новым владельцем объекта только себя. Такое ограничение вводится для того, чтобы владелец объекта не мог отдать «владение» объектом другому субъекту и тем самым снять с себя ответственность за некорректные действия с объектом.

Для определения прав доступа субъектов к объектам при избирательном разграничении доступа используются такие понятия, как *матрица доступа* и *домен безопасности*.

С концептуальной точки зрения текущее состояние прав доступа при избирательном разграничении доступа описывается *матрицей*, в строках которой перечислены субъекты доступа, в столбцах — объекты доступа, а в ячейках — операции, которые субъект может выполнить над объектом.

Домен безопасности (protection domain) определяет набор объектов и типов операций, которые могут производиться над каждым объектом ОС.

Возможность выполнять операции над объектом есть *право доступа*, каждое из которых есть упорядоченная пара <object-name, rights-set>. Таким образом, *домен* есть *набор прав доступа*. Например, если домен *D* имеет право доступа <file *F*, {read, write}>, это означает, что процесс, выполняемый в домене *D*, может читать или писать в файл *F*, но не может выполнять других операций над этим объектом (рис. 8.1).

Домен \ Объект	*F*1	*F*2	*F*3	Printer
*D*1	read		execute	
*D*2		read		
*D*3				print
*D*4	read write		read write	

Рис. 8.1. Специфицирование прав доступа к ресурсам

Связь конкретных субъектов, функционирующих в ОС, может быть организована следующим образом:

- каждый пользователь может быть доменом. В этом случае набор объектов, к которым может быть организован доступ, зависит от идентификации пользователя;
- каждый процесс может быть доменом. В этом случае набор доступных объектов определяется идентификацией процесса;
- каждая процедура может быть доменом. В этом случае набор доступных объектов соответствует локальным переменным, определенным внутри процедуры. Заметим, что, когда процедура выполнена, происходит смена домена.

Модель безопасности, специфицированная выше (см. рис. 8.1), имеет вид матрицы и называется *матрицей доступа*. Столбцы этой матрицы представляют собой объекты, строки — субъекты. В каждой ячейке матрицы хранится совокупность прав доступа, предоставленных данному субъекту на данный объект.

Поскольку реальная матрица доступа очень велика (типичный объем для современной ОС составляет несколько десятков мегабайтов), матрицу доступа никогда не хранят в системе в явном виде. В общем случае эта матрица будет разреженной, т. е. большинство ее клеток будут пустыми. Матрицу доступа можно разложить по столбцам, в результате чего получаются *списки прав доступа* ACL (access control list). В результате разложения матрицы по строкам получаются *мандаты возможностей* (capability list, или capability tickets).

Список прав доступа ACL. Каждая колонка в матрице может быть реализована как список доступа для одного объекта. Очевидно, что пустые клетки могут не учитываться. В результате для каждого объекта имеем список упорядоченных пар <domain, rights-set>, который определяет все домены с непустыми наборами прав для данного объекта.

Элементами списка прав доступа ACL могут быть процессы, пользователи или группы пользователей. При реализации широко применяется предоставление доступа по умолчанию для пользователей, права которых не указаны. Например, в ОС Unix все субъекты-пользователи разделены на три группы (владелец, группа и остальные), и для членов каждой группы контролируются операции чтения, записи и исполнения (rwx). В итоге имеем ACL — 9-битный код, который является атрибутом разнообразных объектов Unix.

Мандаты возможностей. Как отмечалось выше, если матрицу доступа хранить по строкам, т. е. если каждый субъект хранит список объектов и для каждого объекта — список допустимых операций, то такой способ хранения называется «мандаты возможностей» или «перечни возможностей» (capability list). Каждый пользователь обладает несколькими мандатами и может иметь право передавать их другим. Мандаты могут быть рассеяны по системе и вследствие этого представлять большую угрозу для безопасности, чем списки контроля доступа. Их хранение должно быть тщательно продумано.

Избирательное разграничение доступа — наиболее распространенный способ разграничения доступа. Это обусловлено сравнительной простотой его реализации и необременительностью правил такого разграничения доступа для пользователей. Главное достоинство избирательного разграничения доступа — гибкость; основные недостатки — рассредоточенность управления и сложность централизованного контроля.

Вместе с тем, защищенность ОС, подсистема защиты которой реализует только избирательное разграничение доступа, в некоторых случаях может оказаться недостаточной. В частности, в США запрещено хранить информацию, содержащую государственную тайну, в компьютерных системах, поддерживающих только избирательное разграничение доступа.

Расширением модели избирательного разграничения доступа является изолированная (или замкнутая) программная среда.

При использовании изолированной программной среды права субъекта на доступ к объекту определяются не только правами и привилегиями субъекта, но и процессом, с помощью которого субъект обращается к объекту. Можно, например, разрешить обращаться к файлам с расширением .doc только программам Word, Word Viewer и WPview.

Изолированная программная среда существенно повышает защищенность операционной системы от разрушающих программных воздействий, включая программные закладки и компьютерные вирусы. Кроме того, при использовании данной модели повышается защищенность целостности данных, хранящихся в системе.

Полномочное разграничение доступа с контролем информационных потоков

Полномочное, или мандатное, разграничение доступа (mandatory access control) обычно применяется в совокупности с избирательным разграничением доступа. Рассмотрим именно такой случай [56]. Правила разграничения доступа в данной модели формулируются следующим образом.

1. Для любого объекта ОС существует владелец.

2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.

3. Для каждой четверки субъект—объект—метод—процесс возможность доступа определена однозначно в каждый момент времени. При изменении состояния процесса со временем возможность предоставления доступа также может измениться. Вместе с тем, в каждый момент времени возможность доступа определена однозначно. Поскольку права процесса на доступ к объекту меняются с течением времени, они должны проверяться не только при открытии объекта, но и перед выполнением над объектом таких операций, как чтение и запись.

4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность удалить любой объект.

5. В множестве объектов выделяется *множество объектов полномочного разграничения доступа.* Каждый объект полномочного разграничения доступа имеет гриф секретности. Чем выше числовое значение грифа секретности, тем секретнее объект. Нулевое значение грифа секретности означает, что объект несекретен. Если объект не является объектом полномочного разграничения доступа или если объект несекретен, администратор может обратиться к нему по любому методу, как и в предыдущей модели разграничения доступа.

6. Каждый субъект доступа имеет *уровень допуска.* Чем выше числовое значение уровня допуска, тем больший допуск имеет субъект. Нулевое значение уровня допуска означает, что субъект не имеет допуска. Обычно ненулевое значение допуска назначается только субъектам-пользователям и не назначается субъектам, от имени которых выполняются системные процессы.

7. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:

- объект является объектом полномочного разграничения доступа;
- гриф секретности объекта строго выше уровня допуска субъекта, обращающегося к нему;
- субъект открывает объект в режиме, допускающем чтение информации.

Это правило называют *правилом NRU* (Not Read Up — не читать выше).

8. Каждый процесс ОС имеет *уровень конфиденциальности,* равный максимуму из грифов секретности объектов, открытых процессом на протяжении своего существования. Уровень конфиденциальности фактически представляет собой гриф секретности информации, хранящейся в оперативной памяти процесса.

9. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:

- объект является объектом полномочного разграничения доступа;
- гриф секретности объекта строго ниже уровня конфиденциальности процесса, обращающегося к нему;
- субъект собирается записывать в объект информацию,

Это правило предотвращает утечку секретной информации; его называют *правило NWD* (Not Write Down — не записывать ниже).

10. Понизить гриф секретности объекта полномочного разграничения доступа может только субъект, который:

- имеет доступ к объекту согласно правилу 7;
- обладает специальной привилегией, позволяющей ему понижать грифы секретности объектов.

При использовании данной модели разграничения доступа существенно страдает производительность ОС, поскольку права доступа к объекту должны проверяться не только при открытии объекта, но и при каждой операции чтение/запись. Кроме того, эта модель создает пользователям определенные неудобства: если уровень конфиденциальности процесса строго выше нуля, то вся информация в памяти процесса фактически является секретной и не может быть записана в несекретный объект.

Если процесс одновременно работает с двумя объектами, только один из которых является секретным, то он не может записывать информацию из памяти во второй объект. Эта проблема решается посредством использования специального программного интерфейса API для работы с памятью. Области памяти, выделяемые процессам, могут быть описаны как объекты полномочного разграничения доступа, после чего им могут назначаться грифы секретности.

При чтении секретного файла процесс должен считать содержимое такого файла в секретную область памяти, используя для этого функции ОС, гарантирующие невозможность утечки информации. Для работы с секретной областью памяти процесс также должен использовать специальные функции. Поскольку утечка информации из секретных областей памяти в память процесса невозможна, считывание процессом секретной информации в секретные области памяти не отражается на уровне конфиденциальности процесса. Если же процесс считывает секретную информацию в область памяти, не описанную как объект полномочного разграничения доступа, повышается уровень конфиденциальности процесса.

Из вышеизложенного следует, что пользователи ОС, реализующих данную модель разграничения доступа, вынуждены использовать ПО, разработанное с учетом этой модели. В противном случае они будут испытывать серьезные проблемы в

процессе работы с объектами ОС, имеющими ненулевой гриф секретности.

Каждая из рассмотренных моделей разграничения доступа имеет свои достоинства и недостатки.

В большинстве ситуаций применение избирательного разграничения доступа наиболее эффективно. Изолированную программную среду целесообразно использовать в случаях, когда важно обеспечить целостность программ и данных ОС. Полномочное разграничение доступа с контролем информационных потоков следует применять в тех случаях, когда для организации чрезвычайно важно обеспечение защищенности системы от несанкционированной утечки информации. В остальных ситуациях применение этой модели нецелесообразно из-за резкого ухудшения эксплуатационных качеств ОС.

8.2.4. Аудит

Процедура *аудита* применительно к ОС заключается в регистрации в специальном журнале, называемом *журналом аудита* или *журналом безопасности,* событий, которые могут представлять опасность для ОС. Пользователи системы, обладающие правом чтения журнала аудита, называются *аудиторами.*

Необходимость включения в защищенную ОС функций аудита обусловлена следующими обстоятельствами:

- обнаружение попыток вторжения является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения;
- подсистема защиты ОС может не отличить случайные ошибки пользователей от злонамеренных действий. Администратор, просматривая журнал аудита, сможет установить, что произошло при вводе пользователем неправильного пароля — ошибка легального пользователя или атака злоумышленника. Если пользователь пытался угадать пароль 20—30 раз, то это явная попытка подбора пароля;
- администраторы ОС должны иметь возможность получать информацию не только о текущем состоянии системы, но и о том, как ОС функционировала в недавнем прошлом. Такую возможность обеспечивает журнал аудита;

- если администратор ОС обнаружил, что против системы проведена успешная атака, ему важно выяснить, когда была начата атака и каким образом она осуществлялась. Журнал аудита может содержать всю необходимую информацию.

К числу событий, которые могут представлять опасность для ОС, обычно относят следующие:

- вход или выход из системы;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- обращение к удаленной системе;
- смену привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).

Если фиксировать в журнале аудита все события, объем регистрационной информации будет расти слишком быстро, что затруднит ее эффективный анализ. Необходимо предусмотреть выборочное протоколирование как в отношении пользователей, так и в отношении событий.

Требования к аудиту. Подсистема аудита ОС должна удовлетворять следующим требованиям.

1. Добавлять записи в журнал аудита может только ОС. Если предоставить это право какому-то физическому пользователю, этот пользователь получит возможность компрометировать других пользователей, добавляя в журнал аудита соответствующие записи.

2. Редактировать или удалять отдельные записи в журнале аудита не может ни один субъект доступа, в том числе и сама ОС.

3. Просматривать журнал аудита могут только пользователи, обладающие соответствующей привилегией.

4. Очищать журнал аудита могут только пользователи-аудиторы. После очистки журнала в него автоматически вносится запись о том, что журнал аудита был очищен, с указанием времени очистки журнала и имени пользователя, очистившего журнал. ОС должна поддерживать возможность сохранения журнала аудита перед очисткой в другом файле.

5. При переполнении журнала аудита ОС аварийно завершает работу («зависает»). После перезагрузки работать с системой могут только аудиторы. ОС переходит к обычному режиму работы только после очистки журнала аудита.

Для ограничения доступа к журналу аудита должны применяться специальные средства защиты.

Политика аудита — это совокупность правил, определяющих, какие события должны регистрироваться в журнале аудита. Для обеспечения надежной защиты ОС в журнале аудита должны обязательно регистрироваться следующие события:

- попытки входа/выхода пользователей из системы;
- попытки изменения списка пользователей;
- попытки изменения политики безопасности, в том числе и политики аудита.

Окончательный выбор событий, которые должны регистрироваться в журнале аудита, возлагается на аудиторов. При выборе оптимальной политики аудита следует учитывать ожидаемую скорость заполнения журнала аудита. Политика аудита должна оперативно реагировать на изменения в конфигурации ОС, в характере хранимой и обрабатываемой информации и особенно на выявленные попытки атаки ОС.

В некоторых ОС подсистема аудита помимо записи информации о зарегистрированных событиях в специальный журнал предусматривает возможность интерактивного оповещения аудиторов об этих событиях.

Глава 9
ТЕХНОЛОГИИ МЕЖСЕТЕВЫХ ЭКРАНОВ

Межсетевой экран (МЭ) — это специализированный комплекс межсетевой защиты, называемый также *брандмауэром* или системой *firewall*. МЭ позволяет разделить общую сеть на две части (или более) и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet.

Обычно МЭ защищают внутреннюю сеть предприятия от «вторжений» из глобальной сети Internet, хотя они могут использоваться и для защиты от «нападений» из корпоративной интрасети, к которой подключена локальная сеть предприятия. Технология МЭ одна из самых первых технологий защиты корпоративных сетей от внешних угроз.

Для большинства организаций установка МЭ является необходимым условием обеспечения безопасности внутренней сети.

9.1. Функции МЭ

Для противодействия несанкционированному межсетевому доступу МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 9.1). При этом все взаимодействия между этими сетями должны осуществляться только через МЭ. Организационно МЭ входит в состав защищаемой сети.

МЭ, защищающий сразу множество узлов внутренней сети, призван решить:

- задачу ограничения доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам

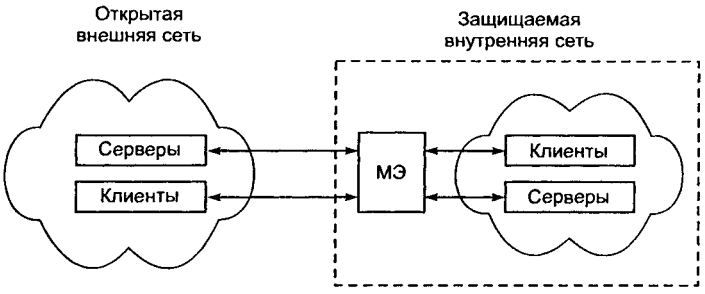


Рис. 9.1. Схема подключения межсетевого экрана МЭ

корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой компании, пытающиеся получить доступ к серверам баз данных, защищаемых МЭ;

- задачу разграничения доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требующимся для выполнения служебных обязанностей.

До сих пор не существует единой общепризнанной классификации МЭ. Их можно классифицировать, например, по следующим основным признакам [32].

По функционированию на уровнях модели OSI:

- пакетный фильтр (экранирующий маршрутизатор — *screening router*);
- шлюз сеансового уровня (экранирующий транспорт);
- прикладной шлюз (*application gateway*);
- шлюз экспертного уровня (*stateful inspection firewall*).

По используемой технологии:

- контроль состояния протокола (*stateful inspection*);
- на основе модулей посредников (*proxy*).

По исполнению:

- аппаратно-программный;
- программный.

По схеме подключения:

- схема единой защиты сети;
- схема с защищаемым закрытым и не защищаемым открытым сегментами сети;
- схема с раздельной защитой закрытого и открытого сегментов сети.

9.1.1. Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований [9, 32]. Фильтрация осуществляется на основе набора предварительно загруженных в МЭ правил, соответствующих принятой политике безопасности. Поэтому МЭ удобно представлять как последовательность фильтров, обрабатывающих информационный поток (рис. 9.2).

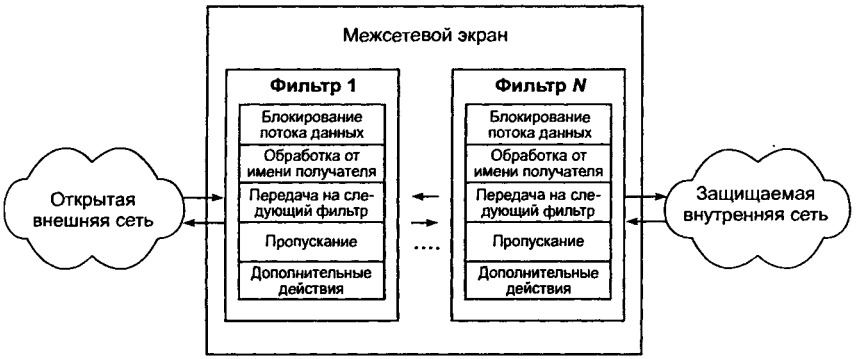


Рис. 9.2. Структура межсетевого экрана

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем:

1) анализа информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;

2) принятия на основе интерпретируемых правил одного из следующих решений:

- не пропустить данные;
- обработать данные от имени получателя и возвратить результат отправителю;
- передать данные на следующий фильтр для продолжения анализа;
- пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, напри-

мер преобразование данных, регистрация событий и др. Соответственно правила фильтрации определяют перечень условий, по которым осуществляется:

- разрешение или запрещение дальнейшей передачи данных;
- выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

- служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
- непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
- внешние характеристики потока информации, например, временные, частотные характеристики, объем данных и т. д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

9.1.2. Выполнение функций посредничества

Функции посредничества МЭ выполняет с помощью специальных программ, называемых *экранирующими агентами* или *программами-посредниками*. Эти программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере МЭ. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

Следует иметь в виду, что МЭ может выполнять функции фильтрации без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней

сетью. Вместе с тем программные посредники могут и не осуществлять фильтрацию потока сообщений.

В общем случае *программы-посредники*, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:

- проверку подлинности передаваемых данных;
- фильтрацию и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- кэширование данных, запрашиваемых из внешней сети;
- идентификацию и аутентификацию пользователей;
- трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
- регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов [9, 32].

Программы-посредники могут осуществлять *проверку подлинности* получаемых и передаваемых данных. Это актуально не только для аутентификации электронных сообщений, но и мигрирующих программ (Java, ActiveX Controls), по отношению к которым может быть выполнен подлог. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей.

Программы-посредники могут выполнять *разграничение доступа* к ресурсам внутренней или внешней сети, используя результаты идентификации и аутентификации пользователей при их обращении к МЭ.

Способы разграничения доступа к ресурсам внутренней сети практически не отличаются от способов разграничения, поддерживаемых на уровне операционной системы.

При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих подходов:

- разрешение доступа только по заданным адресам во внешней сети;
- фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;
- накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дис-

ковой памяти МЭ и полный запрет доступа во внешнюю сеть.

С помощью специальных посредников поддерживается также *кэширование данных*, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска МЭ, называемого в этом случае *proxy-сервером*. Поэтому если при очередном запросе нужная информация окажется на proxy-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого proxy-сервера.

Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на proxy-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам proxy-сервера, а непосредственный доступ к ресурсам внешней сети запрещается.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил. Здесь следует различать два вида программ-посредников:

- экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например FTP, HTTP, Telnet;
- универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов, или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных и, если какой-либо объект не соответствует заданным критериям, то либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например обезвреживает обнаруженные компьютерные вирусы. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы.

МЭ с посредниками позволяют также организовывать защищенные виртуальные сети VPN (Virtual Private Network), например безопасно объединять несколько локальных сетей, подключенных к Internet, в одну виртуальную сеть.

9.1.3. Дополнительные возможности МЭ

Помимо выполнения фильтрации трафика и функций посредничества некоторые МЭ позволяют реализовывать другие, не менее важные функции, без которых обеспечение защиты периметра внутренней сети было бы неполным [9].

Идентификация и аутентификация пользователей. Кроме разрешения или запрещения допуска различных приложений в сеть, МЭ могут также выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам, разделяемым МЭ.

Прежде чем пользователю будет предоставлено право использования какого-либо сервиса, необходимо убедиться, что он действительно тот, за кого себя выдает. Идентификация и аутентификация пользователей являются важными компонентами концепции МЭ. Авторизация пользователя обычно рассматривается в контексте аутентификации — как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы.

Идентификация и аутентификация пользователя иногда осуществляются при предъявлении обычного идентификатора (имени) и пароля. Однако эта схема уязвима с точки зрения безопасности — пароль может быть перехвачен и использован другим лицом. Многие инциденты в сети Internet произошли отчасти из-за уязвимости традиционных многоразовых паролей. Злоумышленники могут наблюдать за каналами в сети Internet и перехватывать передающиеся в них открытым текстом пароли, поэтому такая схема аутентификации считается неэффективной. Пароль следует передавать через общедоступные коммуникации в зашифрованном виде (рис. 9.3). Это позволяет предотвратить получение несанкционированного доступа путем перехвата сетевых пакетов.

Более надежным методом аутентификации является использование одноразовых паролей. Широкое распространение получила технология аутентификации на основе одноразовых паролей SecurID (см. гл. 7 и 13).

Удобно и надежно также применение цифровых сертификатов, выдаваемых доверенными органами, например центром распределения ключей. Большинство программ-посредников разрабатываются таким образом, чтобы пользователь аутентифицировался только в начале сеанса работы с МЭ. После этого от него

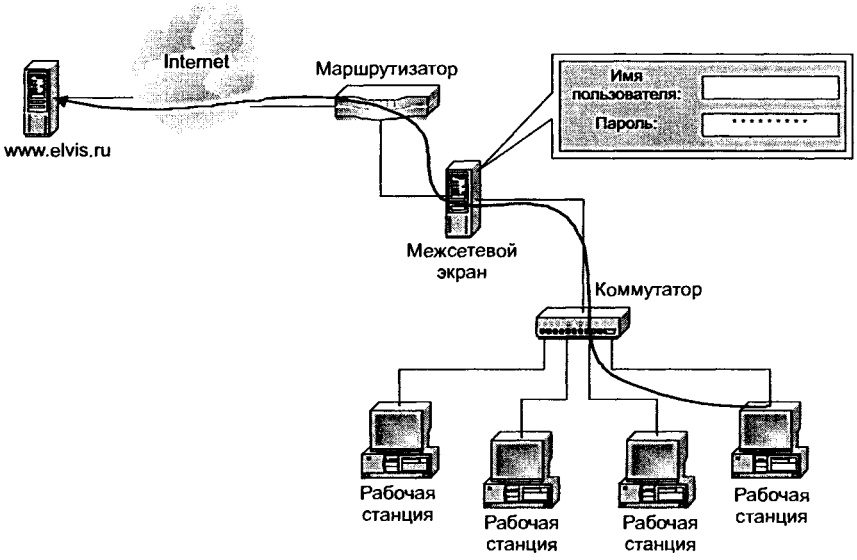


Рис. 9.3. Схема аутентификации пользователя по предъявляемому паролю

не требуется дополнительная аутентификация в течение времени, определяемого администратором.

Так как МЭ могут централизовать управление доступом в сети, они являются подходящим местом для установки программ или устройств усиленной аутентификации. Хотя средства усиленной аутентификации могут использоваться на каждом хосте, более практично их размещение на МЭ. При отсутствии МЭ, использующего меры усиленной аутентификации, неаутентифицированный трафик таких приложений, как Telnet или FTP, может напрямую проходить к внутренним системам в сети.

Ряд МЭ поддерживают Kerberos — один из распространенных методов аутентификации. Как правило, большинство коммерческих МЭ поддерживают несколько различных схем аутентификации, позволяя администратору сетевой безопасности сделать выбор наиболее приемлемой схемы для своих условий.

Трансляция сетевых адресов. Для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, МЭ выполняют очень важную функцию — трансляцию внутренних сетевых адресов (*network address translation*) (рис. 9.4).

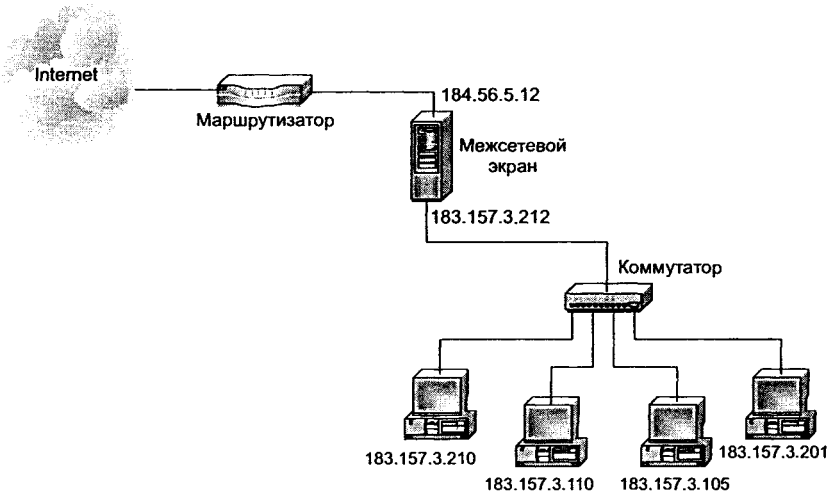


Рис. 9.4. Трансляция сетевых адресов

Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов выполняется автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP-адрес.

Трансляция внутренних сетевых адресов может осуществляться двумя способами — динамически и статически. В первом случае адрес выделяется узлу в момент обращения к МЭ. После завершения соединения адрес освобождается и может быть использован любым другим узлом корпоративной сети. Во втором случае адрес узла всегда привязывается к одному адресу МЭ, из которого передаются все исходящие пакеты. IP-адрес МЭ становится единственным активным IP-адресом, который попадает во внешнюю сеть. В результате все исходящие из внутренней сети пакеты оказываются отправленными МЭ, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например в сети Internet. Это эффективно решает проблему расшире-

ния адресного пространства внутренней сети и дефицита адресов внешней сети.

Администрирование, регистрация событий и генерация отчетов. Простота и удобство администрирования является одним из ключевых аспектов в создании эффективной и надежной системы защиты. Ошибки при определении правил доступа могут образовать дыру, через которую возможен взлом системы. Поэтому в большинстве МЭ реализованы сервисные утилиты, облегчающие ввод, удаление, просмотр набора правил. Наличие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе или редактирования правил. Как правило, утилиты позволяют просматривать информацию, сгруппированную по каким-либо критериям, например все, что относится к конкретному пользователю или сервису.

Важными функциями МЭ являются *регистрация событий, реагирование на задаваемые события,* а также *анализ зарегистрированной информации* и *составление отчетов.* МЭ, являясь критическим элементом системы защиты корпоративной сети, имеет возможность регистрации всех действий, им фиксируемых. К таким действиям относятся не только пропуск или блокирование сетевых пакетов, но и изменение правил разграничения доступа администратором безопасности и другие действия. Такая регистрация позволяет обращаться к создаваемым журналам по мере необходимости (в случае возникновения инцидента безопасности или сбора доказательств для предоставления их в судебные инстанции или для внутреннего расследования).

При правильно настроенной системе фиксации сигналов о подозрительных событиях (alarm) МЭ может дать детальную информацию о том, были ли МЭ или сеть атакованы или зондированы. Собирать статистику использования сети и доказательства ее зондирования важно по нескольким причинам. Прежде всего нужно знать наверняка, что МЭ устойчив к зондированию и атакам, и определить, адекватны ли меры защиты МЭ. Кроме того, статистика использования сети важна в качестве исходных данных при проведении исследований и анализе риска для формулирования требований к сетевому оборудованию и программам.

Многие МЭ содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей. Системы учета по-

зволяют произвести анализ статистики и предоставляют администраторам подробные отчеты. За счет использования специальных протоколов МЭ могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, т. е. выдача предупредительных сигналов. Любой МЭ, который не способен посылать предупредительные сигналы при обнаружении нападения, нельзя считать эффективным средством межсетевой защиты.

9.2. Особенности функционирования МЭ на различных уровнях модели OSI

МЭ поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI.

Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно различают такие неделимые МЭ (рис. 9.5), как:

- экранирующий маршрутизатор;
- шлюз сеансового уровня (экранирующий транспорт);
- шлюз прикладного уровня (экранирующий шлюз) [9, 32].

Используемые в сетях протоколы (TCP/IP, SPX/IPX) не полностью соответствуют эталонной модели OSI, поэтому экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели. Например, прикладной экран может осуществлять автоматическое зашифровывание сообщений при их передаче во внешнюю сеть, а также автоматическое расшифровывание криптографически закрытых принимаемых данных. В этом случае такой экран функционирует не только на прикладном уровне модели OSI, но и на уровне представления.

Шлюз сеансового уровня при своем функционировании охватывает транспортный и сетевой уровни модели OSI. Экрани-

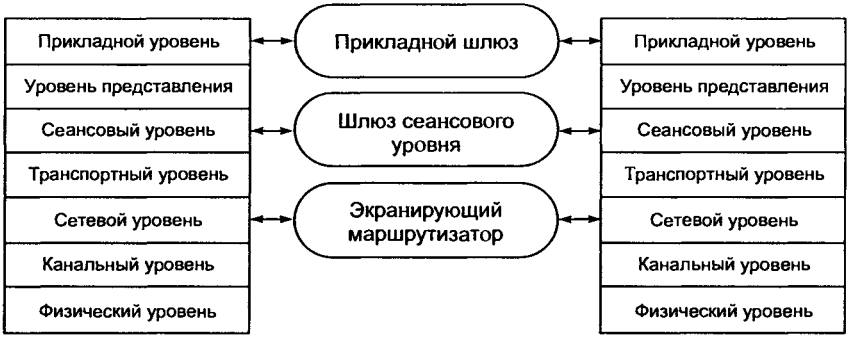


Рис. 9.5. Типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI

рующий маршрутизатор при анализе пакетов сообщений проверяет их заголовки не только сетевого, но и транспортного уровня.

МЭ указанных типов имеют свои достоинства и недостатки. Многие из используемых МЭ являются либо прикладными шлюзами, либо экранирующими маршрутизаторами, не обеспечивая полную безопасность межсетевого взаимодействия. Надежную защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет экранирующий маршрутизатор, шлюз сеансового уровня, а также прикладной шлюз.

Рассмотрим функционирование прикладного шлюза.

9.2.1. Прикладной шлюз

Прикладной шлюз, называемый также *экранирующим шлюзом*, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает наиболее надежную защиту межсетевых взаимодействий [9, 32]. Защитные функции прикладного шлюза, как и шлюза сеансового уровня, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество функций защиты, к которым относятся следующие:

- идентификация и аутентификация пользователей при попытке установления соединений через МЭ;
- проверка подлинности информации, передаваемой через шлюз;

- разграничение доступа к ресурсам внутренней и внешней сетей;
- фильтрация и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
- регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов;
- кэширование данных, запрашиваемых из внешней сети.

Поскольку функции прикладного шлюза относятся к функциям посредничества, этот шлюз представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) — по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др.). Программный посредник (*application proxy*) каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе.

Прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, т. е. функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью (рис. 9.6).

Посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уров-

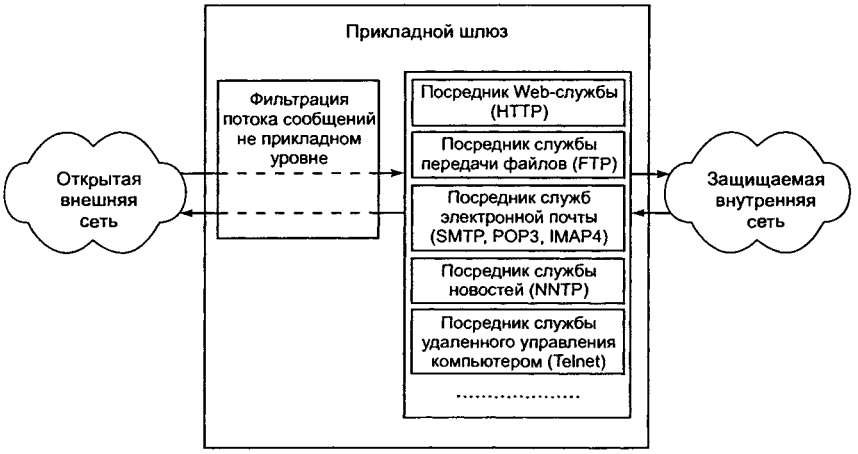


Рис. 9.6. Схема функционирования прикладного шлюза

ня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями (программными серверами), во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели OSI.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP — серверы HTTP, FTP, SMTP, NNTP и др. Эти программные серверы функционируют на МЭ в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам TCP/IP.

Шлюз прикладного уровня обладает следующими достоинствами:

- обеспечивает высокий уровень защиты локальной сети благодаря возможности выполнения большинства функций посредничества;
- защита на уровне приложений позволяет осуществлять большое число дополнительных проверок, уменьшая тем самым вероятность проведения успешных атак, возможных из-за недостатков программного обеспечения;
- при нарушении его работоспособности блокируется сквозное прохождение пакетов между разделяемыми сетями, в результате чего безопасность защищаемой сети не снижается из-за возникновения отказов.

К недостаткам прикладного шлюза относятся:

- высокие требования к производительности и ресурсоемкости компьютерной платформы;
- отсутствие «прозрачности» для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.

9.2.2. Варианты исполнения МЭ

Существует два основных варианта исполнения МЭ — программный и программно-аппаратный. В свою очередь программно-аппаратный вариант имеет две разновидности — в виде специализированного устройства и в виде модуля в маршрутизаторе или коммутаторе.

В настоящее время чаще используется программное решение, которое на первый взгляд выглядит более привлекательным. Это связано с тем, что для его применения достаточно, ка-

залось бы, только приобрести программное обеспечение (ПО) МЭ и установить на любой компьютер, имеющийся в организации. Однако на практике далеко не всегда в организации находится свободный компьютер, удовлетворяющий достаточно высоким требованиям по системным ресурсам. Поэтому одновременно с приобретением ПО приобретается и компьютер для его установки. Затем следует процесс установки на компьютер операционной системы (ОС) и ее настройка, что также требует времени и оплаты работы установщиков. И только после этого устанавливается и настраивается ПО системы обнаружения атак. Нетрудно заметить, что использование обычного персонального компьютера далеко не так просто, как кажется на первый взгляд.

Поэтому в последние годы значительно возрос интерес к программно-аппаратным решениям [9, 32], которые постепенно вытесняют «чисто» программные системы. Широкое распространение стали получать специализированные программно-аппаратные решения, называемые *security appliance*. Программно-аппаратный комплекс межсетевого экранирования обычно состоит из компьютера, а также функционирующих на нем ОС и специального ПО. Следует отметить, что это специальное ПО часто называют firewall. Используемый компьютер должен быть достаточно мощным и физически защищенным, например находиться в специально отведенном и охраняемом помещении. Кроме того, он должен иметь средства защиты от загрузки ОС с несанкционированного носителя. Программно-аппаратные комплексы используют специализированные или обычные ПО (как правило, на базе FreeBSD, Linux или Microsoft Windows NT (2000)), «урезанные» для выполнения заданных функций и удовлетворяющие ряду требований:

- иметь средства разграничения доступа к ресурсам системы;
- блокировать доступ к компьютерным ресурсам в обход предоставляемого программного интерфейса;
- запрещать привилегированный доступ к своим ресурсам из локальной сети;
- содержать средства мониторинга/аудита любых административных действий.

Достоинства специализированных программно-аппаратных решений:

- *простота внедрения в технологию обработки информации.* Такие средства поставляются с заранее установленной и настроенной ОС и защитными механизмами, поэтому

необходимо только подключить их к сети, что выполняется в течение нескольких минут;

- *простота управления.* Данные средства могут управляться с любой рабочей станции Windows 9x, NT, 2000 или Unix. Взаимодействие консоли управления с устройством осуществляется либо по стандартным протоколам, например Telnet или SNMP, либо при помощи специализированных или защищенных протоколов, например SSH или SSL;
- *отказоустойчивость и высокая доступность.* Исполнение МЭ в виде специализированного программно-аппаратного комплекса позволяет реализовать механизмы обеспечения не только программной, но и аппаратной отказоустойчивости и высокой доступности;
- *высокая производительность и надежность.* За счет исключения из ОС всех «ненужных» сервисов и подсистем, программно-аппаратный комплекс работает более эффективно с точки зрения производительности и надежности;
- *специализация на защите.* Решение только задач обеспечения сетевой безопасности не приводит к затратам ресурсов на выполнение других функций, например маршрутизации и т. п.

9.3. Схемы сетевой защиты на базе МЭ

При подключении корпоративной или локальной сети к глобальным сетям необходимы:

- защита корпоративной или локальной сети от удаленного НСД со стороны глобальной сети;
- сокрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
- разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть.

Для эффективной защиты межсетевого взаимодействия система МЭ должна быть правильно установлена и сконфигурирована. Данный процесс состоит:

- из формирования политики межсетевого взаимодействия;
- выбора схемы подключения и настройки параметров функционирования МЭ.

9.3.1. Формирование политики межсетевого взаимодействия

Политика межсетевого взаимодействия является составной частью общей политики безопасности в организации. Она определяет требования к безопасности информационного обмена организации с внешним миром и должна отражать два аспекта [9, 32]:

- политику доступа к сетевым сервисам;
- политику работы МЭ.

Политика доступа к сетевым сервисам определяет правила предоставления и использования всех возможных сервисов защищаемой компьютерной сети. В рамках данной политики должны быть заданы все сервисы, предоставляемые через МЭ, и допустимые адреса клиентов для каждого сервиса. Кроме того, для пользователей должны быть указаны правила, описывающие, когда, кто, каким сервисом и на каком компьютере может воспользоваться. Задаются также ограничения на методы доступа, например на использование протоколов SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Ограничение методов доступа необходимо для того, чтобы пользователи не могли обращаться к «запрещенным» сервисам Internet обходными путями. Правила аутентификации пользователей и компьютеров, а также условия работы пользователей вне локальной сети организации должны быть определены отдельно.

Для того чтобы МЭ успешно защищал ресурсы организации, политика доступа пользователей к сетевым сервисам должна быть реалистичной. Реалистичной считается такая политика, при которой найден баланс между защитой сети организации от известных рисков и необходимым доступом пользователей к сетевым сервисам.

Политика работы МЭ задает базовый принцип управления межсетевым взаимодействием, положенный в основу функционирования МЭ. Может быть выбран один из двух принципов:

1) запрещено все, что явно не разрешено;

2) разрешено все, что явно не запрещено.

Фактически выбор принципа устанавливает, насколько «подозрительной» или «доверительной» должна быть система защиты. В зависимости от выбора, решение может быть принято как в пользу безопасности и в ущерб удобству использования сетевых сервисов, так и наоборот.

При выборе принципа 1 МЭ настраивается так, чтобы блокировать любые явно не разрешенные межсетевые взаимодействия. Этот принцип соответствует классической модели доступа, используемой во всех областях информационной безопасности. Такой подход позволяет адекватно реализовать принцип минимизации привилегий, поэтому с точки зрения безопасности он является лучшим. Администратор безопасности должен на каждый тип разрешенного взаимодействия задавать правила доступа (одно и более). Администратор не сможет по забывчивости оставить разрешенными какие-либо полномочия, так как по умолчанию они будут запрещены. Доступные лишние сервисы могут быть использованы во вред безопасности, что особенно характерно для закрытого и сложного ПО, в котором могут быть различные ошибки и некорректности. Принцип 1, в сущности, является признанием факта, что незнание может причинить вред. Следует отметить, что правила доступа, сформулированные в соответствии с этим принципом, могут доставлять пользователям определенные неудобства.

При выборе принципа 2 МЭ настраивается так, чтобы блокировать только явно запрещенные межсетевые взаимодействия. В этом случае повышается удобство использования сетевых сервисов со стороны пользователей, но снижается безопасность межсетевого взаимодействия. Пользователи имеют больше возможностей обойти МЭ, например, могут получить доступ к новым сервисам, не запрещаемым политикой (или даже не указанным в политике), или запустить запрещенные сервисы на нестандартных портах TCP/UDP, которые не запрещены политикой. Администратор может учесть не все действия, которые запрещены пользователям. Ему приходится работать в режиме реагирования, предсказывая и запрещая те межсетевые взаимодействия, которые отрицательно воздействуют на безопасность сети. При реализации принципа 2 внутренняя сеть оказывается менее защищенной от нападений хакеров, поэтому производители МЭ обычно отказываются от его использования.

МЭ является симметричным. Для него отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю сеть, и наоборот. В общем случае его работа основана на динамическом выполнении двух функций:

- фильтрации проходящих через него информационных потоков;
- посредничества при реализации межсетевых взаимодействий.

В зависимости от типа экрана эти функции могут выполняться с различной полнотой. Простые МЭ ориентированы на выполнение только одной из них. Комплексные МЭ обеспечивают совместное выполнение указанных функций защиты. Собственная защищенность МЭ достигается с помощью тех же средств, что и защищенность универсальных систем [9].

Чтобы эффективно обеспечивать безопасность сети, комплексный МЭ обязан управлять всем потоком, проходящим через него, и отслеживать свое состояние. Для принятия управляющих решений по используемым сервисам МЭ должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других приложений.

Недостаточно просто проверять пакеты по отдельности. Информация о состоянии соединения, полученная из инспекции соединений в прошлом и других приложений — главный фактор в принятии управляющего решения при установлении нового соединения. При принятии решения учитываются как состояние соединения (полученное из прошлого потока данных), так и состояние приложения (полученное из других приложений). Полнота и правильность управления требуют, чтобы комплексный МЭ имел возможность анализа и использования следующих элементов:

- *информации о соединениях* — информации от всех семи уровней в пакете;
- *истории соединений* — информации, полученной от предыдущих соединений;
- *состояния уровня приложения* — информации о состоянии, полученной из других приложений. Например, аутентифицированному до настоящего момента пользователю можно предоставить доступ через МЭ только для авторизованных видов сервиса;
- *агрегирующих элементов* — вычислений разнообразных выражений, основанных на всех вышеперечисленных факторах.

9.3.2. Основные схемы подключения МЭ

При подключении корпоративной сети к глобальным сетям необходимо разграничить доступ в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть, а также обес-

печить защиту подключаемой сети от удаленного НСД со стороны глобальной сети. При этом организация заинтересована в сокрытии информации о структуре своей сети и ее компонентов от пользователей глобальной сети. Работа с удаленными пользователями требует установления жестких ограничений доступа к информационным ресурсам защищаемой сети.

Часто возникает потребность иметь в составе корпоративной сети несколько сегментов с разными уровнями защищенности:

- свободно доступные сегменты (например, рекламный WWW-сервер);
- сегмент с ограниченным доступом (например, для доступа сотрудникам организации с удаленных узлов);
- закрытые сегменты (например, финансовая локальная подсеть организации).

Для подключения МЭ могут использоваться различные схемы, которые зависят от условий функционирования защищаемой сети, а также от количества сетевых интерфейсов и других характеристик, используемых МЭ. Широкое распространение получили схемы:

- защиты сети с использованием экранирующего маршрутизатора;
- единой защиты локальной сети;
- с защищаемой закрытой и не защищаемой открытой подсетями;
- с раздельной защитой закрытой и открытой подсетей [9, 32].

Рассмотрим подробнее схему с защищаемой закрытой и не защищаемой открытой подсетями. Если в составе локальной сети имеются общедоступные открытые серверы, то их целесообразно вынести как открытую подсеть до МЭ (рис. 9.7). Этот способ об-

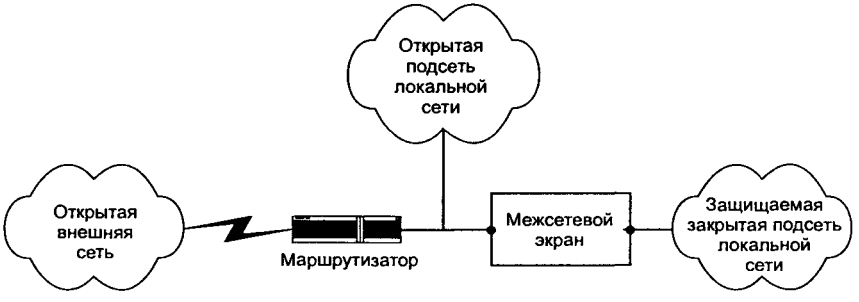


Рис. 9.7. Схема с защищаемой закрытой и не защищаемой открытой подсетями

ладает высокой защищенностью закрытой части локальной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до МЭ.

Некоторые МЭ позволяют разместить эти серверы на себе. Однако такое решение не является лучшим с точки зрения безопасности самого МЭ и загрузки компьютера. Схему подключения МЭ с защищаемой закрытой подсетью и не защищаемой открытой подсетью целесообразно использовать лишь при невысоких требованиях по безопасности к открытой подсети.

Если же к безопасности открытых серверов предъявляются повышенные требования, тогда необходимо использовать схему с раздельной защитой закрытой и открытой подсетей.

9.3.3. Персональные и распределенные сетевые экраны

За последние несколько лет в структуре корпоративных сетей произошли определенные изменения. Если раньше границы таких сетей можно было четко очертить, то сейчас это практически невозможно. Еще недавно такая граница проходила через все маршрутизаторы или иные устройства (например, модемы), через которые осуществлялся выход во внешние сети. В удаленных офисах организации ситуация была схожа. Однако сейчас полноправным пользователем защищаемой МЭ сети является сотрудник, находящийся за пределами защищаемого периметра. К таким сотрудникам относятся пользователи, работающие на дому или находящиеся в командировке. Несомненно им также требуется защита. Но все традиционные МЭ построены так, что защищаемые пользователи и ресурсы должны находиться под их защитой с внутренней стороны корпоративной или локальной сети, что является невозможным для мобильных пользователей.

Для решения этой проблемы были предложены следующие подходы:

- применение распределенных МЭ (distributed firewall);
- использование возможностей виртуальных частных сетей VPN (virtual private network) (см. гл. 10).

Распределенный межсетевой экран (distributed firewall) — централизованно управляемая совокупность сетевых мини-экранов, защищающих отдельные компьютеры сети.

Для индивидуальных пользователей представляет интерес технология *персонального сетевого экранирования*. В этом случае сетевой экран устанавливается на защищаемый персональный компьютер. Такой экран, называемый *персональным экраном компьютера* (personal firewall) или *системой сетевого экранирования*, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко.

Эти средства не только защищают от внешних атак компьютеры, на которых они установлены, но и обеспечивают защиту трафика, передаваемого за пределы данного узла (т. е. организуют защищенные каналы VPN). Именно такое решение позволило обеспечить защиту сетей с нечетко очерченными границами.

Наличие функции централизованного управления у распределенного МЭ — его главное отличие от персонального экрана. Если персональные сетевые экраны управляются только с компьютера, на котором они установлены, и идеально подходят для домашнего применения, то распределенные МЭ могут управляться централизованно, с единой консоли управления, установленной в главном офисе организации. Это позволило некоторым производителям выпускать МЭ в двух версиях:

- персональной (для индивидуальных пользователей);
- распределенной (для корпоративных пользователей).

В современных условиях более 50 % различных атак и попыток доступа к информации осуществляется изнутри локальных сетей, поэтому классический «периметровый» подход к созданию системы защиты корпоративной сети становится недостаточно эффективным. Корпоративную сеть можно считать действительно защищенной от НСД только при наличии в ней средств защиты точек входа со стороны Internet и решений, обеспечивающих безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия. Решения на основе распределенных или персональных МЭ наи-

лучшим образом обеспечивают безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия [64].

9.3.4. Проблемы безопасности МЭ

МЭ не решает все проблемы безопасности корпоративной сети. Кроме описанных выше достоинств МЭ, существуют ограничения в их использовании и угрозы безопасности, от которых МЭ не могут защитить. Отметим наиболее существенные из этих ограничений [9, 43]:

- *возможное ограничение пропускной способности.* Традиционные МЭ являются потенциально узким местом сети, так как все соединения должны проходить через МЭ и в некоторых случаях изучаться МЭ;
- *отсутствие встроенных механизмов защиты от вирусов.* Традиционные МЭ не могут защитить от пользователей, загружающих зараженные вирусами программы для ПЭВМ из интернетовских архивов или при передаче таких программ в качестве приложений к письму, поскольку эти программы могут быть зашифрованы или сжаты большим числом способов;
- *отсутствие эффективной защиты от получаемого из Internet опасного содержимого* (апплеты Java, управляющие элементы ActiveX, сценарии JavaScript и т. п.). Специфика мобильного кода такова, что он может быть использован как средство для проведения атак. Мобильный код может быть реализован в виде:
  - вируса, который вторгается в ИС и уничтожает данные на локальных дисках, постоянно модифицируя свой код и затрудняя тем самым свое обнаружение и удаление;
  - агента, перехватывающего пароли, номера кредитных карт и т. п.;
  - программы, копирующей конфиденциальные файлы, содержащие деловую и финансовую информацию и пр.;
- *МЭ не может защитить от ошибок и некомпетентности администраторов и пользователей*;
- *традиционные МЭ являются по существу средствами, только блокирующими атаки.* В большинстве случаев они защищают от атак, которые уже находятся в процессе осуществле-

ния. Более эффективным было бы не только блокирование, но и упреждение атак, т. е. устранение предпосылок реализации вторжений. Для организации упреждения атак необходимо использовать средства обнаружения атак и поиска уязвимостей, которые будут своевременно обнаруживать и рекомендовать меры по устранению «слабых мест» в системе защиты. Технологии обнаружения атак и анализа защищенности сетей рассматриваются в гл. 14.

Для защиты информационных ресурсов распределенных корпоративных систем необходимо применение комплексной системы информационной безопасности, которая позволит эффективно использовать достоинства МЭ и компенсировать их недостатки с помощью других средств безопасности.

Глава 10
ОСНОВЫ ТЕХНОЛОГИИ ВИРТУАЛЬНЫХ ЗАЩИЩЕННЫХ СЕТЕЙ VPN

Задача создания компьютерной сети предприятия в пределах одного здания может быть решена относительно легко. Однако современная инфраструктура корпораций включает в себя географически распределенные подразделения самой корпорации, ее партнеров, клиентов и поставщиков. Поэтому создание корпоративной сети стало существенно более сложной задачей.

С бурным развитием Internet и сетей коллективного доступа произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные каналы Internet. Предприятия стремятся использовать такие каналы для передачи критичной коммерческой и управленческой информации.

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования в бизнесе открытых сетей в начале 1990-х гг. родилась и активно развивается концепция построения виртуальных частных сетей — VPN (Virtual Private Network).

10.1. Концепция построения виртуальных защищенных сетей VPN

В основе концепции построения виртуальных сетей VPN лежит достаточно простая идея: если в глобальной сети имеются два узла, которым нужно обменяться информацией, то между этими двумя узлами необходимо построить виртуальный защищенный туннель для обеспечения конфиденциальности и целостности информации, передаваемой через открытые сети; доступ

к этому виртуальному туннелю должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям.

Преимущества, получаемые компанией от создания таких виртуальных туннелей, заключаются прежде всего в значительной экономии финансовых средств, поскольку в этом случае компания может отказаться от построения или аренды дорогих выделенных каналов связи для создания собственных intranet/extranet сетей и использовать для этого дешевые Интернет-каналы, надежность и скорость передачи которых в большинстве своем уже не уступает выделенным линиям. Очевидная экономическая эффективность от внедрения VPN-технологий стимулирует предприятия к активному их внедрению.

10.1.1. Основные понятия и функции сети VPN

При подключении корпоративной локальной сети к открытой сети возникают угрозы безопасности двух основных типов:

- НСД к внутренним ресурсам корпоративной локальной сети, получаемый злоумышленником в результате несанкционированного входа в эту сеть;
- НСД к корпоративным данным в процессе их передачи по открытой сети.

Обеспечение безопасности информационного взаимодействия локальных сетей и отдельных компьютеров через открытые сети, в частности через сеть Интернет, возможно путем эффективного решения следующих задач:

- защита подключенных к открытым каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;
- защита информации в процессе ее передачи по открытым каналам связи.

Как уже отмечалось выше, для защиты локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды обычно используют МЭ, поддерживающие безопасность информационного взаимодействия путем фильтрации двустороннего потока сообщений, а также выполнения функций посредничества при обмене информацией. МЭ располагают на стыке между локальной и открытой сетью. Для защиты отдельного удаленного компьютера, подключенного к

открытой сети, на этом компьютере устанавливают ПО сетевого экрана, и такой сетевой экран называется персональным.

Защита информации в процессе ее передачи по открытым каналам основана на использовании виртуальных защищенных сетей VPN. *Виртуальной защищенной сетью VPN* (*Virtual Private Network*) называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных. Виртуальная защищенная сеть VPN формируется путем построения виртуальных защищенных каналов связи, создаваемых на базе открытых каналов связи общедоступной сети. Эти виртуальные защищенные каналы связи называются *туннелями* VPN. Сеть VPN позволяет с помощью туннелей VPN соединить центральный офис, офисы филиалов, офисы бизнес-партнеров и удаленных пользователей и безопасно передавать информацию через Интернет (рис. 10.1).

Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети. Защита информации в процессе ее передачи по туннелю VPN основана:

- на аутентификации взаимодействующих сторон;
- криптографическом закрытии (шифровании) передаваемых данных;
- проверке подлинности и целостности доставляемой информации.

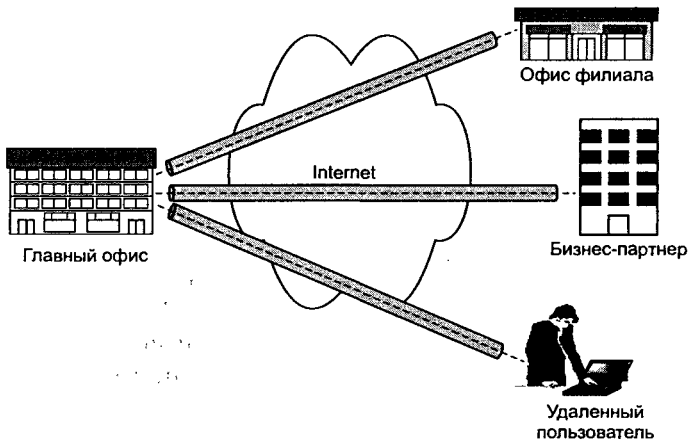


Рис. 10.1. Виртуальная защищенная сеть VPN

Для этих функций характерна взаимосвязь друг с другом. При их реализации используются криптографические методы защиты информации. Эффективность такой защиты обеспечивается за счет совместного использования симметричных и асимметричных криптографических систем. Туннель VPN, формируемый устройствами VPN, обладает свойствами защищенной выделенной линии, которая развертывается в рамках общедоступной сети, например Интернета. Устройства VPN могут играть в виртуальных частных сетях роль VPN-клиента, VPN-сервера или шлюза безопасности VPN.

VPN-клиент представляет собой программный или программно-аппаратный комплекс, выполняемый обычно на базе персонального компьютера. Его сетевое ПО модифицируется для выполнения шифрования и аутентификации трафика, которым это устройство обменивается с другими VPN-клиентами, VPN-серверами или шлюзами безопасности VPN. Обычно реализация VPN-клиента представляет собой программное решение, дополняющее стандартную ОС — Windows NT/2000/XP или Unix.

VPN-сервер представляет собой программный или программно-аппаратный комплекс, устанавливаемый на компьютере, выполняющем функции сервера. VPN-сервер обеспечивает защиту серверов от НСД из внешних сетей, а также организацию защищенных соединений (ассоциаций) с отдельными компьютерами и с компьютерами из сегментов локальных сетей, защищенных соответствующими VPN-продуктами. VPN-сервер является функциональным аналогом продукта VPN-клиент для серверных платформ. Он отличается прежде всего расширенными ресурсами для поддержания множественных соединений с VPN-клиентами. VPN-сервер может поддерживать защищенные соединения с мобильными пользователями.

Шлюз безопасности VPN (*security gateway*) — это сетевое устройство, подключаемое к двум сетям и выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним. Размещен шлюз безопасности VPN так, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. Сетевое соединение шлюза VPN прозрачно для пользователей позади шлюза, и представляется им выделенной линией, хотя на самом деле прокладывается через открытую сеть с коммутацией пакетов. Адрес шлюза безопасности VPN указывается как внешний адрес входящего туннелируемого пакета, а внутренний адрес пакета является адресом

конкретного хоста позади шлюза. Шлюз безопасности VPN может быть реализован в виде отдельного программного решения, отдельного аппаратного устройства, а также в виде маршрутизатора или МЭ, дополненных функциями VPN.

Открытая внешняя среда передачи информации включает как каналы скоростной передачи данных, в качестве которой используется сеть Интернет, так и более медленные общедоступные каналы связи, в качестве которых обычно применяются каналы телефонной сети. Эффективность виртуальной частной сети VPN определяется степенью защищенности информации, циркулирующей по открытым каналам связи. Для безопасной передачи данных через открытые сети широко используют *инкапсуляцию* и *туннелирование*. С помощью методики туннелирования пакеты данных передаются через общедоступную сеть, как по обычному двухточечному соединению. Между каждой парой «отправитель — получатель данных» устанавливается своеобразный туннель — логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

Суть туннелирования состоит в том, чтобы инкапсулировать, т. е. «упаковать», передаваемую порцию данных, вместе со служебными полями, в новый «конверт». При этом пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Следует отметить, что туннелирование само по себе не защищает данные от НСД или искажения, но благодаря туннелированию появляется возможность полной криптографической защиты инкапсулируемых исходных пакетов. Чтобы обеспечить конфиденциальность передаваемых данных, отправитель шифрует исходные пакеты, упаковывает их во внешний пакет с новым IP-заголовком и отправляет по транзитной сети (рис. 10.2).

Особенность технологии туннелирования в том, что она позволяет зашифровывать исходный пакет целиком, вместе с заго-

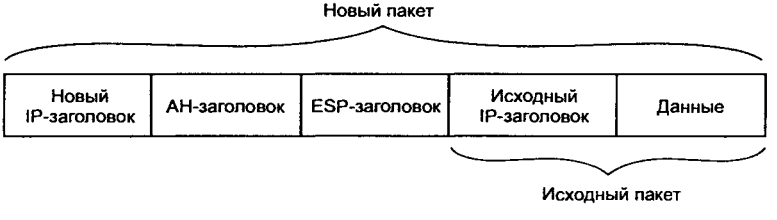


Рис. 10.2. Пример пакета, подготовленного для туннелирования

ловком, а не только его поле данных. Это важно, поскольку некоторые поля заголовка содержат информацию, которая может быть использована злоумышленником. В частности, из заголовка исходного пакета можно извлечь сведения о внутренней структуре сети — данные о количестве подсетей и узлов и их IP-адресах. Злоумышленник может использовать такую информацию при организации атак на корпоративную сеть. Исходный пакет с зашифрованным заголовком не может быть использован для организации транспортировки по сети. Поэтому для защиты исходного пакета применяют его инкапсуляцию и туннелирование. Исходный пакет зашифровывают полностью, вместе с заголовком, и затем этот зашифрованный пакет помещают в другой внешний пакет с открытым заголовком. Для транспортировки данных по открытой сети используются открытые поля заголовка внешнего пакета.

По прибытии в конечную точку защищенного канала из внешнего пакета извлекают внутренний исходный пакет, расшифровывают его и используют его восстановленный заголовок для дальнейшей передачи по внутренней сети (рис. 10.3).

Туннелирование может быть использовано для защиты не только конфиденциальности содержимого пакета, но и его целостности и аутентичности, при этом электронную цифровую подпись можно распространить на все поля пакета.

В дополнение к сокрытию сетевой структуры между двумя точками, туннелирование может также предотвратить возмож-

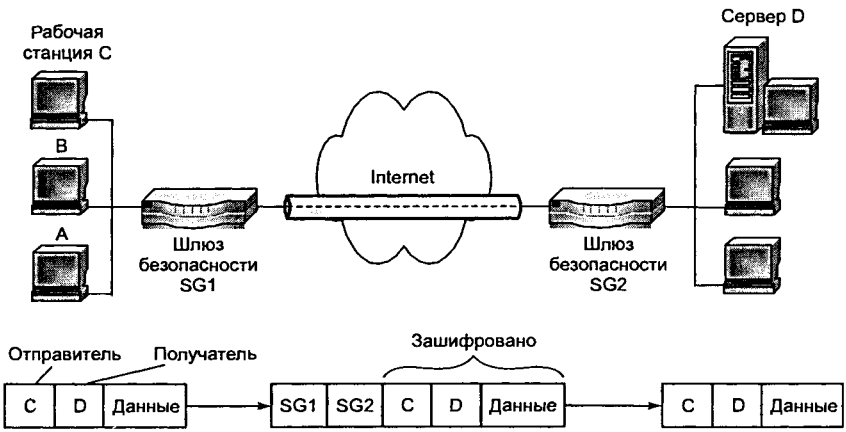


Рис. 10.3. Схема виртуального защищенного туннеля

ный конфликт адресов между двумя локальными сетями. При создании локальной сети, не связанной с Internet, компания может использовать любые IP-адреса для своих сетевых устройств и компьютеров. При объединении ранее изолированных сетей эти адреса могут начать конфликтовать друг с другом и с адресами, которые уже используются в Internet. Инкапсуляция пакетов решает эту проблему, поскольку позволяет скрыть первоначальные адреса и добавить новые, уникальные в пространстве IP-адресов Internet, которые затем используются для пересылки данных по разделяемым сетям. Сюда же входит задача настройки IP-адреса и других параметров для мобильных пользователей, подключающихся к локальной сети.

Механизм туннелирования широко применяется в различных протоколах формирования защищенного канала. Обычно туннель создается только на участке открытой сети, где существует угроза нарушения конфиденциальности и целостности данных, например между точкой входа в открытый Интернет и точкой входа в корпоративную сеть. При этом для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних исходных пакетах в защищенном виде. Следует отметить, что сам механизм туннелирования не зависит от того, с какой целью применяется туннелирование. Туннелирование может применяться не только для обеспечения конфиденциальности и целостности всей передаваемой порции данных, но и для организации перехода между сетями с разными протоколами (например, IPv4 и IPv6). Туннелирование позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол. В результате появляется возможность решить проблемы взаимодействия нескольких разнотипных сетей, начиная с необходимости обеспечения целостности и конфиденциальности передаваемых данных и заканчивая преодолением несоответствий внешних протоколов или схем адресации.

Реализацию механизма туннелирования можно представить как результат работы протоколов трех типов: протокола-«пассажира», несущего протокола и протокола туннелирования. Например, в качестве протокола-«пассажира» может быть использован транспортный протокол IPX, переносящий данные в локальных сетях филиалов одного предприятия. Наиболее распространенным вариантом несущего протокола является протокол IP сети Интернет. В качестве протоколов туннелирования могут быть ис-

пользованы протоколы канального уровня PPTP и L2TP, а также протокол сетевого уровня IPSec. Благодаря туннелированию становится возможным сокрытие инфраструктуры Internet от VPN-приложений.

Туннели VPN могут создаваться для различных типов конечных пользователей — либо это локальная сеть LAN (*local area network*) со шлюзом безопасности, либо отдельные компьютеры удаленных и мобильных пользователей. Для создания виртуальной частной сети крупного предприятия нужны VPN-шлюзы, VPN-серверы и VPN-клиенты. VPN-шлюзы целесообразно использовать для защиты локальных сетей предприятия, VPN-серверы и VPN-клиенты используют для организации защищенных соединений удаленных и мобильных пользователей с корпоративной сетью через Интернет.

10.1.2. Варианты построения виртуальных защищенных каналов

Безопасность информационного обмена необходимо обеспечивать как в случае объединения локальных сетей, так и в случае доступа к локальным сетям удаленных или мобильных пользователей [62]. При проектировании VPN обычно рассматриваются две основные схемы:

1) виртуальный защищенный канал между локальными сетями (канал ЛВС—ЛВС);

2) виртуальный защищенный канал между узлом и локальной сетью (канал клиент—ЛВС) (рис. 10.4).

Схема 1 соединения позволяет заменить дорогостоящие выделенные линии между отдельными офисами и создать постоянно доступные защищенные каналы между ними. В этом случае шлюз безопасности служит интерфейсом между туннелем и локальной сетью, при этом пользователи локальных сетей используют туннель для общения друг с другом. Многие компании используют данный вид VPN в качестве замены или дополнения к имеющимся соединениям глобальной сети, таким как frame relay.

Схема 2 защищенного канала VPN предназначена для установления соединений с удаленными или мобильными пользователями. Создание туннеля инициирует клиент (удаленный пользователь). Для связи со шлюзом, защищающим удаленную сеть, он запускает на своем компьютере специальное клиентское ПО.

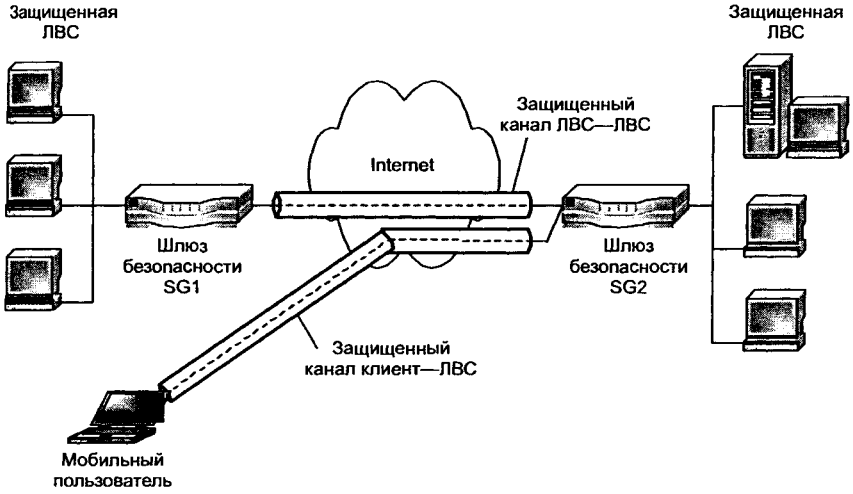


Рис. 10.4. Виртуальные защищенные каналы типа ЛВС—ЛВС и клиент—ЛВС

Этот вид VPN заменяет собой коммутируемые соединения и может использоваться наряду с традиционными методами удаленного доступа.

Существуют варианты схем виртуальных защищенных каналов. В принципе любой из двух узлов виртуальной корпоративной сети, между которыми формируется виртуальный защищенный канал, может принадлежать конечной или промежуточной точке защищаемого потока сообщений.

С точки зрения обеспечения информационной безопасности лучшим является вариант, при котором конечные точки защищенного туннеля совпадают с конечными точками защищаемого потока сообщений. В этом случае обеспечивается защищенность канала вдоль всего пути следования пакетов сообщений. Однако такой вариант ведет к децентрализации управления и избыточности ресурсных затрат. В этом случае необходима установка средств создания VPN на каждом клиентском компьютере локальной сети. Это усложняет централизованное управление доступом к компьютерным ресурсам и не всегда оправдано экономически. Отдельное администрирование каждого клиентского компьютера с целью конфигурирования в нем средств защиты является достаточно трудоемкой процедурой в большой сети.

Если внутри локальной сети, входящей в виртуальную сеть, не требуется защита трафика, тогда в качестве конечной точки

защищенного туннеля можно выбрать МЭ или пограничный маршрутизатор этой локальной сети. Если же поток сообщений внутри локальной сети должен быть защищен, тогда в качестве конечной точки туннеля в этой сети должен выступать компьютер, который участвует в защищенном взаимодействии. При доступе к локальной сети удаленного пользователя компьютер этого пользователя должен быть конечной точкой виртуального защищенного канала.

Достаточно распространенным является вариант, когда защищенный туннель прокладывается только внутри открытой сети с коммутацией пакетов, например внутри Интернета. Этот вариант отличается удобством применения, но обладает сравнительно низкой безопасностью. В качестве конечных точек такого туннеля обычно выступают провайдеры Интернета или пограничные маршрутизаторы (межсетевые экраны) локальной сети.

При объединении локальных сетей туннель формируется только между пограничными провайдерами Интернета, или маршрутизаторами (межсетевыми экранами) локальной сети. При удаленном доступе к локальной сети туннель создается между сервером удаленного доступа провайдера Интернета, а также пограничным провайдером Интернета или маршрутизатором (межсетевым экраном) локальной сети. Построенные по данному варианту виртуальные корпоративные сети обладают хорошей масштабируемостью и управляемостью. Сформированные защищенные туннели полностью прозрачны для клиентских компьютеров и серверов локальной сети, входящей в такую виртуальную сеть. ПО этих узлов остается без изменений. Однако данный вариант характеризуется сравнительно низкой безопасностью информационного взаимодействия, поскольку частично трафик проходит по открытым каналам связи в незащищенном виде. Если создание и эксплуатацию такой VPN берет на себя провайдер ISP, тогда вся виртуальная частная сеть может быть построена на его шлюзах прозрачно для локальных сетей и удаленных пользователей предприятия. Но в этом случае возникают проблемы доверия к провайдеру и постоянной оплаты его услуг.

Защищенный туннель создается компонентами виртуальной сети, функционирующими на узлах, между которыми формируется туннель. Эти компоненты принято называть инициатором туннеля и терминатором туннеля.

Инициатор туннеля инкапсулирует исходный пакет в новый пакет, содержащий новый заголовок с информацией об отправи-

теле и получателе. Инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты немаршрутизируемых протоколов, например NetBEUI. Все передаваемые по туннелю пакеты являются пакетами IP. Маршрут между инициатором и терминатором туннеля определяет обычная маршрутизируемая сеть IP, которая может быть сетью, отличной от Интернета.

Инициировать и разрывать туннель могут различные сетевые устройства и ПО. Например, туннель может быть инициирован ноутбуком мобильного пользователя, оборудованным модемом и соответствующим ПО для установления соединений удаленного доступа. В качестве инициатора может выступить также маршрутизатор локальной сети, наделенный соответствующими функциональными возможностями. Туннель обычно завершается коммутатором сети или шлюзом провайдера услуг.

Терминатор туннеля выполняет процесс, обратный инкапсуляции. Терминатор удаляет новые заголовки и направляет каждый исходный пакет адресату в локальной сети.

Конфиденциальность инкапсулируемых пакетов обеспечивается путем их шифрования, а целостность и подлинность — путем формирования электронной цифровой подписи. Существует множество методов и алгоритмов криптографической защиты данных, поэтому необходимо, чтобы инициатор и терминатор туннеля своевременно согласовали друг с другом и использовали одни и те же методы и алгоритмы защиты. Для обеспечения возможности расшифровывания данных и проверки цифровой подписи при приеме инициатор и терминатор туннеля должны также поддерживать функции безопасного обмена ключами. Кроме того, конечные стороны информационного взаимодействия должны пройти аутентификацию, чтобы гарантировать создание туннелей VPN только между уполномоченными пользователями.

Существующая сетевая инфраструктура корпорации может быть подготовлена к использованию VPN как с помощью программного, так и с помощью аппаратного обеспечения.

10.1.3. Средства обеспечения безопасности VPN

При построении защищенной виртуальной сети VPN первостепенное значение имеет задача обеспечения информационной безопасности. Согласно общепринятому определению, под безопасностью данных понимают их конфиденциальность, целост-

ность и доступность. Применительно к задачам VPN критерии безопасности данных могут быть определены следующим образом:

- *конфиденциальность* — гарантия того, что в процессе передачи данных по защищенным каналам VPN эти данные могут быть известны только легальным отправителю и получателю;
- *целостность* — гарантия сохранности передаваемых данных во время прохождения по защищенному каналу VPN. Любые попытки изменения, модификации, разрушения или создания новых данных будут обнаружены и станут известны легальным пользователям;
- *доступность* — гарантия того, что средства, выполняющие функции VPN, постоянно доступны легальным пользователям. Доступность средств VPN является комплексным показателем, который зависит от надежности реализации, качества обслуживания и степени защищенности самого средства от внешних атак.

Конфиденциальность обеспечивается с помощью различных методов и алгоритмов симметричного и асимметричного шифрования. Целостность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на асимметричных методах шифрования и односторонних функциях.

Аутентификация осуществляется на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт, протоколов строгой аутентификации, обеспечивает установление VPN-соединения только между легальными пользователями и предотвращает доступ к средствам VPN нежелательных лиц.

Авторизация подразумевает предоставление абонентам, доказавшим свою легальность (аутентичность), разных видов обслуживания, в частности разных способов шифрования их трафика. Авторизация и управление доступом часто реализуются одними и теми же средствами.

Для обеспечения безопасности передаваемых данных в виртуальных защищенных сетях должны быть решены следующие основные задачи сетевой безопасности:

- взаимная аутентификация абонентов при установлении соединения;
- обеспечение конфиденциальности, целостности и аутентичности передаваемой информации;

- авторизация и управление доступом;
- безопасность периметра сети и обнаружение вторжений;
- управление безопасностью сети.

Аутентификация абонентов. Процедура аутентификации (установление подлинности) разрешает вход для легальных пользователей и предотвращает доступ к сети нежелательных лиц.

Методы, алгоритмы и ряд протоколов аутентификации подробно рассмотрены в гл. 7; протоколы и системы аутентификации удаленных пользователей приведены в гл. 13.

Обеспечение конфиденциальности, целостности и аутентичности информации. Задача обеспечения конфиденциальности информации заключается в защите передаваемых данных от несанкционированного чтения и копирования. Основным средством обеспечения конфиденциальности информации является шифрование.

Алгоритмы шифрования и электронной цифровой подписи рассмотрены в гл. 6.

Авторизация и управление доступом. Ключевым компонентом безопасности VPN является гарантия того, что доступ к компьютерным ресурсам получают авторизованные пользователи, в то время как для неавторизованных пользователей сеть полностью закрыта.

При построении программных средств авторизации применяются:

- централизованная схема авторизации;
- децентрализованная схема авторизации.

Основное назначение централизованной системы авторизации — реализовать принцип единого входа. Управление процессом предоставления ресурсов пользователю осуществляется сервером. Централизованный подход к процессу авторизации реализован в системах Kerberos, RADIUS и TACACS.

В последнее время активно развивается так называемое *ролевое управление доступом*. Оно решает не столько проблемы безопасности, сколько улучшает управляемость систем. Суть ролевого управления доступом заключается в том, что между пользователями и их привилегиями помещают промежуточные сущности — роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему вполне определенные права.

Поскольку ролей много меньше, чем пользователей и привилегий, использование ролей способствует понижению сложности

и, следовательно, улучшению управляемости системы. Кроме того, на основании ролевой модели управления доступом можно реализовать такой важный принцип, как разделение обязанностей (например, невозможность в одиночку скомпрометировать критически важный процесс).

Управление доступом и организация защищенного удаленного доступа рассматриваются в гл. 13.

Безопасность периметра сети и обнаружение вторжений. Жесткий контроль доступа к приложениям, сервисам и ресурсам защищаемой сети является важной функцией правильно построенной сети. Использование таких средств безопасности, как МЭ, системы обнаружения вторжений, системы аудита безопасности, антивирусные комплексы обеспечивает системную защиту перемещаемых по сети данных.

Важной частью общего решения безопасности сети являются МЭ, которые контролируют трафик, пересекающий периметр защищаемой сети и накладывают ограничения на пропуск трафика в соответствии с политикой безопасности организации (см. гл. 3).

Дополнительным элементом гарантии безопасности периметра сети является система обнаружение вторжений IDS (Intrusion Detection System), работающая в реальном времени и предназначенная для обнаружения, фиксации и прекращения неавторизованной сетевой активности как от внешних, так и от внутренних источников.

Системы анализа защищенности сканируют корпоративную сеть с целью выявления потенциальных уязвимостей безопасности, давая возможность менеджерам сети лучше защитить сеть от атак.

Системы антивирусной защиты описаны в гл. 14, системы обнаружения вторжений и системы анализа защищенности рассматриваются в гл. 15.

Управление безопасностью сети. Сети VPN интегрируют как сами сетевые устройства, так и многочисленные сервисы управления безопасностью и пропускной способностью. Компаниям необходимо целостное управление этими устройствами и сервисами через инфраструктуру VPN, включая пользователей удаленного доступа и средств extranet. В связи с этим управление средствами VPN становится одной из важнейших задач обеспечения эффективного функционирования VPN. Система управления корпоративной сетью должна включать необходимый на-

бор средств для управления политиками безопасности, устройствами и сервисами VPN любого масштаба.

Система управления безопасностью сети является краеугольным камнем семейства продуктов, обеспечивающих сквозную безопасность VPN. Для обеспечения высокого уровня безопасности и управляемости VPN, и в частности системы распределения криптографических ключей и сертификатов, необходимо обеспечить централизованное скоординированное управление безопасностью всей защищаемой корпоративной сети.

Методы и средства управления сетевой безопасностью рассматриваются в гл. 16.

10.2. VPN-решения для построения защищенных сетей

В настоящее время технологии построения виртуальных защищенных частных сетей (VPN) привлекают все больше внимания со стороны крупных компаний (банков, ведомств, крупных государственных структур и т. д.). Причина такого интереса заключается в том, что VPN-технологии действительно дают возможность не только существенно сократить расходы на содержание выделенных каналов связи с удаленными подразделениями (филиалами), но и повысить конфиденциальность обмена информацией.

VPN-технологии позволяют организовывать защищенные туннели как между офисами компании, так и к отдельным рабочим станциям и серверам. Потенциальным клиентам предлагается широкий спектр оборудования и ПО для создания виртуальных защищенных сетей — от интегрированных многофункциональных и специализированных устройств до чисто программных продуктов.

10.2.1. Классификация сетей VPN

Благодаря технологии VPN многие компании начинают строить свою стратегию с учетом использования Интернета в качестве главного средства передачи информации, причем даже той, которая является уязвимой или жизненно важной.

Существуют разные признаки классификации VPN. Наиболее часто используются:

- «рабочий» уровень модели OSI;
- архитектура технического решения VPN;
- способ технической реализации VPN.

Классификация VPN по «рабочему» уровню модели OSI

Для технологий безопасной передачи данных по общедоступной (незащищенной) сети применяют обобщенное название — *защищенный канал* (*secure channel*). Термин «канал» подчеркивает тот факт, что защита данных обеспечивается между двумя узлами сети (хостами или шлюзами) вдоль некоторого виртуального пути, проложенного в сети с коммутацией пакетов.

Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях модели взаимодействия открытых систем OSI (рис. 10.5).

Рис. 10.5. Уровни протоколов защищенного канала

Класификация VPN по «рабочему» уровню модели OSI представляет значительный интерес, поскольку от выбранного уровня OSI во многом зависит функциональность реализуемой VPN и ее совместимость с приложениями КИС, а также с другими средствами защиты.

По признаку «рабочего» уровня модели OSI различают следующие группы VPN:

- VPN канального уровня;
- VPN сетевого уровня;
- VPN сеансового уровня.

VPN канального уровня. Средства VPN, используемые на канальном уровне модели OSI, позволяют обеспечить инкапсуляцию различных видов трафика третьего уровня (и выше) и построение виртуальных туннелей типа «точка—точка» (от маршрутизатора к маршрутизатору или от персонального компьютера к шлюзу ЛВС). К этой группе относятся VPN-продукты, которые используют протоколы L2F (Layer 2 Forwarding) и PPTP (Point-to-Point Tunneling Protocol), а также стандарт L2TP (Layer 2 Tunneling Protocol), разработанный совместно фирмами Cisco Systems и Microsoft.

VPN сетевого уровня. VPN-продукты сетевого уровня выполняют инкапсуляцию IP в IP. Одним из широко известных протоколов на этом уровне является протокол IPSec (IP Security), предназначенным для аутентификации, туннелирования и шифрования IP-пакетов. Стандартизованный консорциумом Internet Engineering Task Force (IETF) протокол IPSec вобрал в себя все лучшие решения по шифрованию пакетов и должен войти в качестве обязательного компонента в протокол IPv6.

С протоколом IPSec связан протокол IKE (Internet Key Exchange), решающий задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами. Протокол IKE автоматизирует обмен ключами и устанавливает защищенное соединение, тогда как IPSec кодирует и «подписывает» пакеты. Кроме того, IKE позволяет изменять ключ для уже установленного соединения, что повышает конфиденциальность передаваемой информации.

VPN сеансового уровня. Некоторые VPN используют другой подход под названием «посредники каналов» (circuit proxy). Этот метод функционирует над транспортным уровнем и ретранслирует трафик из защищенной сети в общедоступную сеть Internet для каждого сокета в отдельности. (Сокет IP идентифицируется комбинацией TCP-соединения и конкретного порта или заданным портом UDP. Стек TCP/IP не имеет пятого — сеансового — уровня, однако ориентированные на сокеты операции часто называют операциями сеансового уровня.)

Шифрование информации, передаваемой между инициатором и терминатором туннеля, часто осуществляется с помощью защиты транспортного уровня TLS (Transport Layer Security). Для стандартизации аутентифицированного прохода через МЭ консорциум IETF определил протокол под названием SOCKS, и в

настоящее время протокол SOCKS v.5 применяется для стандартизованной реализации посредников каналов.

Протоколы защиты на канальном, транспортном и сеансовом уровнях подробно рассматриваются в гл. 11. Особенности защиты на сетевом уровне с помощью протоколов IPSec и IKE разбираются в гл. 12.

Классификация VPN по архитектуре технического решения

По архитектуре технического решения принято выделять три основных вида виртуальных частных сетей:

- внутрикорпоративные VPN (Intranet VPN);
- VPN с удаленным доступом (Remote Access VPN);
- межкорпоративные VPN (Extranet VPN).

Внутрикорпоративные сети VPN предназначены для обеспечения защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными сетями связи, включая выделенные линии.

VPN с удаленным доступом предназначены для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам мобильным и/или удаленным (home-office) сотрудникам компании.

Межкорпоративные сети VPN предназначены для обеспечения защищенного обмена информацией со стратегическими партнерами по бизнесу, поставщиками, крупными заказчиками, пользователями, клиентами и т. д. Extranet VPN обеспечивает прямой доступ из сети одной компании к сети другой компании и тем самым способствует повышению надежности связи, поддерживаемой в ходе делового сотрудничества.

Следует отметить, что в последнее время наблюдается тенденция к конвергенции различных конфигураций VPN.

Классификация VPN по способу технической реализации

Конфигурация и характеристики виртуальной частной сети во многом определяются типом применяемых VPN-устройств.

По способу технической реализации различают VPN на основе:

- маршрутизаторов;
- межсетевых экранов;
- программных решений;

- специализированных аппаратных средств со встроенными шифропроцессорами.

VPN на основе маршрутизаторов. Данный способ построения VPN предполагает применение маршрутизаторов для создания защищенных каналов. Поскольку вся информация, исходящая из локальной сети, проходит через маршрутизатор, то вполне естественно возложить на него и задачи шифрования. Пример оборудования для VPN на маршрутизаторах — устройства компании Cisco Systems.

VPN на основе межсетевых экранов. МЭ большинства производителей поддерживают функции туннелирования и шифрования данных, например продукт FireWall-1 компании Check Point Software Technologies. При использовании МЭ на базе ПК нужно помнить, что подобное решение подходит только для небольших сетей с небольшим объемом передаваемой информации. Недостатками этого метода являются высокая стоимость решения в пересчете на одно рабочее место и зависимость производительности от аппаратного обеспечения, на котором работает МЭ.

VPN на основе программного обеспечения. VPN-продукты, реализованные программным способом, с точки зрения производительности уступают специализированным устройствам, однако обладают достаточной мощностью для реализации VPN-сетей. Следует отметить, что в случае удаленного доступа требования к необходимой полосе пропускания невелики. Поэтому чисто программные продукты легко обеспечивают производительность, достаточную для удаленного доступа. Несомненным достоинством программных продуктов является гибкость и удобство в применении, а также относительно невысокая стоимость.

VPN на основе специализированных аппаратных средств. Главное преимущество таких VPN — высокая производительность, поскольку быстродействие обусловлено тем, что шифрование в них осуществляется специализированными микросхемами. Специализированные VPN-устройства обеспечивают высокий уровень безопасности, однако они дóроги.

10.2.2. Основные варианты архитектуры VPN

Существует множество разновидностей виртуальных частных сетей. Их спектр варьирует от провайдерских сетей, позволяющих управлять обслуживанием клиентов непосредственно на их пло-

щадях, до корпоративных сетей VPN, разворачиваемых и управляемых самими компаниями. Тем не менее, принято выделять три основных вида виртуальных частных сетей: VPN с удаленным доступом (Remote Access VPN), внутрикорпоративные VPN (Intranet VPN) и межкорпоративные VPN (Extranet VPN) [9].

VPN с удаленным доступом (рис. 10.6) позволяют значительно сократить ежемесячные расходы на использование коммутируемых и выделенных линий. Принцип их работы прост: пользователи устанавливают соединения с местной точкой доступа к глобальной сети, после чего их вызовы туннелируются через Интернет, что избавляет от платы за междугородную и международную связь или выставления счетов владельцам бесплатных междугородных номеров; затем все вызовы концентрируются на соответствующих узлах и передаются в корпоративные сети.

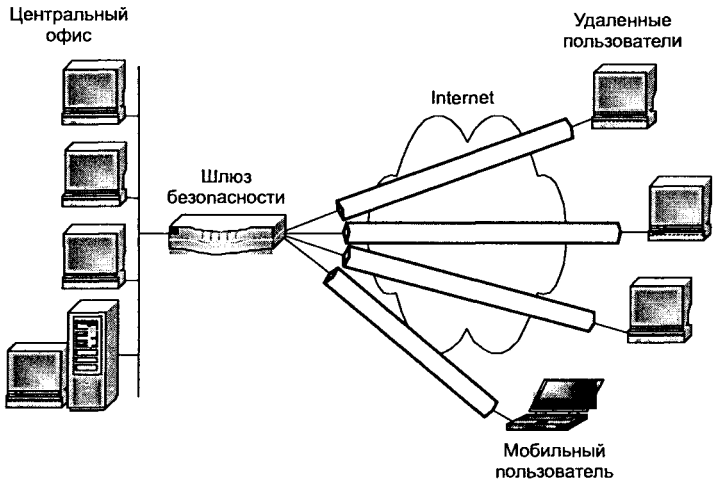


Рис. 10.6. Виртуальная частная сеть с удаленным доступом

Преимущества перехода от частно управляемых dial networks к Remote Access VPN:

- возможность использования местных dial-in numbers вместо междугородних позволяет значительно снизить затраты на междугородние телекоммуникации;
- эффективная система установления подлинности удаленных и мобильных пользователей обеспечивает надежное проведение процедуры аутентификации;

- высокая масштабируемость и простота развертывания для новых пользователей, добавляемых к сети;
- сосредоточение внимания компании на основных корпоративных бизнес-целях вместо отвлечения на проблемы обеспечения работы сети.

Существенная экономия при использовании Remote Access VPN является мощным стимулом, однако применение открытого Internet в качестве объединяющей магистрали для транспорта чувствительного корпоративного трафика становится все более масштабным, что делает механизмы защиты информации жизненно важными элементами данной технологии.

Внутрикорпоративные сети VPN (рис. 10.7) строятся с использованием Internet или разделяемых сетевых инфраструктур, предоставляемых сервис-провайдерами. Компании достаточно отказаться от использования дорогостоящих выделенных линий, заменив их более дешевой связью через Internet. Это существенно сокращает расходы на использование полосы пропускания, поскольку в Internet расстояние никак не влияет на стоимость соединения.

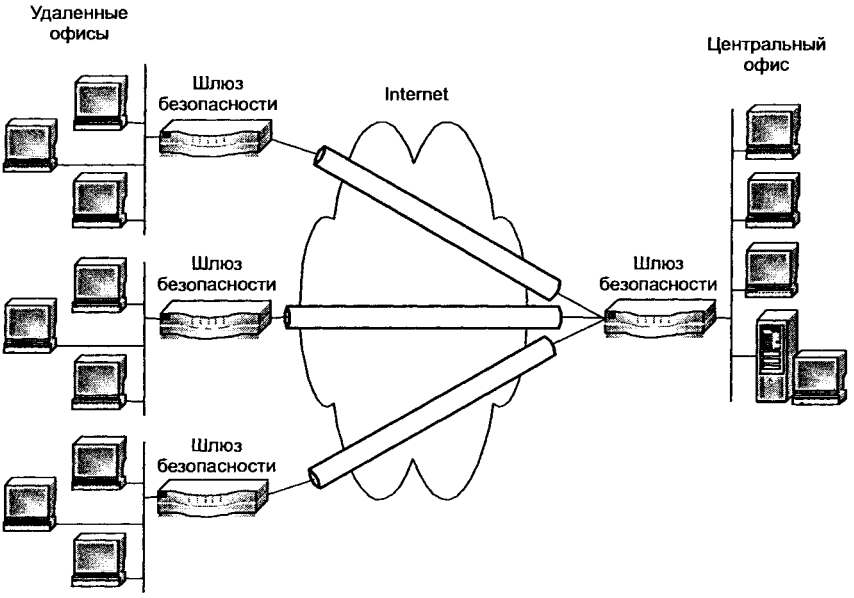


Рис. 10.7. Соединение узлов сети с помощью технологии Intranet VPN

Достоинства Intranet VPN:

- применение мощных криптографических протоколов шифрования данных для защиты конфиденциальной информации;
- надежность функционирования при выполнении таких критических приложений, как системы автоматизированной продажи и системы управления базами данных;
- гибкость управления эффективным размещением быстро возрастающего числа новых пользователей, новых офисов и новых программных приложений.

Построение Intranet VPN, использующее Internet, является самым рентабельным способом реализации VPN-технологии. Однако в Internet уровни сервиса вообще не гарантируются. Компании, которым требуются гарантированные уровни сервиса, должны рассмотреть возможность развертывания своих VPN с использованием разделяемых сетевых инфраструктур, предоставляемых сервис-провайдерами.

Межкорпоративная сеть VPN (рис. 10.8) — это сетевая технология, которая обеспечивает прямой доступ из сети одной компании к сети другой компании и, таким образом, способствует повышению надежности связи, поддерживаемой в ходе делового сотрудничества.

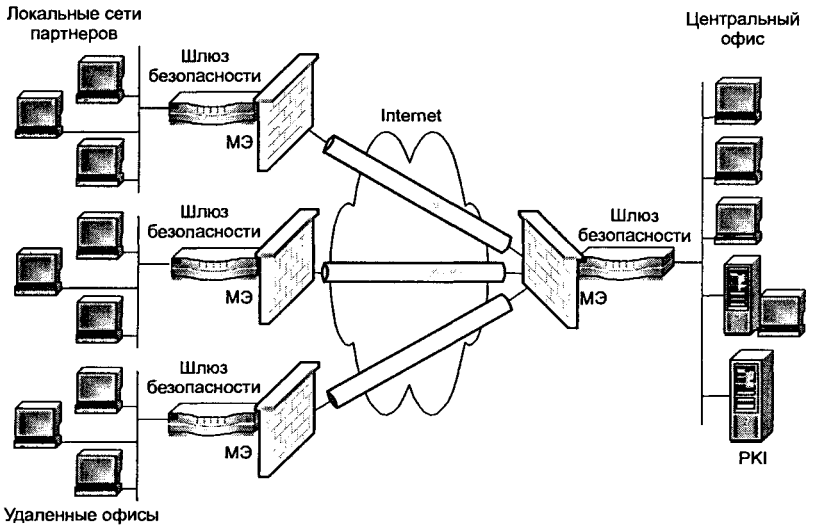


Рис. 10.8. Межкорпоративная сеть Extranet VPN

Сети Extranet VPN в целом похожи на внутрикорпоративные виртуальные частные сети с той лишь разницей, что проблема защиты информации является для них более острой. Для Extranet VPN характерно использование стандартизированных VPN-продуктов, гарантирующих способность к взаимодействию с различными VPN-решениями, которые деловые партнеры могли бы применять в своих сетях.

Когда несколько компаний принимают решение работать вместе и открывают друг для друга свои сети, они должны позаботиться о том, чтобы их новые партнеры имели доступ только к определенной информации. При этом конфиденциальная информация должна быть надежно защищена от несанкционированного использования. Именно поэтому в межкорпоративных сетях большое значение придается контролю доступа из открытой сети посредством МЭ. Важна и аутентификация пользователей, призванная гарантировать, что доступ к информации получают только те, кому он действительно разрешен. Вместе с тем, развернутая система защиты от несанкционированного доступа не должна привлекать к себе внимания.

Соединения Extranet VPN развертываются, используя те же архитектуру и протоколы, которые применяются при реализации Intranet VPN и Remote Access VPN. Основное различие заключается в том, что разрешение доступа, которое дается пользователям Extranet VPN, связано с сетью их партнера.

Иногда в отдельную группу выделяют локальный вариант сети VPN (Localnet VPN). Локальная сеть Localnet VPN обеспечивает защиту информационных потоков, циркулирующих внутри локальных сетей компании (как правило, Центрального офиса), от НСД со стороны «излишне любопытных» сотрудников самой компании. В настоящее время наблюдается тенденция к конвергенции различных способов реализаций VPN [9, 65].

10.3. Достоинства применения технологий VPN

Эффективное применение ИТ в сочетании с технологиями в области информационной безопасности является важнейшим стратегическим фактором повышения конкурентоспособности современных предприятий и организаций. Технология виртуальных частных сетей VPN позволяет решать эти задачи, обеспечи-

вая связь между сетями, а также между удаленным пользователем и корпоративной сетью с помощью защищенного канала (туннеля), «проложенного» в общедоступной сети Интернет.

Достоинства использования VPN-технологий для защиты информации в распределенных сетевых ИС масштаба предприятия:

- возможность защиты всей корпоративной сети — от крупных локальных сетей офисов до отдельных рабочих мест. Защита может быть распространена на все звенья сети — от сегментов локальных сетей до коммуникационных каналов глобальных сетей, в том числе выделенных и коммутируемых линий;
- масштабируемость системы защиты, т. е. для защиты объектов различной сложности и производительности можно использовать адекватные по уровню сложности, производительности и стоимости программные или программно-аппаратные средства защиты;
- использование ресурсов открытых сетей в качестве отдельных коммуникационных звеньев корпоративной сети; все угрозы, возникающие при использовании сетей общего пользования, будут компенсироваться средствами защиты информации;
- обеспечение подконтрольности работы сети и достоверная идентификация всех источников информации. При необходимости может быть обеспечена аутентификация трафика на уровне отдельных пользователей;
- сегментация ИС и организация безопасной эксплуатации системы, обрабатывающей информацию различных уровней конфиденциальности, программными и программно-аппаратными средствами защиты информации.

Технология VPN входит в число важнейших технологий, которые планируют использовать предприятия в ближайшем будущем.

Глава 11
ЗАЩИТА НА КАНАЛЬНОМ И СЕАНСОВОМ УРОВНЯХ

Виртуальный защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях модели взаимодействия открытых систем OSI. От выбранного рабочего уровня OSI зависит функциональность реализуемой VPN и ее совместимость с приложениями КИС, а также с другими средствами защиты.

Средства VPN, применяемые на *канальном уровне* модели OSI, позволяют обеспечить инкапсуляцию различных видов трафика третьего уровня (и выше) и построение виртуальных туннелей типа «точка—точка» (от маршрутизатора к маршрутизатору или от персонального компьютера к шлюзу ЛВС).

При построении защищенных виртуальных сетей на *сеансовом уровне* появляется возможность криптографической защиты информационного обмена, включая аутентификацию, а также реализации ряда функций посредничества между взаимодействующими сторонами.

11.1. Протоколы формирования защищенных каналов на канальном уровне

Протоколы PPTP (Point-to-Point Tunneling Protocol), L2F (Layer-2 Forwarding) и L2TP (Layer-2 Tunneling Protocol) — это протоколы туннелирования канального уровня модели OSI. Общим свойством этих протоколов является то, что они использу-

ются для организации защищенного многопротокольного удаленного доступа к ресурсам корпоративной сети через открытую сеть, например через Интернет.

Все три протокола — PPTP, L2F и L2TP — обычно относят к протоколам формирования защищенного канала, однако этому определению точно соответствует только протокол PPTP, который обеспечивает туннелирование и шифрование передаваемых данных. Протоколы L2F и L2TP поддерживают только функции туннелирования. Для защиты туннелируемых данных в этих протоколах необходимо использовать некоторый дополнительный протокол, в частности IPSec.

Клиентское ПО обычно использует для удаленного доступа стандартный протокол канального уровня PPP (Point-to-Point Protocol). Протоколы PPTP, L2F и L2TP основываются на протоколе PPP и являются его расширениями. Первоначально протокол PPP, расположенный на канальном уровне, был разработан для инкапсуляции данных и их доставки по соединениям типа «точка—точка». Этот протокол служит также для организации асинхронных (например, коммутируемых) соединений. В частности, в настройках коммутируемого доступа удаленных систем Windows 2000 или Windows 9x обычно указывается подключение к серверу по протоколу PPP.

В набор PPP входят протокол управления соединением LCP (Link Control Protocol), ответственный за конфигурацию, установку, работу и завершение соединения «точка—точка», и протокол управления сетью NCP (Network Control Protocol), способный инкапсулировать в PPP протоколы сетевого уровня для транспортировки через соединение «точка—точка». Это позволяет одновременно передавать пакеты Novell IPX и Microsoft IP по одному соединению PPP.

Для доставки конфиденциальных данных из одной точки в другую через сети общего пользования сначала производится инкапсуляция данных с помощью протокола PPP, затем протоколы PPTP и L2TP выполняют шифрование данных и собственную инкапсуляцию. После того как туннельный протокол доставляет пакеты из начальной точки туннеля в конечную, выполняется деинкапсуляция.

На физическом и канальном уровнях протоколы PPTP и L2TP идентичны, но на этом их сходство заканчивается и начинаются различия.

11.1.1. Протокол PPTP

Протокол PPTP (Point-to-Point Tunneling Protocol), разработанный компанией Microsoft при поддержке других компаний, предназначен для создания защищенных виртуальных каналов при доступе удаленных пользователей к локальным сетям через Интернет. Он предполагает создание криптозащищенного туннеля на канальном уровне модели OSI как для случая прямого соединения удаленного компьютера с открытой сетью, так и для случая подсоединения его к открытой сети по телефонной линии через провайдера [9, 32].

Протокол PPTP получил практическое распространение благодаря компании Microsoft, реализовавшей его в своих ОС Windows NT/2000. Некоторые производители МЭ и шлюзов VPN также поддерживают этот протокол. Протокол PPTP позволяет создавать защищенные каналы для обмена данными по протоколам IP, IPX или NetBEUI. Данные этих протоколов упаковываются в кадры PPP и затем инкапсулируются посредством протокола PPTP в пакеты протокола IP, с помощью которого переносятся в зашифрованном виде через любую сеть TCP/IP.

Пакеты, передаваемые в рамках сессии PPTP, имеют следующую структуру (рис. 11.1):

- заголовок канального уровня, используемый внутри Интернета, например заголовок кадра Ethernet;
- заголовок IP, содержащий адреса отправителя и получателя пакета;
- заголовок общего метода инкапсуляции для маршрутизации GRE (Generic Routing Encapsulation);
- исходный пакет PPP, включающий пакет IP, IPX или NetBEUI.

Рис. 11.1. Структура пакета для пересылки по туннелю PPTP

Принимающий узел сети извлекает из пакетов IP кадры PPP, а затем извлекает из кадра PPP исходный пакет IP, IPX или NetBEUI и отправляет его по локальной сети конкретному адресату. Многопротокольность инкапсулирующих протоколов ка-

нального уровня, к которым относится протокол PPTP, является их важным преимуществом перед протоколами защищенного канала более высоких уровней. Например, если в корпоративной сети используются IPX или NetBEUI, применение протоколов IPSec или SSL просто невозможно, поскольку они ориентированы только на один протокол сетевого уровня IP.

Такой способ инкапсуляции обеспечивает независимость от протоколов сетевого уровня модели OSI и позволяет осуществлять защищенный удаленный доступ через открытые IP-сети к любым локальным сетям (IP, IPX или NetBEUI). Согласно протоколу PPTP при создании защищенного виртуального канала производится аутентификация удаленного пользователя и шифрование передаваемых данных (рис. 11.2).

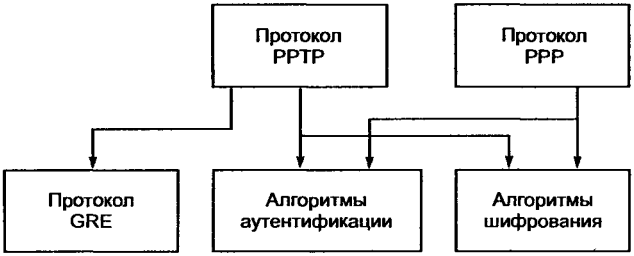


Рис. 11.2. Архитектура протокола PPTP

Для аутентификации удаленного пользователя могут использоваться различные протоколы, применяемые для PPP. В реализации PPTP, включенной компанией Microsoft в Windows 98/NT/2000, поддерживаются следующие протоколы аутентификации: протокол распознавания по паролю PAP (Password Authentication Protocol), протокол распознавания при рукопожатии MSCHAP (Microsoft Challenge-Handshaking Authentication Protocol) и протокол распознавания EAP-TLS (Extensible Authentication Protocol — Transport Layer Security). При использовании протокола PAP идентификаторы и пароли передаются по линии связи в незашифрованном виде, при этом только сервер проводит аутентификацию клиента. При использовании протоколов MSCHAP и EAP-TLS обеспечиваются защита от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем и взаимная аутентификация клиента и VPN-сервера.

Шифрование с помощью PPTP гарантирует, что никто не сможет получить доступ к данным при пересылке через Internet. Протокол шифрования MPPE (Microsoft Point-to-Point Encryption) совместим только с MSCHAP (версии 1 и 2) и EAP-TLS и умеет автоматически выбирать длину ключа шифрования при согласовании параметров между клиентом и сервером. Протокол MPPE поддерживает работу с ключами длиной 40, 56 или 128 бит. Протокол PPTP изменяет значение ключа шифрования после каждого принятого пакета.

Для протокола PPTP определены две основные схемы применения:

1) схема туннелирования при прямом соединении удаленного компьютера с Интернетом;

2) схема туннелирования при подключении удаленного компьютера к Интернету по телефонной линии через провайдера [32, 45].

Рассмотрим реализацию 1-й схемы туннелирования (рис. 11.3). Удаленный пользователь устанавливает удаленное соединение с локальной сетью с помощью клиентской части сервиса удаленного доступа RAS (Remote Access Service), входящего в состав Windows 98/NT. Затем пользователь обращается к серверу удаленного доступа локальной сети, указывая его IP-адрес, и устанавливает с ним связь по протоколу PPTP.

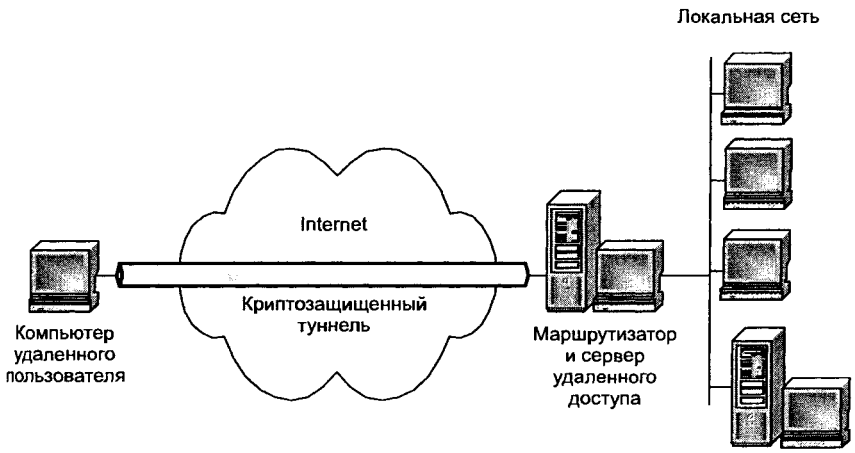


Рис. 11.3. Схема туннелирования при прямом подсоединении компьютера удаленного пользователя к Internet

Функции сервера удаленного доступа может выполнять пограничный маршрутизатор локальной сети. На компьютере удаленного пользователя должны быть установлены клиентская часть сервиса RAS и драйвер PPTP, которые входят в состав Windows 98/NT, а на сервере удаленного доступа локальной сети — сервер RAS и драйвер PPTP, входящие в состав Windows NT Server. Протокол PPTP определяет несколько служебных сообщений, которыми обмениваются взаимодействующие стороны. Служебные сообщения передаются по протоколу TCP. После успешной аутентификации начинается процесс защищенного информационного обмена. Внутренние серверы локальной сети могут не поддерживать протокол PPTP, поскольку пограничный маршрутизатор извлекает кадры PPP из пакетов IP и посылает их по локальной сети в необходимом формате — IP, IPX или NetBIOS.

2-я схема туннелирования не получила широкого распространения.

11.1.2. Протокол L2TP

Протокол L2F (Layer-2 Forwarding) был разработан компанией Cisco Systems для построения защищенных виртуальных сетей на канальном уровне модели OSI как альтернатива протоколу PPTP.

Однако в настоящее время он фактически поглощен протоколом L2TP, поэтому далее будут рассматриваться основные возможности и свойства протокола L2TP.

Протокол L2TP (Layer-2 Tunneling Protocol) разработан в организации IETF (Internet Engineering Task Force) при поддержке компаний Microsoft и Cisco Systems. Протокол L2TP разрабатывался как протокол защищенного туннелирования PPP-трафика через сети общего назначения с произвольной средой. Работа над этим протоколом велась на основе протоколов PPTP и L2F, и в результате он вобрал в себя лучшие качества исходных протоколов [9].

В отличие от PPTP, протокол L2TP не привязан к протоколу IP, поэтому он может быть использован в сетях с коммутацией пакетов, например в сетях ATM (Asynchronous Transfer Mode) или в сетях с ретрансляцией кадров (frame relay). Кроме того, в протокол L2TP добавлена важная функция управления потока-

ми данных, а также ряд отсутствующих в спецификации протокола PPTP функций защиты, в частности, включена возможность работы с протоколами AH и ESP стека протоколов IPSec (рис. 11.4).

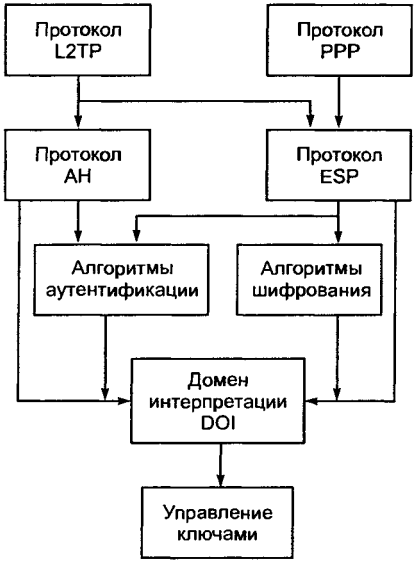


Рис. 11.4. Архитектура протокола L2TP

В сущности, гибридный протокол L2TP представляет собой расширение протокола PPP функциями аутентификации удаленных пользователей, создания защищенного виртуального соединения и управления потоками данных.

Протокол L2TP применяет в качестве транспорта протокол UDP и использует одинаковый формат сообщений как для управления туннелем, так и для пересылки данных.

Хотя протокол PPTP обеспечивает достаточную степень безопасности, но все же протокол L2TP (поверх IPSec) надежнее. Протокол L2TP (поверх IPSec) обеспечивает аутентификацию на уровнях «пользователь» и «компьютер», а также выполняет аутентификацию и шифрование данных.

После того как L2TP (поверх IPSec) завершает процесс аутентификации компьютера, выполняется аутентификация на уровне пользователя.

В отличие от своих предшественников — протоколов PPTP и L2F, протокол L2TP предоставляет возможность открывать между конечными абонентами сразу несколько туннелей, каждый из которых может быть выделен для отдельного приложения. Эти особенности обеспечивают гибкость и безопасность туннелирования.

Согласно спецификации протокола L2TP роль сервера удаленного доступа провайдера должен выполнять концентратор доступа LAC (L2TP Access Concentrator), который обеспечивает удаленному пользователю сетевой доступ к его локальной сети через Интернет. В качестве сервера удаленного доступа локальной сети должен выступать сетевой сервер LNS (L2TP Network Server), функционирующий на совместимых с протоколом PPP платформах (рис. 11.5).

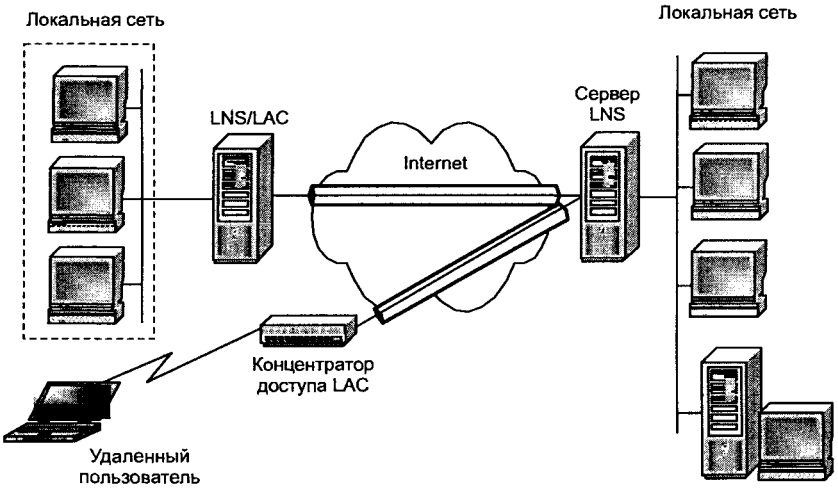


Рис. 11.5. Схемы туннелирования по протоколу L2TP

Формирование защищенного виртуального канала в протоколе L2TP осуществляется в три этапа:

- установление соединения с сервером удаленного доступа локальной сети;
- аутентификация пользователя;
- конфигурирование защищенного туннеля [9].

Следует отметить, что протокол L2TP не определяет конкретных методов криптозащиты и предполагает возможность приме-

нения различных стандартов шифрования. Если защищенный туннель планируется сформировать в IP-сетях, тогда для реализация криптозащиты используется протокол IPSec. Протокол L2TP поверх IPSec обеспечивает более высокую степень защиты данных, чем PPTP, так как использует алгоритм шифрования 3DES или AES. Если такой высокий уровень защиты не нужен, можно использовать алгоритм DES с одним 56-разрядным ключом. Кроме того, при помощи алгоритма HMAC (Hash Message Authentication Code) протокол L2TP обеспечивает аутентификацию данных, для чего этот алгоритм создает хэш длиной 128 разрядов.

Таким образом, функциональные возможности протоколов PPTP и L2TP различны. Протокол PPTP может применяться только в IP-сетях. Протокол L2TP может использоваться не только в IP-сетях. Протокол L2TP поверх IPSec предлагает больше уровней безопасности, чем PPTP, и может гарантировать почти 100%-ю безопасность важных для организации данных.

Однако при всех своих достоинствах протокол L2TP не смог преодолеть ряд недостатков туннельной передачи данных на канальном уровне:

- для реализации протокола L2TP необходима поддержка провайдеров ISP;
- протокол L2TP ограничивает трафик рамками выбранного туннеля и лишает пользователей доступа к другим частям Интернета;
- спецификация L2TP обеспечивает стандартное шифрование только в IP-сетях с помощью протокола IPSec.

11.2. Протоколы формирования защищенных каналов на сеансовом уровне

Самым высоким уровнем модели OSI, на котором возможно формирование защищенных виртуальных каналов, является пятый — сеансовый уровень. При построении защищенных виртуальных сетей на сеансовом уровне появляется возможность криптографической защиты информационного обмена, включая аутентификацию, а также реализации ряда функций посредничества между взаимодействующими сторонами.

Действительно, сеансовый уровень модели OSI отвечает за установку логических соединений и управление этими соедине-

ниями. Поэтому существует возможность применения на этом уровне программ-посредников, проверяющих допустимость запрошенных соединений и обеспечивающих выполнение других функций защиты межсетевого взаимодействия.

Однако на сеансовом уровне начинается непосредственная зависимость от приложений, реализующих высокоуровневые протоколы. Поэтому реализация протоколов защиты информационного обмена, соответствующих этому уровню, в большинстве случаев требует внесения изменений в высокоуровневые сетевые приложения.

Для защиты информационного обмена на сеансовом уровне широкое распространение получил протокол SSL (Secure Sockets Layer). Для выполнения на сеансовом уровне функций посредничества между взаимодействующими сторонами организацией IETF (Internet Engineering Task Force) в качестве стандарта принят протокол SOCKS [9].

11.2.1. Протоколы SSL/TLS

Протокол SSL применяется в качестве протокола защищенного канала, работающего на сеансовом уровне модели OSI. Этот протокол использует криптографические методы защиты информации для обеспечения безопасности информационного обмена. Протокол SSL выполняет все функции по созданию защищенного канала между двумя абонентами сети, включая их взаимную аутентификацию, обеспечение конфиденциальности, целостности и аутентичности передаваемых данных. Ядром протокола SSL является технология комплексного использования асимметричных и симметричных криптосистем.

Взаимная аутентификация обеих сторон в SSL выполняется путем обмена цифровыми сертификатами открытых ключей пользователей (клиента и сервера), заверенными цифровой подписью специальных сертификационных центров. Протокол SSL поддерживает сертификаты, соответствующие общепринятому стандарту X.509, а также стандарты инфраструктуры открытых ключей PKI (Public Key Infrastructure), с помощью которой организуется выдача и проверка подлинности сертификатов.

Конфиденциальность обеспечивается шифрованием передаваемых сообщений с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении со-

единения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов. Использование для защиты сообщений симметричных ключей связано с тем, что скорость процессов шифрования и расшифрования на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей. Подлинность и целостность циркулирующей информации обеспечивается за счет формирования и проверки электронной цифровой подписи.

В качестве алгоритмов асимметричного шифрования используются алгоритм RSA, а также алгоритм Диффи — Хеллмана. Допустимыми алгоритмами симметричного шифрования являются RC2, RC4, DES, 3DES и AES. Для вычисления хэш-функций могут применяться стандарты MD5 и SHA-1. В протоколе SSL версии 3.0 набор криптографических алгоритмов является расширяемым.

Согласно протоколу SSL криптозащищенные туннели создаются между конечными точками виртуальной сети. Инициаторами каждого защищенного туннеля являются клиент и сервер, функционирующие на компьютерах в конечных точках туннеля (рис. 11.6).

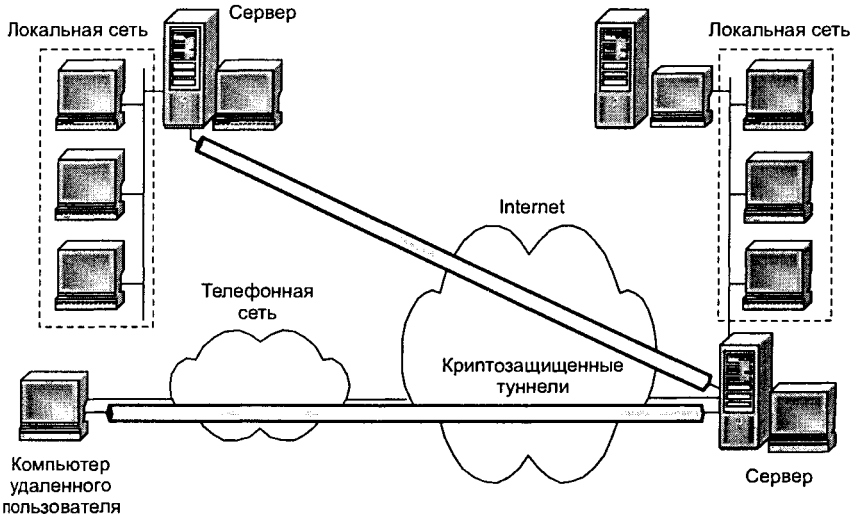


Рис. 11.6. Криптозащищенные туннели, сформированные на основе протокола SSL

Протокол SSL предусматривает следующие этапы взаимодействия клиента и сервера при формировании и поддержке защищаемого соединения:

- установление SSL-сессии;
- защищенное взаимодействие.

В процессе установления SSL-сессии решаются следующие задачи:

- аутентификация сторон;
- согласование криптографических алгоритмов и алгоритмов сжатия, которые будут использоваться при защищенном информационном обмене;
- формирование общего секретного мастер-ключа;
- генерация на основе сформированного мастер-ключа общих секретных сеансовых ключей для криптозащиты информационного обмена [9, 65].

Процедура установления SSL-сессии, называемая также процедурой рукопожатия, отрабатывается перед непосредственной защитой информационного обмена и выполняется по протоколу начального приветствия (Handshake Protocol), входящему в состав протокола SSL.

При установлении повторных соединений между клиентом и сервером стороны могут, по взаимному соглашению, формировать новые сеансовые ключи на основе «старого» общего «секрета» (данная процедура называется «продолжением» SSL сессии).

Протокол SSL 3.0 поддерживает три режима аутентификации:

- взаимную аутентификацию сторон;
- одностороннюю аутентификацию сервера без аутентификации клиента;
- полную анонимность.

При использовании последнего варианта обеспечивается защита информационного обмена без каких-либо гарантий относительно подлинности сторон. В этом случае взаимодействующие стороны не защищены от атак, связанных с подменой участников взаимодействия.

В реализациях протокола SSL для аутентификации взаимодействующих сторон и формирования общих секретных ключей обычно используют алгоритм RSA.

Соответствие между открытыми ключами и их владельцами устанавливается с помощью цифровых сертификатов, выдаваемых специальными центрами сертификации (см. гл. 13).

Протокол SSL прошел проверку временем, работая в популярных браузерах Netscape Navigator и Internet Explorer, а также Web-серверах ведущих производителей. В январе 1999 г. на смену версии SSL 3.0 пришел протокол TLS (Transport Layer Security), который базируется на протоколе SSL и в настоящее время является стандартом Интернета. Различия между протоколами SSL 3.0 и TLS 1.0 не слишком существенны. Протокол SSL стал промышленным протоколом, развиваемым и продвигаемым вне технических координирующих институтов Internet.

Протокол SSL поддерживается ПО серверов и клиентов, выпускаемых ведущими западными компаниями. Существенным недостатком протокола SSL является то, что практически все продукты, поддерживающие SSL, из-за экспортных ограничений доступны за пределами США лишь в усеченном варианте (с длиной сеансового ключа 40 бит для алгоритмов симметричного шифрования и 512 бит для алгоритма RSA, используемого на этапе установления SSL-сессии).

К недостаткам протоколов SSL и TLS можно отнести то, что для транспортировки своих сообщений они используют только один протокол сетевого уровня — IP, и, следовательно, могут работать только в IP-сетях.

Кроме того, в SSL для аутентификации и шифрования используются одинаковые ключи, что при определенных условиях может привести к потенциальной уязвимости. Подобное решение дает возможность собрать больше статистического материала, чем при аутентификации и шифровании разными ключами.

11.2.2. Протокол SOCKS

Протокол SOCKS организует процедуру взаимодействия клиент-серверных приложений на сеансовом уровне модели OSI через сервер-посредник, или proxy-сервер [9].

В общем случае программы-посредники, которые традиционно используются в МЭ, могут выполнять следующие функции:

- идентификацию и аутентификацию пользователей;
- криптозащиту передаваемых данных;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- фильтрацию и преобразование потока сообщений, например поиск вирусов и прозрачное шифрование информации;

- трансляцию внутренних сетевых адресов для исходящих потоков сообщений.

Первоначально протокол SOCKS разрабатывался только для перенаправления запросов к серверам со стороны клиентских приложений, а также возврата этим приложениям полученных ответов. Перенаправление запросов и ответов между клиент-серверными приложениями уже позволяет реализовать функцию трансляции сетевых IP-адресов NAT (Network Address Translation). Замена у исходящих пакетов внутренних IP-адресов отправителей одним IP-адресом шлюза позволяет скрыть топологию внутренней сети от внешних пользователей и тем самым усложнить задачу НСД.

На основе протокола SOCKS могут быть реализованы и другие функции посредничества по защите сетевого взаимодействия. Например, протокол SOCKS может применяться для контроля над направлениями информационных потоков и разграничения доступа в зависимости от атрибутов пользователей и информации. Эффективность использования протокола SOCKS для выполнения функций посредничества обеспечивается его ориентацией на сеансовый уровень модели OSI. По сравнению с посредниками прикладного уровня на сеансовом уровне достигается более высокое быстродействие и независимость от высокоуровневых протоколов (HTTP, FTP, POP3, SMTP и др.). Кроме того, протокол SOCKS не привязан к протоколу IP и не зависит от ОС. Например, для обмена информацией между клиентскими приложениями и посредником может использоваться протокол IPX.

Благодаря протоколу SOCKS МЭ и виртуальные частные сети могут организовать безопасное взаимодействие и обмен информацией между разными сетями. Протокол SOCKS позволяет реализовать безопасное управление этими системами на основе унифицированной стратегии. Следует отметить, что на основе протокола SOCKS могут создаваться защищенные туннели для каждого приложения и сеанса в отдельности.

Согласно спецификации протокола SOCKS различают *SOCKS-сервер*, который целесообразно устанавливать на шлюз (МЭ) сети, и *SOCKS-клиент*, который устанавливают на каждый пользовательский компьютер. SOCKS-сервер обеспечивает взаимодействие с любым прикладным сервером от имени соответствующего этому серверу прикладного клиента. SOCKS-клиент предназначен для перехвата всех запросов к прикладному серверу со стороны клиента и передачи их SOCKS-серверу. Следует

отметить, что SOCKS-клиенты, выполняющие перехват запросов клиентских приложений и взаимодействие с SOCKS-сервером, могут быть встроены в универсальные клиентские программы. SOCKS-серверу известно о трафике на уровне сеанса (сокета), поэтому он может осуществлять тщательный контроль и, в частности, блокировать работу конкретных приложений пользователей, если они не имеют необходимых полномочий на информационный обмен.

Протокол SOCKS v5 одобрен организацией IETF (Internet Engineering Task Force) в качестве стандарта Internet и включен в RFC 1928 [9].

Общая схема установления соединения по протоколу SOCKS v5 может быть описана следующим образом:

- запрос прикладного клиента, желающего установить соединение с каким-либо прикладным сервером в сети, перехватывает установленный на этом же компьютере SOCKS-клиент;
- соединившись с SOCKS-сервером, SOCKS-клиент сообщает ему идентификаторы всех методов аутентификации, которые он поддерживает;
- SOCKS-сервер решает, каким методом аутентификации воспользоваться (если SOCKS-сервер не поддерживает ни один из методов аутентификации, предложенных SOCKS-клиентом, соединение разрывается);
- при поддержке каких-либо предложенных методов аутентификации SOCKS-сервер в соответствии с выбранным методом аутентифицирует пользователя, от имени которого выступает SOCKS-клиент; в случае безуспешной аутентификации SOCKS-сервер разрывает соединение;
- после успешной аутентификации SOCKS-клиент передает SOCKS-серверу DNS-имя или IP-адрес запрашиваемого прикладного сервера в сети и далее SOCKS-сервер на основе имеющихся правил разграничения доступа принимает решение об установлении соединения с этим прикладным сервером;
- в случае установления соединения прикладной клиент и прикладной сервер взаимодействуют друг с другом по цепочке соединений, в которой SOCKS-сервер ретранслирует данные, а также может выполнять функции посредничества по защите сетевого взаимодействия; например, если в ходе аутентификации SOCKS-клиент и SOCKS-сервер об-

менялись сеансовым ключом, то весь трафик между ними может шифроваться.

Аутентификация пользователя, выполняемая SOCKS-сервером, может основываться на цифровых сертификатах в формате X.509 или паролях. Для шифрования трафика между SOCKS-клиентом и SOCKS-сервером могут быть использованы протоколы, ориентированные на сеансовый или более низкие уровни модели OSI. Кроме аутентификации пользователей, трансляции IP-адресов и криптозащиты трафика, SOCKS-сервер может выполнять также такие функции, как:

- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- фильтрация потока сообщений, например, динамический поиск вирусов;
- регистрация событий и реагирование на задаваемые события;
- кэширование данных, запрашиваемых из внешней сети.

Протокол SOCKS осуществляет встроенную поддержку популярных Web-навигаторов Netscape Navigator и Netscape Communicator компании Netscape, а также Internet Explorer компании Microsoft.

Специальные программы, называемые *соксификаторами*, дополняют клиентские приложения поддержкой протокола SOCKS. К таким программам относится, например, NEC SocksCap и др. При установке соксификатор внедряется между пользовательскими приложениями и стеком коммуникационных протоколов. Далее в процессе работы он перехватывает коммуникационные вызовы, формируемые приложениями, и перенаправляет их в случае надобности на SOCKS-сервер. При отсутствии нарушений установленных правил безопасности работа SOCKS-клиента совершенно прозрачна для клиентских приложений и пользователей.

Таким образом, для формирования защищенных виртуальных сетей по протоколу SOCKS в точке сопряжения каждой локальной сети с Интернетом на компьютере-шлюзе устанавливается SOCKS-сервер, а на рабочих станциях в локальных сетях и на компьютерах удаленных пользователей устанавливаются SOCKS-клиенты. По существу, SOCKS-сервер можно рассматривать как МЭ, поддерживающий протокол SOCKS (рис. 11.7).

Удаленные пользователи могут подключаться к Интернету любым способом — по коммутируемой или выделенной линии. При попытке пользователя защищенной виртуальной сети установить

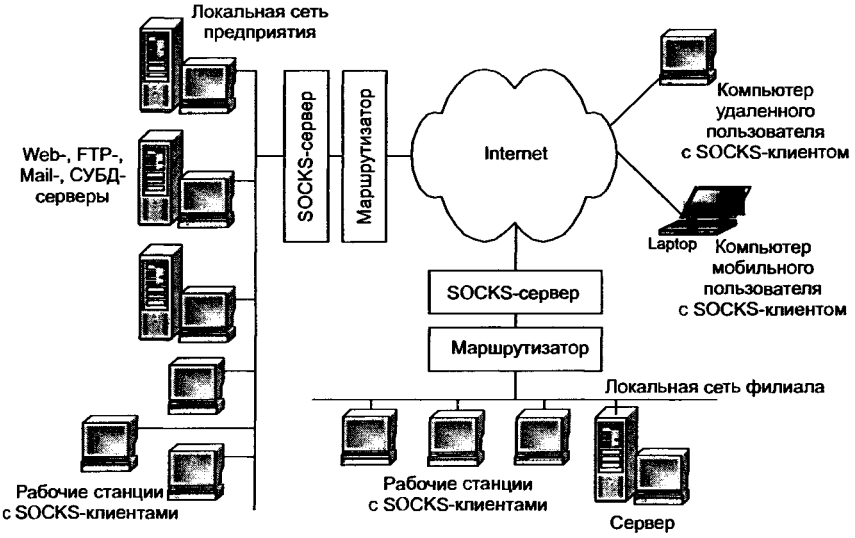


Рис. 11.7. Схема взаимодействия по протоколу SOCKS

соединение с каким-либо прикладным сервером SOCKS-клиент начинает взаимодействовать с SOCKS-сервером. По завершении первого этапа взаимодействия пользователь будет аутентифицирован, а проверка правил доступа покажет, имеет ли он право соединиться с конкретным серверным приложением, функционирующем на компьютере с указанным адресом. Дальнейшее взаимодействие может происходить по криптографически защищенному каналу [45].

Помимо защиты локальной сети от НСД, на SOCKS-сервер может возлагаться контроль доступа пользователей этой локальной сети к открытым ресурсам Интернета (Telnet, WWW, SMTP, POP и др.). Доступ является полностью авторизованным, так как идентифицируются и аутентифицируются конкретные пользователи, а не компьютеры, с которых они входят в сеть. Правила доступа могут запрещать или разрешать соединения с конкретными ресурсами Интернета в зависимости от полномочий конкретного сотрудника. Действие правил доступа может зависеть и от других параметров, например от метода аутентификации или времени суток.

В дополнение к функциям разграничения доступа может выполняться регистрация событий и реагирование на задаваемые события. Для достижения более высокой степени безопасности

сетевого взаимодействия серверы локальной сети, к которым разрешен доступ со стороны Интернета, должны быть выделены в отдельный подсоединяемый к SOCKS-серверу сегмент, образующий защищаемую открытую подсеть.

11.3. Защита беспроводных сетей

Беспроводные сети начинают использоваться практически во всем мире. Это обусловлено их удобством, гибкостью и сравнительно невысокой стоимостью. Беспроводные технологии должны удовлетворять ряду требований к качеству, скорости, радиусу приема и защищенности, причем защищенность часто является самым важным фактором.

Сложность обеспечения безопасности беспроводной сети очевидна. Если в проводных сетях злоумышленник должен сначала получить физический доступ к кабельной системе или оконечным устройствам, то в беспроводных сетях это условие отпадает само собой: поскольку данные передаются «по воздуху», для получения доступа достаточно обычного приемника, установленного в радиусе действия сети (см. разд. 2.2.3).

Однако, несмотря на различия в реализации, подход к безопасности беспроводных сетей и их проводных аналогов идентичен: здесь присутствуют аналогичные требования к обеспечению конфиденциальности и целостности передаваемых данных и, конечно же, к проверке подлинности как беспроводных клиентов, так и точек доступа.

Общие сведения

Как и все стандарты IEEE 802, базовый стандарт организации беспроводных локальных сетей IEEE 802.11 работает на нижних двух уровнях модели ISO/OSI — физическом и канальном. Сетевое приложение, сетевая ОС или протокол (например, TCP/IP) будут так же хорошо работать в сети 802.11, как и в сети Ethernet.

Основная архитектура, особенности и службы определяются в базовом стандарте 802.11 (см. разд. 4.2), который определяет два режима работы беспроводной сети — режим клиент/сервер (или режим инфраструктуры) и режим «точка—точка» (Ad-hoc).

В режиме клиент/сервер беспроводная сеть состоит как минимум из одной точки доступа AP (Access point), подключенной к проводной сети, и некоторого набора беспроводных оконечных станций. Такая конфигурация носит название *базового набора служб BSS* (Basic Service Set). Два или более BSS, образующих единую подсеть, формируют *расширенный набор служб ESS* (Extended Service Set). Так как большинству беспроводных станций требуется получать доступ к файловым серверам, принтерам, Интернету, доступным в проводной локальной сети, они будут работать в режиме клиент/сервер.

Режим «точка—точка» — это простая сеть, в которой связь между многочисленными станциями устанавливается напрямую, без использования специальной точки доступа. Такой режим полезен в том случае, если инфраструктура беспроводной сети не сформирована (например, в отеле, выставочном зале, аэропорту).

На физическом уровне стандарта 802.11 определены 2 широкополосных радиочастотных метода передачи и 1 — в инфракрасном диапазоне. Радиочастотные методы работают в ISM диапазоне 2,4 ГГц и обычно используют полосу 83 МГц от 2,400 ГГц до 2,483 ГГц. Технологии широкополосного сигнала, используемые в радиочастотных методах, увеличивают надежность, пропускную способность, позволяют многим несвязанным друг с другом устройствам разделять одну полосу частот с минимальными помехами друг для друга.

Основное дополнение, внесенное стандартом 802.11b в основной стандарт, — это поддержка двух новых скоростей передачи данных — 5,5 и 11 Mbps. Для достижения этих скоростей был выбран метод прямой последовательности DSSS (Direct Sequence Spread Spectrum).

Канальный (Data Link) уровень стандарта 802.11 состоит из двух подуровней: управления логической связью LLC (Logical Link Control) и управления доступом к носителю MAC (Media Access Control).

Обеспечение безопасности беспроводных сетей

Система защиты беспроводных сетей WLAN, основанная на протоколе WEP (Wired Equivalent Privacy) первоначального стандарта 802.11, имеет существенные недостатки. Однако появились более эффективные технологии обеспечения информационной безопасности WLAN, которые описаны в стандарте WPA (Wi-Fi

Protected Access) организации Wi-Fi Alliance и стандарте 802.11i института IEEE и призваны устранить недостатки стандарта 802.11. Поскольку процесс разработки стандарта 802.11i слишком затянулся, организация Wi-Fi Alliance была вынуждена предложить в 2002 г. собственную технологию обеспечения информационной безопасности WLAN — стандарт WPA.

Стандарт WPA весьма привлекателен тем, что относительно прост в реализации и позволяет защитить ныне действующие WLAN. Стандарты WPA и 802.11i совместимы друг с другом, поэтому использование поддерживающих WPA продуктов можно считать начальным этапом перехода к системе защиты на базе стандарта 802.11i (см. разд. 4.2).

Между технологиями стандартов 802.11i и WPA много общего. Так, в них определена идентичная архитектура системы безопасности с улучшенными механизмами аутентификации пользователей и протоколами распространения и обновления ключей. Но есть и существенные различия. Например, технология WPA базируется на протоколе динамических ключей TKIP (Temporal Key Integrity Protocol), поддержку которого в большинстве устройств WLAN можно реализовать путем обновления их ПО, а в более функциональной концепции стандарта 802.11i предусмотрено использование нового стандарта шифрования AES (Advanced Encryption Standard), с которым совместимо лишь новейшее оборудование для WLAN.

В стандарте WPA предусмотрено использование защитных протоколов 802.1x, EAP, TKIP и RADIUS.

Механизм аутентификации пользователей основан на протоколе контроля доступа 802.1x (разработан для проводных сетей) и протоколе расширенной аутентификации EAP (Extensible Authentication Protocol). Последний позволяет сетевому администратору задействовать алгоритмы аутентификации пользователей посредством сервера RADIUS (см. гл. 13).

Функции обеспечения конфиденциальности и целостности данных базируются на протоколе TKIP, который в отличие от протокола WEP использует более эффективный механизм управления ключами, но тот же самый алгоритм RC4 для шифрования данных. Согласно протоколу TKIP, сетевые устройства работают с 48-битовым вектором инициализации (в отличие от 24-битового вектора инициализации протокола WEP) и реализуют правила изменения последовательности его битов, что исключает повторное использование ключей и осуществление replay-атак.

В протоколе TKIP предусмотрены генерация нового ключа для каждого передаваемого пакета и улучшенный контроль целостности сообщений с помощью криптографической контрольной суммы MIC (Message Integrity Code), препятствующей хакеру изменять содержимое передаваемых пакетов.

Система сетевой безопасности стандарта WPA работает в двух режимах: PSK (Pre-Shared Key) и Enterprise (корпоративный). Для развертывания системы, работающей в режиме PSK, необходим разделяемый пароль. Такую систему несложно устанавливать, но она защищает WLAN не столь надежно, как это делает система, функционирующая в режиме Enterprise с иерархией динамических ключей. Хотя протокол TKIP работает с тем же самым блочным шифром RC4, который предусмотрен спецификацией протокола WEP, технология WPA защищает данные надежнее последнего.

Чтобы точки доступа WLAN стали совместимыми со стандартом WPA, достаточно модернизировать их ПО. Для перевода же сетевой инфраструктуры на стандарт 802.11i потребуется новое оборудование, поддерживающее алгоритм шифрования AES, так как AES-шифрование создает большую нагрузку на центральный процессор беспроводного клиентского устройства.

Чтобы корпоративные точки доступа работали в системе сетевой безопасности стандарта WPA или 802.11i, они должны поддерживать аутентификацию пользователей по протоколу RADIUS и реализовывать предусмотренный стандартом метод шифрования — TKIP или AES, что потребует модернизации их ПО. И еще одно требование — быстро осуществлять повторную аутентификацию пользователей после разрыва соединения с сетью. Это особенно важно для нормального функционирования приложений, работающих в реальном масштабе времени.

Если сервер RADIUS, применяемый для контроля доступа пользователей проводной сети, поддерживает нужные методы аутентификации EAP, то его можно задействовать и для аутентификации пользователей WLAN. В противном случае следует установить сервер WLAN RADIUS. Этот сервер работает следующим образом: сначала он проверяет аутентифицирующую информацию пользователя (на соответствие содержимому своей БД об их идентификаторах и паролях) или его цифровой сертификат, а затем активизирует динамическую генерацию ключей шифрования точкой доступа и клиентской системой для каждого сеанса связи.

Для работы технологии WPA требуется механизм EAP-TLS (Transport Layer Security), тогда как в стандарте IEEE 802.11i применение конкретных методов аутентификации EAP не оговаривается. Выбор метода аутентификации EAP определяется спецификой работы клиентских приложений и архитектурой сети. Чтобы ноутбуки и карманные ПК работали в системе сетевой безопасности стандарта WPA или 802.11i, они должны быть оснащены клиентскими программами, поддерживающими стандарт 802.1x.

Самым простым, с точки зрения развертывания, вариантом системы сетевой безопасности стандарта WPA является система, работающая в режиме PSK. Она предназначена для небольших и домашних офисов и не нуждается в сервере RADIUS, а для шифрования пакетов и расчета криптографической контрольной суммы MIC в ней используется пароль PSK. Обеспечиваемый ею уровень информационной безопасности сети вполне достаточен для большинства вышеуказанных офисов. С целью повышения эффективности защиты данных следует применять пароли, содержащие не менее 20 символов.

Предприятиям целесообразно внедрять у себя системы сетевой безопасности стандарта WPA с серверами RADIUS. Большинство компаний предпочитают именно такие системы, поскольку работающие в режиме PSK решения сложнее администрировать и они более уязвимы для хакерских атак.

До тех пор пока средства стандарта 802.11i не станут доступными на рынке, WPA будет оставаться самым подходящим стандартом для защиты WLAN.

Стандарты WPA и 802.11i в достаточной степени надежны и обеспечивают высокий уровень защищенности беспроводных сетей. Тем не менее одного протокола защиты недостаточно — следует также уделять внимание правильному построению и настройке сети.

Физическая защита. При развертывании Wi-Fi-сети необходимо физически ограничить доступ к беспроводным точкам.

Правильная настройка. Парадокс современных беспроводных сетей заключается в том, что пользователи не всегда включают и используют встроенные механизмы аутентификации и шифрования.

Защита пользовательских устройств. Не следует полностью полагаться на встроенные механизмы защиты сети. Наиболее оптимальным является метод эшелонированной обороны, пер-

вая линия которой — средства защиты, установленные на стационарном ПК, ноутбуке или КПК.

Традиционные меры. Эффективная работа компьютера в сети немыслима без классических мер защиты — своевременной установки обновлений, использования защитных механизмов, встроенных в ОС и приложения, а также антивирусов. Однако этих мер на сегодня недостаточно, так как они ориентированы на защиту от уже известных угроз.

Мониторинг сети. Слабое звено в корпоративной сети — самовольно установленные точки доступа. Актуальной является задача локализации несанкционированных точек доступа. Специальные средства локализации точек доступа позволяют графически отображать место расположения «чужого» терминала на карте этажа или здания. Если классические методы не спасают от вторжения, следует применять системы обнаружения атак.

VPN-агенты. Многие точки доступа работают в открытом режиме, поэтому необходимо использовать методы защиты передаваемых данных. На защищаемом компьютере должен быть установлен VPN-клиент, который возьмет на себя решение этой задачи. Практически все современные ОС (например, Windows XP) содержат в своем составе такие программные компоненты.

Глава 12
ЗАЩИТА НА СЕТЕВОМ УРОВНЕ — ПРОТОКОЛ IPSEC

Радикальное устранение уязвимостей компьютерных сетей возможно при создании системы защиты не для отдельных классов приложений, а для сети в целом. Применительно к IP-сетям это означает, что системы защиты должны действовать на сетевом уровне модели OSI. Преимущество такого выбора заключается в том очевидном факте, что в IP-сетях именно сетевой уровень отличается наибольшей гомогенностью: независимо от вышележащих протоколов, физической среды передачи и технологии канального уровня транспортировка данных по сети не может быть произведена в обход протокола IP. Поэтому реализация защиты сети на третьем уровне автоматически гарантирует как минимум такую же степень защиты всех сетевых приложений, причем без какой-либо модификации последних.

При формировании защищенных виртуальных каналов на сетевом уровне модели OSI достигается оптимальное соотношение между прозрачностью и качеством защиты. Размещение средств защиты на сетевом уровне делает их прозрачными для приложений, так как между сетевым уровнем и приложением функционирует реализация протокола транспортного уровня. Для пользователей процедуры защиты оказываются столь же прозрачными, как и сам протокол IP. На сетевом уровне существует возможность достаточно полной реализации функций защиты трафика и управления ключами, поскольку именно на сетевом уровне выполняется маршрутизация пакетов сообщений.

Стек протоколов IPSec используется для аутентификации участников обмена, туннелирования трафика и шифрования IP-пакетов. Основное назначение протокола IPSec (*Internet Protocol Security*) — обеспечение безопасной передачи данных по се-

тям IP. Поскольку архитектура IPSec совместима с протоколом IPv4, ее поддержку достаточно обеспечить на обоих концах соединения; промежуточные сетевые узлы могут вообще ничего «не знать» об IPSec. Протокол IPSec может защищать трафик как текущей версии протокола IPv4, применяемой сегодня в Internet, так и трафик новой версии IPv6, которая постепенно внедряется в Internet.

12.1. Архитектура средств безопасности IPSec

Основное назначение протоколов IPSec — обеспечение безопасной передачи данных по сетям IP. Применение IPSec гарантирует:

- целостность передаваемых данных (т. е. данные при передаче не искажены, не потеряны и не продублированы);
- аутентичность отправителя (т. е. данные переданы именно тем отправителем, который доказал, что он тот, за кого себя выдает);
- конфиденциальность передаваемых данных (т. е. данные передаются в форме, предотвращающей их несанкционированный просмотр).

Следует отметить, что обычно в понятие безопасности данных включают еще одно требование — доступность данных, что в рассматриваемом контексте можно интерпретировать как гарантию их доставки. Протоколы IPSec не решают данную задачу, оставляя ее протоколу транспортного уровня TCP. Стек протоколов IPSec обеспечивает защиту информации на сетевом уровне, что делает эту защиту невидимой для работающих приложений.

Фундаментальной единицей коммуникации в IP-сетях является IP-пакет. IP-пакет содержит S-адрес источника и D-адрес получателя сообщения, транспортный заголовок, информацию о типе данных, переносимых в этом пакете, и сами данные (рис. 12.1).

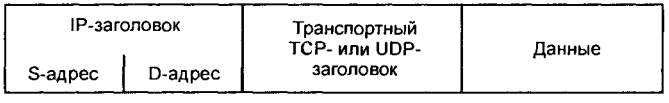


Рис. 12.1. Структура IP-пакета

Пользователь воспринимает сеть как надежно защищенную среду только в том случае, если он уверен, что его партнер по обмену — именно тот, за кого он себя выдает (аутентификация сторон), что передаваемые пакеты не просматриваются посторонними лицами (конфиденциальность связи) и что получаемые данные не подверглись изменению в процессе передачи (целостность данных).

Для того чтобы обеспечить аутентификацию, конфиденциальность и целостность передаваемых данных стек протоколов IPSec построен на базе стандартизованных криптографических технологий:

- обмена ключами согласно алгоритму Диффи — Хеллмана для распределения секретных ключей между пользователями в открытой сети;
- криптографии открытых ключей для подписывания обменов Диффи — Хеллмана, чтобы гарантировать подлинность двух сторон и избежать атак типа «man-in-the-middle»;
- цифровых сертификатов для подтверждения подлинности открытых ключей;
- блочных симметричных алгоритмов шифрования данных;
- алгоритмов аутентификации сообщений на базе функций хэширования.

Протокол IPSec определяет стандартные способы защиты информационного обмена на сетевом уровне модели OSI для IP-сети, являющейся основным видом окрытых сетей. Данный протокол входит в состав новой версии протокола IP (IPv6) и применим также к его текущей версии (IPv4). Для протокола IPv4 поддержка IPSec является желательной, а для IPv6 — обязательной. Протокол IPSec представляет собой систему открытых стандартов, которая имеет четко очерченное ядро, и в то же время позволяет дополнять ее новыми протоколами, алгоритмами и функциями. Стандартизованными функциями IPSec-защиты могут пользоваться протоколы более высоких уровней, в частности, управляющие протоколы, протоколы конфигурирования, а также протоколы маршрутизации.

Основными задачами установления и поддержания защищенного канала являются следующие:

- аутентификация пользователей или компьютеров при инициации защищенного канала;
- шифрование и аутентификация передаваемых данных между конечными точками защищенного канала;

- обеспечение конечных точек канала секретными ключами, необходимыми для работы протоколов аутентификации и шифрования данных.

Для решения перечисленных задач система IPSec использует комплекс средств безопасности информационного обмена.

Большинство реализаций протокола IPSec имеют следующие компоненты.

Основной протокол IPSec. Этот компонент реализует протоколы ESP и AH. Он обрабатывает заголовки, взаимодействует с БД SPD и SAD для определения политики безопасности, применяемой к пакету.

Протокол управления обменом ключевой информации IKE (Internet Key Exchange). IKE обычно представляется как процесс пользовательского уровня, за исключением реализаций, встроенных в ОС.

База данных политик безопасности SPD (Security Policy Database). Это один из важнейших компонентов, поскольку он определяет политику безопасности, применяемую к пакету. SPD используется основным протоколом IPSec при обработке входящих и исходящих пакетов.

База данных безопасных ассоциаций SAD (Security Association Database). БД SAD хранит список безопасных ассоциаций SA (Security Association) для обработки входящей и исходящей информации. Исходящие SA используются для защиты исходящих пакетов, а входящие SA используются для обработки пакетов с заголовками IPSec. БД SAD заполняется SA вручную или с помощью протокола управления ключами IKE.

Управление политикой безопасности и безопасными ассоциациями SA. Это — приложения, которые управляют политикой безопасности и SA [9].

Основной протокол IPSec (реализующий ESP и AH) тесно взаимодействует с транспортным и сетевым уровнем стека протоколов TCP/IP. Фактически протокол IPSec является частью сетевого уровня. Основной модуль протокола IPSec обеспечивает два интерфейса: входной и выходной. Входной интерфейс используется входящими пакетами, а выходной — исходящими. Реализация IPSec не должна зависеть от интерфейса между транспортным и сетевым уровнем стека протоколов TCP/IP.

БД SPD и SAD существенно влияют на эффективность работы IPSec. Выбор структуры данных для хранения SPD и SAD является критическим моментом, от которого зависит производи-

тельность IPSec. Особенности реализации SPD и SAD зависят от требований производительности и совместимости системы.

Все протоколы, входящие в IPSec, можно разделить на две группы:

1) протоколы, непосредственно производящие обработку передаваемых данных (для обеспечения их защиты);

2) протоколы, позволяющие автоматически согласовать параметры защищенных соединений, необходимые для протоколов 1-й группы.

Архитектура средств безопасности IPSec представлена на рис. 12.2.

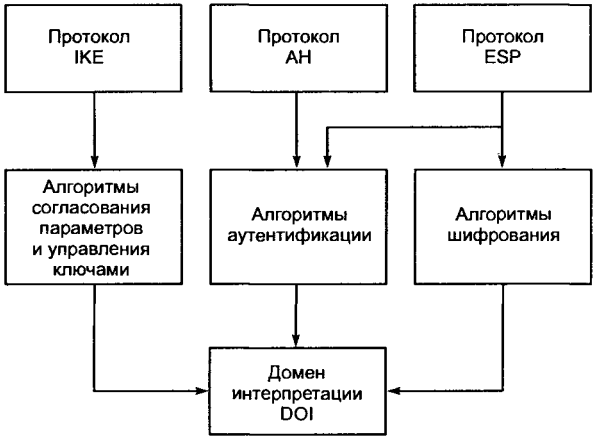


Рис. 12.2. Архитектура стека протоколов IPSec

На *верхнем уровне* расположены 3 протокола, составляющих ядро IPSec:

- протокол согласования параметров виртуального канала и управления ключами IKE (Internet Key Exchange), определяющий способ инициализации защищенного канала, включая согласование используемых алгоритмов криптозащиты, а также процедуры обмена и управления секретными ключами в рамках защищенного соединения;
- протокол аутентифицирующего заголовка AH (Authentication header), обеспечивающий аутентификацию источника данных, проверку их целостности и подлинности после приема, а также защиту от навязывания повторных сообщений;

- протокол инкапсулирующей защиты содержимого ESP (Encapsulating Security Payload), обеспечивающий криптографическое закрытие, аутентификацию и целостность передаваемых данных, а также защиту от навязывания повторных сообщений.

Разделение функций защиты между двумя протоколами AH и ESP обусловлено применяемой во многих странах практикой ограничения экспорта и/или импорта средств, обеспечивающих конфиденциальность данных путем шифрования. Каждый из протоколов AH и ESP может использоваться как самостоятельно, так и совместно с другим. Из краткого перечисления функций протоколов AH и ESP видно, что возможности этих протоколов частично перекрываются.

Протокол AH отвечает только за обеспечение целостности и аутентификации данных, в то время как протокол ESP является более мощным, поскольку может шифровать данные, а кроме того, выполнять функции протокола AH (хотя, как увидим позднее, аутентификация и целостность обеспечиваются им в несколько урезанном виде).

Протокол ESP может поддерживать функции шифрования и аутентификации/целостности в любых комбинациях, т. е. либо и ту и другую группу функций, либо только аутентификацию/целостность, либо только шифрование.

Средний уровень архитектуры IPSec образуют алгоритмы согласования параметров и управления ключами, применяемые в протоколе IKE, а также алгоритмы аутентификации и шифрования, используемые в протоколах аутентифицирующего заголовка AH и инкапсулирующей защиты содержимого ESP.

Следует отметить, что протоколы защиты виртуального канала верхнего уровня архитектуры IPSec (AH и ESP) не зависят от конкретных криптографических алгоритмов. За счет возможности использования большого числа разнообразных алгоритмов аутентификации и шифрования IPSec обеспечивает высокую степень гибкости организации защиты сети. Гибкость IPSec состоит в том, что для каждой задачи предлагается несколько способов ее решения. Выбранные методы для одной задачи обычно не зависят от методов реализации других задач. Например, выбор для шифрования алгоритма AES не влияет на выбор функции вычисления дайджеста, используемого для аутентификации данных.

Нижний уровень архитектуры IPSec образует так называемый домен интерпретации DOI (Domain of Interpretation). Необходи-

мость применения домена интерпретации DOI обусловлена следующими причинами. Протоколы AH и ESP имеют модульную структуру, допуская применение пользователями по их согласованному выбору различных криптографических алгоритмов шифрования и аутентификации. Поэтому необходим модуль, который мог бы обеспечить совместную работу всех применяемых и вновь включаемых протоколов и алгоритмов. Именно такие функции возложены на домен интерпретации DOI. Домен интерпретации DOI в качестве БД хранит сведения об используемых в IPSec протоколах и алгоритмах, их параметрах, протокольных идентификаторах и т. п. По существу, он выполняет роль фундамента в архитектуре IPSec. Для того чтобы использовать алгоритмы, соответствующие национальным стандартам в качестве алгоритмов аутентификации и шифрования в протоколах AH и ESP, необходимо зарегистрировать эти алгоритмы в домене интерпретации DOI [9].

12.2. Защита передаваемых данных с помощью протоколов AH и ESP

Протокол аутентифицирующего заголовка AH и протокол инкапсулирующей защиты содержимого ESP могут работать в туннельном или транспортном режимах. Для выполнения своих задач по обеспечению безопасной передачи данных протоколы AH и ESP включают в обрабатываемые ими пакеты дополнительную служебную информацию, оформляя ее в виде заголовков.

12.2.1. Протокол аутентифицирующего заголовка AH

Протокол аутентифицирующего заголовка AH (Authentication Header) обеспечивает проверку аутентичности и целостности IP-пакетов, а также защиту от воспроизведения ранее посланных IP-пакетов.

Протокол AH позволяет приемной стороне убедиться, что:

- пакет был отправлен именно той стороной, с которой установлена данная ассоциация;
- содержимое пакета не подверглось искажениям в процессе передачи его по сети;

- пакет не является дубликатом некоторого пакета, полученного ранее.

Протокол AH полностью защищает от подлога и искажения содержимое IP-пакетов, включая данные протоколов более высоких уровней. Полнота защиты полей IP-заголовков зависит от используемого режима работы — туннельного или транспортного. Однако протокол AH не обеспечивает конфиденциальность передаваемых данных, т. е. не предназначен для их шифрования. Данные могут быть прочитаны промежуточными узлами, но не могут быть изменены. Целостность и аутентичность данных обеспечиваются добавлением аутентифицирующего заголовка (AH) перед заголовком IP и заголовком транспортного уровня (TCP/UDP). Формат заголовка AH показан на рис. 12.3.

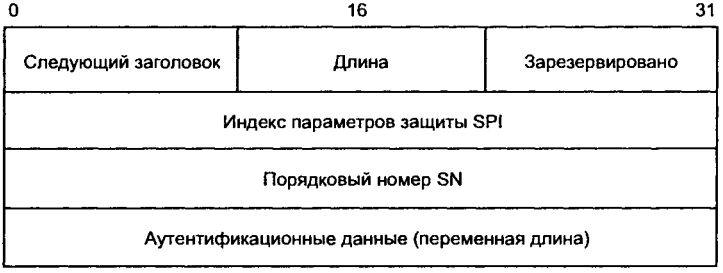


Рис. 12.3. Формат заголовка AH

Заголовок AH включает в себя поля:

- *следующий заголовок* (*Next Header*) — однобайтовое поле, содержащее код протокола следующего заголовка, вложенного в IPSec-пакет, например код протокола TCP или ESP, чей заголовок следует за AH;
- *длина* (*Payload Len*) — указывает длину заголовка AH в 32-битных словах;
- *индекс параметров защиты SPI* (*Security Parameters Index*) — представляет собой 32-разрядную метку безопасной ассоциации SA (Security Association), содержащей все параметры туннеля IPSec, включая типы криптографических алгоритмов и ключи шифрования. На основании индекса SPI пакет будет правильно отнесен к одной из существующих ассоциаций в приемном шлюзе (или хосте). Если же активной ассоциации, на которую указывает метка SPI, не существует, то пакет просто отбрасывается;

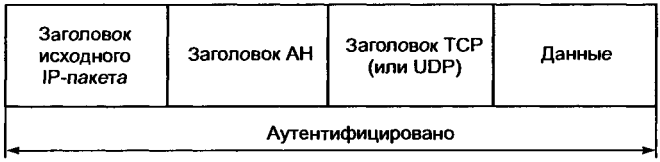
- *порядковый номер SN* (*Sequence Number*) — беззнаковое 32-битное число, увеличиваемое на единицу после передачи каждого защищенного по протоколу AH IP-пакета. Обеспечивает защиту от ложного воспроизведения ранее посланных IP-пакетов. При формировании каждого защищенного сеанса информационного обмена в рамках туннеля IPSec взаимодействующие стороны делают свои счетчики нулевыми, а потом согласованным образом увеличивают их. Получатель проверяет это поле с целью удостовериться, что пакета с таким номером принято еще не было. Если же такой пакет уже был, он не принимается;
- *аутентификационные данные* (*Authentication Data*) — поле переменной длины, содержащее информацию, используемую для аутентификации пакета и называемую *MAC-кодом* (Message Authentication Code). Это поле называют также *цифровой подписью*, *дайджестом* или *кодом проверки целостности* — *ICV* (Integrity Check Value) пакета. Содержимое поля Authentication Data вычисляется с помощью одного из двух обязательно поддерживаемых протоколом AH алгоритмов HMAC-MD5 и HMAC-SHA1, основанных на применении односторонних хэш-функций с секретными ключами. Длина дайджеста зависит от выбранного алгоритма, поэтому это поле имеет в общем случае переменный размер. Наиболее часто используемый алгоритм HMAC-MD5 порождает 16-байтный дайджест.

Протокол AH защищает весь IP-пакет за исключением некоторых полей в IP-заголовке, таких как *время жизни* (TTL) и *тип службы* (Type of Service), которые могут меняться в процессе передачи пакета в сети. Заметим, что протокол AH обеспечивает защиту от изменений IP-адресов в заголовке пакета. Протокол аутентификации AH создает своеобразный конверт, обеспечивающий аутентификацию источника данных, их целостность и защиту от навязывания повторных сообщений.

Местоположение заголовка AH в пакете зависит от того, в каком режиме — транспортном или туннельном — сконфигурирован защищенный канал. На рис. 12.4 показано расположение AH-заголовка относительно IP-заголовка в обоих режимах.

В *транспортном режиме* заголовок исходного IP-пакета становится внешним заголовком, за ним следует заголовок AH, а затем все данные защищаемого пакета (т. е. пакет протокола верхнего уровня). Протокол AH защищает весь полученный та-

IP-пакет после применения протокола AH в транспортном режиме



IP-пакет после применения протокола AH в туннельном режиме

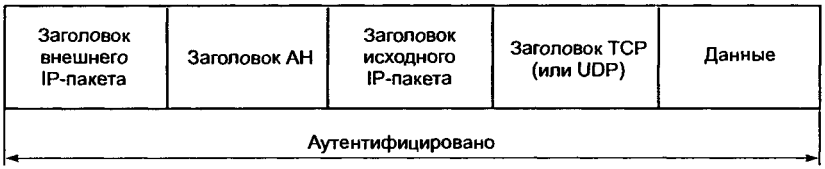


Рис. 12.4. IP-пакет после применения протокола AH в транспортном и туннельном режимах

ким образом пакет, включая заголовок IP и собственно сам заголовок AH. Таким образом, любое изменение данных в пакете или заголовков будет обнаружено. Следует также заметить, что в этом режиме данные пакета отсылаются открытыми, т. е. данные пакета защищены от изменений, но не защищены от просмотра. В частности, не удается скрыть IP-адреса источника и назначения от возможного просмотра посторонними лицами, поскольку эти поля всегда присутствуют в незашифрованном виде и соответствуют действительным адресам хостов.

В *туннельном режиме* в качестве заголовка внешнего IP-пакета создается новый заголовок IP. IP-адреса посылающей и принимающей сторон могут отличаться от адресов в заголовке исходного IP-пакета. В защищенном IP-пакете внутренний (первоначальный) IP-заголовок содержит целевой адрес пакета, а внешний IP-заголовок содержит адрес конца туннеля. За новым заголовком внешнего IP-пакета следует заголовок AH, а затем весь исходный пакет (заголовок IP и сами данные). Как и в случае транспортного режима, протокол AH защищает весь созданный пакет (два заголовка IP, заголовок AH и данные), что также позволяет обнаружить любые изменения в пакете. Как и в транспортном режиме, сам пакет не защищен от просмотра.

Независимо от режима работы, протокол AH предоставляет меры защиты от атак, направленных на нарушение целостности и подлинности пакетов сообщений. С помощью этого протокола

аутентифицируется каждый пакет, что делает программы, пытающиеся перехватить управление сеансом, неэффективными. Протокол AH обеспечивает аутентификацию не только содержимого, но и заголовков IP-пакетов. Однако следует иметь в виду, что аутентификация по протоколу AH не допускает манипулирования основными полями IP-заголовка во время прохождения пакета. По этой причине данный протокол нельзя применять в среде, где используется механизм трансляции сетевых адресов NAT (Network Address Translation), поскольку для его работы необходимо манипулирование IP-заголовками.

Протокол AH может применяться как отдельно, так и в комбинации с протоколом ESP или даже с пакетом, который уже содержит AH-заголовок (вложенное применение).

12.2.2. Протокол инкапсулирующей защиты ESP

Протокол инкапсулирующей защиты содержимого ESP (Encapsulating Security Payload) обеспечивает конфиденциальность, аутентичность, целостность и защиту от повторов для пакетов данных. Следует отметить, что конфиденциальность данных протокол ESP обеспечивает всегда, а целостность и аутентичность являются для него опциональными требованиями. Конфиденциальность данных обеспечивается путем шифрования содержимого отдельных пакетов. Целостность и аутентичность данных обеспечиваются на основе вычисления дайджеста.

Из приведенного перечня функций по защите информационного обмена видно, что функциональность протокола ESP шире, чем у протокола AH. Протокол ESP поддерживает все функции протокола AH по защите зашифрованных потоков данных от подлога, воспроизведения и случайного искажения, а также обеспечивает конфиденциальность данных.

В протоколе ESP функции аутентификации и криптографического закрытия могут быть задействованы либо вместе, либо отдельно друг от друга. При выполнении шифрования без аутентификации появляется возможность использования механизма трансляции сетевых адресов NAT (Network Address Translation), поскольку в этом случае адреса в заголовках IP-пакетов можно модифицировать [9].

Для решения своих задач протокол ESP использует заголовок формата, приведенного на рис. 12.5.

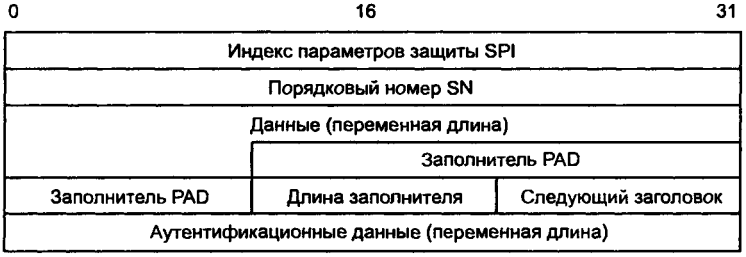


Рис. 12.5. Формат заголовка ESP

Заголовок ESP содержит следующие поля:

- *индекс параметров защиты SPI* (*Security Parameters Index*) — используется совместно с адресом получателя и протоколом защиты (AH или ESP). Указывает соответствующее соглашение SA. Получатель использует это значение для определения соглашения о защите, с которым идентифицируется этот пакет;
- *порядковый номер SN* (*Sequence Number*)— обеспечивает защиту от повторов для SA. Представляет собой 32-битное число, первоначально равное 1 и увеличивающееся с шагом 1. Оно не повторяется циклически и указывает номер пакета, отсылаемого по данному соглашению. Получатель проверяет это поле с целью удостовериться, что пакета с таким номером принято еще не было. Если же такой пакет уже был, он не принимается;
- *данные* (*Payload Data*);
- *заполнитель* (*Padding*) — дописывается от 0 до 255 байт для 32-битного выравнивания с размером блока шифра;
- *длина заполнителя* (*Padding Length*) — указывает длину поля заполнителя в байтах;
- *следующий заголовок* (*Next Header*) — указывает природу передаваемых данных (например, TCP или UDP);
- *аутентификационные данные* (*Authentication Data*) — содержат *код проверки целостности ICV* (Integrity Check Value) и *код аутентичности сообщения*, используемые для проверки подлинности отправителя и целостности сообщения. Значение ICV вычисляется для заголовка ESP, передаваемых данных и концевой метки ESP. Поле Authentication Data помещается в заголовок ESP только при включенной аутентификации.

Нетрудно заметить, что некоторые поля заголовка ESP аналогичны полям заголовка AH: Next Header, SPI, SN, Authentication Data. Но есть и два дополнительных поля — *заполнитель* (Padding) и *длина заполнителя* (Pad Length). Заполнитель может понадобиться в трех случаях. Во-первых, для нормальной работы некоторых алгоритмов шифрования необходимо, чтобы шифруемый текст содержал кратное число блоков определенного размера. Во-вторых, формат заголовка ESP требует, чтобы поле данных заканчивалось на границе четырех байтов. В-третьих, заполнитель можно использовать для сокрытия действительного размера пакета в целях обеспечения так называемой частичной конфиденциальности трафика, хотя протокол ESP ограничивает возможности маскировки 255 байтами заполнителя; это сделано для того, чтобы не слишком снижалась полезная пропускная способность канала связи из-за большого объема избыточных данных.

Как видно из рис. 12.5, заголовок делится на две части, разделяемые *полем данных* (полезная нагрузка — Payload Data). Первая часть, которая далее будет обозначаться как *заголовок ESP*, образуется двумя полями — SPI и SN — и размещается перед полем данных. Остальные служебные поля протокола ESP расположены в конце пакета. Непосредственно за полем данных следует так называемый *трейлер*, в который входят *заполнитель* (Padding), *длина заполнителя* (Pad Length), а также указатель на протокол *следующего уровня* (Next Header). Завершает пакет *поле контроля целостности* (Authentication Data). В том случае, когда при установлении безопасной ассоциации принято решение не использовать возможности ESP по обеспечению целостности, это поле отсутствует.

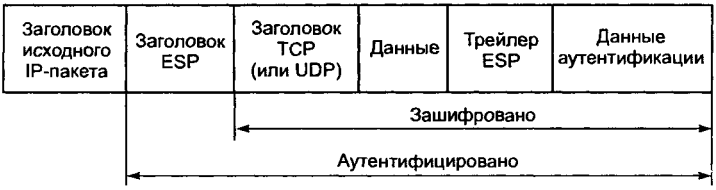
ПО перечисленных протоколов (утилиты шифрования, цифровой подписи и пр.) может функционировать на серверах или компьютерах конечных пользователей. Однако чаще его устанавливают на маршрутизаторах или специальных устройствах, которые в архитектуре IPSec именуются *шлюзами безопасности* (security gateway).

Протокол ESP также используют в двух режимах — транспортном и туннельном. На рис. 12.6 показано расположение ESP заголовка в туннельном и транспортном режимах [62].

В транспортном режиме зашифрованные данные транспортируются непосредственно между хостами. В транспортном режиме протокола ESP заголовок исходного IP-пакета остается внешним. Заголовок ESP помещается в передаваемый пакет ме-

жду заголовками протоколов третьего (IP) и четвертого (например, TCP) уровней. Следует заметить, что поля протокола ESP следуют после стандартного IP-заголовка, а это означает, что такой пакет может маршрутизироваться в сети с помощью обычного оборудования, поддерживающего IP.

IP-пакет после применения протокола ESP в транспортном режиме



IP-пакет после применения протокола ESP в туннельном режиме

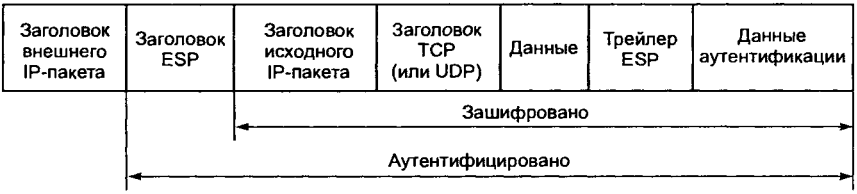


Рис. 12.6. IP-пакет после применения протокола ESP в транспортном и туннельном режимах

Шифрованию подвергаются только данные исходного IP-пакета (пакет верхнего уровня) и заключительная часть ESP заголовка (ESP trailer). В этом режиме ESP не шифрует заголовок IP-пакета, иначе маршрутизатор не сможет прочитать поля заголовка и корректно осуществить продвижение пакета между сетями. В число шифруемых полей не попали также поля SPI и SN, которые должны передаваться в открытом виде, для того чтобы прибывший пакет можно было отнести к определенной ассоциации SA и защититься от ложного воспроизведения пакета.

В отличие от протокола AH, контроль целостности и аутентичности данных в протоколе ESP не распространяется на заголовок исходного пакета, и по этой причине имеет смысл применять оба протокола совместно — ESP для шифрования, а AH для контроля целостности.

Таким образом, адресная информация (IP-адреса отсылающей и принимающей сторон) видна при пересылке пакета по

сети, и несанкционированное изменение этих IP-адресов не будет замечено.

В туннельном режиме основная роль отводится шлюзам безопасности, поскольку предполагается, что клиентские станции (или серверы) могут не поддерживать IPSec и отправляют в сеть обычный IP-трафик. Перед тем как достичь каналов глобальной сети, каждый исходный IP-пакет сначала попадает в шлюз, который помещает этот пакет целиком в «оболочку» IPSec, зашифровывая его содержимое вместе с исходным IP-заголовком. Чтобы обеспечить возможность маршрутизации получившегося пакета, шлюз снабжает его новым IP-заголовком и только после этого отправляет в сеть. Шлюз, находящийся на противоположном конце соединения, расшифровывает этот пакет и передает его на оконечное устройство в первоначальном виде. Описанная процедура называется *туннелированием*.

Из рис. 12.6 видно, что в туннельном режиме в качестве внешнего заголовка создается новый заголовок IP. Весь исходный IP-пакет (и данные и заголовок IP) и заключительная часть заголовка ESP (трейлер ESP) шифруются. Поэтому адресная информация исходного IP-пакета не доступна для просмотра. Заголовок внешнего IP-пакета протоколом ESP не защищается.

Туннелирование позволяет распространить действие средств защиты на сетевой уровень модели OSI и, в частности, скрыть истинные адреса источника и получателя. При этом уменьшается риск атак, основанных на детальном анализе трафика.

Сравнивая протоколы ESP и AH можно заметить, что они дублируют функциональность друг друга в области обеспечения аутентификации данных. Главным отличием протокола AH от ESP в данном вопросе является то, что протокол AH обеспечивает аутентификацию всего пакета (и IP заголовка и самих данных), в то время как протокол ESP аутентифицирует только данные из пакета (см. рис. 12.6). При шифровании в протоколе ESP используется симметричный секретный ключ, т. е. передаваемые данные зашифровываются и расшифровываются с помощью одного и того же ключа. Для протокола ESP также определен перечень обязательных алгоритмов шифрования — DES, MD5 и SHA-1.

При аутентификации данных протокол ESP использует те же алгоритмы HMAC, что и протокол AH (использующие MD5 или SHA-1 в качестве функции хеширования). Однако способы применения различаются (см. рис. 12.6).

В транспортном режиме:
- протокол ESP аутентифицирует только данные из пакета, не затрагивая IP-заголовка;
- протокол AH защищает и данные и оба заголовка.

В туннельном режиме:
- аутентификация в ESP протоколе применяется к данным пакета и исходному IP-заголовку, но не затрагивает новый IP-заголовок;
- протокол AH аутентифицирует данные, AH-заголовок и оба IP-заголовка.

Протокол ESP может применяться отдельно или совместно с протоколом AH. При совместном использовании протоколы AH и ESP могут комбинироваться разными способами. Если используется транспортный режим, то аналогично тому, как в рамках ESP аутентификация идет следом за шифрованием, протокол AH должен применяться после протокола ESP. В туннельном режиме протоколы AH и ESP применяются к разным вложенным пакетам и, кроме того, допускается многократная вложенность туннелей с различными начальными и/или конечными точками.

12.2.3. Алгоритмы аутентификации и шифрования в IPSec

Стек протоколов IPSec представляет собой согласованный набор открытых стандартов, имеющий вполне определенное ядро, и в то же время он может быть достаточно просто дополнен новыми протоколами, алгоритмами и функциями. Благодаря модульной структуре протоколы AH и ESP допускают применение пользователями по их согласованному выбору различных криптографических алгоритмов аутентификации и шифрования. Для шифрования данных в IPSec (протокол ESP) может быть применен практически любой симметричный алгоритм шифрования, использующий секретные ключи.

Для обеспечения целостности и аутентификации данных (протоколы AH и ESP) используется один из приемов шифрования — шифрование с помощью *односторонней функции* (one-way function), называемой также *хэш-функцией* (hash function) или *дайджест-функцией* (digest function) [45, 72]. Эта функция, примененная к шифруемым данным, дает в результате значение-дай-

джест, состоящее из фиксированного небольшого числа байт. Дайджест передается в IP-пакете вместе с исходным сообщением. Получатель, зная, какая односторонняя функция шифрования была применена для составления дайджеста, заново вычисляет его, используя исходное сообщение. Если значения полученного и вычисленного дайджестов совпадают, это значит, что содержимое пакета во время передачи не было подвергнуто никаким изменениям. Знание дайджеста не дает возможности восстановить исходное сообщение и поэтому не может быть использовано для защиты конфиденциальности, но оно позволяет проверить целостность данных.

Дайджест является своего рода контрольной суммой для исходного сообщения. В отличие от традиционной контрольной суммы при вычислении дайджеста используется секретный ключ. Если для получения дайджеста применялась односторонняя функция с параметром (в качестве которого выступает секретный ключ), известным только отправителю и получателю, любая модификация исходного сообщения будет немедленно обнаружена.

В целях обеспечения совместимости продуктов разных производителей рабочая группа IETF определила базовый набор поддерживаемых функций и алгоритмов, который должен быть однотипно реализован во всех продуктах, поддерживающих IPSec. На сегодня определены 2 алгоритма аутентификации и 7 алгоритмов шифрования.

В настоящий момент для протоколов AH и ESP зарегистрировано 2 алгоритма аутентификации — HMAC-MD5 и HMAC-SHA1. Алгоритм HMAC (Keyed-Hashing for Message Authentication Code) определяется стандартом RFC 2104. Функции MD5 (Message Digest version 5, стандарт RFC 1321) и SHA1 (Secure Hash Algorithm version 1, стандарт FIPS 180-1) являются функциями хеширования. Алгоритмы HMAC-MD5 и HMAC-SHA1 являются алгоритмами аутентификации с общим секретным ключом. Секретный ключ имеет длину 128 бит в случае MD5 и 160 бит в случае SHA1 [9].

Если секретный ключ известен только передающей и принимающей сторонам, это обеспечит аутентификацию источника данных, а также целостность пакетов, пересылаемых между двумя сторонами. Ключи для HMAC генерируются посредством процедуры ISAKMP/Oakley. Для обеспечения совместимости оборудования и ПО на начальной стадии реализации протокола

IPSec один из зарегистрированных алгоритмов аутентификации принято использовать по умолчанию. В качестве такого алгоритма определен алгоритм HMAC-MD5.

Структура алгоритма HMAC показана на рис. 12.7. Принцип действия алгоритма HMAC заключается в двухкратной обработке пакета функцией хеширования, управляемой ключом аутентификации (например, функцией хеширования MD5). Как видно из рисунка, оба раза в обрабатываемые данные включается секретный ключ, который обеспечивает аутентификацию передаваемой информации. Полученная контрольная сумма помещается в заголовок AH протокола. Проверка аутентификации на другой стороне осуществляется путем повторного вычисления контрольной суммы для пришедшего пакета с использованием такого же ключа и сравнения полученного результата с присланным.

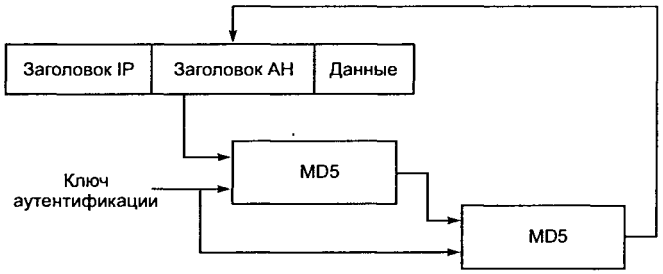


Рис. 12.7. Структура HMAC алгоритма

Алгоритм HMAC реализует симметричную схему аутентификации, используя параметр проверки целостности пакета ICV (Integrity Check Value). По сути, он представляет собой цифровую подпись, помещаемую в поле аутентификации и позволяющую отправителю подписать результат предварительного хеширования содержательной части пакета ESP.

Анализ содержимого этого поля дает возможность получателю идентифицировать источник данных и убедиться в том, что они не были изменены в процессе передачи. Если для протокола ESP функции аутентификации являются факультативными, то для протокола AH процесс аутентификации обязателен.

Для протокола ESP зарегистрировано несколько алгоритмов шифрования. Чаще всего в качестве алгоритмов шифрования для ESP применяются DES (Data Encryption Standard), 3DES (тройной DES) и новый стандарт шифрования AES (Advanced

Encryption Standard). Для обеспечения IPSec-совместимости по умолчанию в качестве алгоритма шифрования стандартом предусмотрен симметричный метод DES-CBC (Cipher Block Chaining) с явно заданным вектором инициализации IV и с 56-разрядным ключом. Алгоритм AES повсюду встраивается в стандарт IPSec как альтернатива DES и 3DES.

Выбор алгоритма шифрования целиком зависит от разработчика. Возможность выбора алгоритма шифрования предоставляет пользователю дополнительное преимущество: злоумышленник должен не только вскрыть шифр, но и определить, какой именно шифр ему надо вскрывать, а вместе с необходимостью подбора ключей, это еще более уменьшает его шансы своевременно расшифровать данные пользователя.

IPSec может работать совместно с протоколами L2TP или L2F, которые выполняют только туннелирование, но не обеспечивают шифрование и аутентификацию данных. Эти протоколы создают через Internet туннель для пакетов любых протоколов, упаковывая их в пакеты IP. Когда трафик с помощью L2F или L2TP оказывается упакованным в пакеты IP, то дальше для его защиты можно использовать IPSec. В результате комбинирование IPSec с протоколами туннелирования типа L2F/L2TP позволяет решить задачу защиты данных для протоколов, отличных от IP.

Алгоритмическая независимость протоколов AH и ESP требует предварительного согласования взаимодействующими сторонами набора применяемых алгоритмов и их параметров.

12.3. Протокол управления криптоключами IKE

Протоколы ESP и AH позволяют реализовать важнейшие атрибуты защищенной передачи — конфиденциальность связи, аутентификацию сторон и целостность данных. Однако их функции теряют всякую ценность в отсутствие мощной поддерживающей инфраструктуры, которая обеспечивала бы распределение ключей и согласование протоколов между участниками обмена.

Роль такой инфраструктуры в IPSec выполняет группа протоколов IKE (*Internet KeyExchange*). Это название пришло в 1998 г. на смену более раннему — ISAKMP/Oakley, которое непосредственно указывало на происхождение средств управления ключами в составе IPSec.

Протокол ISAKMP (*Internet Security Association and Key Management Protocol*), описанный в документе RFC 2408, позволяет согласовывать алгоритмы и математические структуры (так называемые мультипликативные группы, определенные на конечном поле) для процедуры обмена ключами Диффи — Хеллмана, а также процессов аутентификации [98, 102]. Протокол Oakley, описанный в RFC 2412, основан на алгоритме Диффи — Хеллмана и служит для организации непосредственного обмена ключами.

Протоколы IKE решают три задачи:

- осуществляют аутентификацию взаимодействующих сторон, согласовывают алгоритмы шифрования и характеристики ключей, которые будут использоваться в защищенном сеансе обмена информацией;
- обеспечивают создание, управление ключевой информации соединения, непосредственный обмен ключами (в том числе возможность их частой смены);
- управляют параметрами соединения и защитой от некоторых типов атак, контролируют выполнение всех достигнутых соглашений.

Разработчики IPSec начали свою деятельность с решения последней из перечисленных задач. В результате на свет появилась *концепция защищенных виртуальных соединений* или *безопасных ассоциаций SA* (*Security Associations*).

12.3.1. Установление безопасной ассоциации SA

Основой функционирования IPSec являются защищенные виртуальные соединения или *безопасные ассоциации SA* (Security Associations). Для того чтобы протоколы AH и ESP могли выполнять свою работу по защите передаваемых данных, между двумя конечными точками должна быть сформирована ассоциация SA — соглашение о защите обмена данными между двумя взаимодействующими партнерами.

Установление SA должно начинаться со взаимной аутентификации сторон, потому что меры безопасности теряют всякий смысл, если данные передаются или принимаются неавторизованными пользователями. Процедуры установления SA оправданы лишь в том случае, если у каждой из сторон имеется полная

уверенность в том, что ее партнер — именно тот, за кого он себя выдает.

Для выполнения аутентификации сторон в IKE применяются два основных способа.

Первый способ основан на использовании разделяемого секрета. Перед инициализацией IPSec-устройств, образующих безопасные ассоциации, в их БД помещается предварительно распределенный разделяемый секрет. Цифровая подпись на основе односторонней функции, например, MD5, использующей в качестве аргумента этот предварительно распределенный секрет, доказывает аутентичность противоположной стороны.

Второй способ основан на использовании технологии цифровой подписи и цифровых сертификатов стандарта X.509. Каждая из сторон подписывает свой цифровой сертификат своим закрытым ключом и передает эти данные противоположной стороне. Если подписанный сертификат расшифровывается открытым ключом отправителя, то это удостоверяет тот факт, что отправитель, предоставивший данные, действительно обладает ответной частью данного открытого ключа — соответствующим закрытым ключом.

Однако следует отметить, что для удостоверения аутентичности стороны нужно еще убедиться в аутентичности самого сертификата, и для этого сертификат должен быть подписан не только его владельцем, но и некоторой третьей стороной, выдавшей сертификат и вызывающей доверие. В архитектуре IPSec эта третья сторона именуется *органом сертификации CA* (Certification Authority). Этот орган призван засвидетельствовать подлинность обеих сторон и должен пользоваться полным доверием сторон, а его открытый ключ — известен всем узлам, использующим его сертификаты для удостоверения личностей друг друга.

После проведения взаимной аутентификации взаимодействующие стороны могут непосредственно перейти к согласованию параметров защищенного канала. Выбираемые параметры SA определяют: протокол, используемый для обеспечения безопасности передачи данных; алгоритм аутентификации протокола AH и его ключи; алгоритм шифрования, используемый протоколом ESP, и его ключи; наличие или отсутствие криптографической синхронизации; способы защиты сеанса обмена; частоту смены ключей и ряд других параметров. Важным параметром SA является так называемый криптографический материал, т. е. секретные ключи, используемые в работе протоколов AH и ESP. Сервисы

безопасности, предлагаемые IPSec, используют для формирования криптографических ключей разделяемые секреты.

Параметры SA должны устраивать обе конечные точки защищенного канала. Поэтому при использовании автоматической процедуры установления SA протоколы IKE, работающие по разные стороны канала, выбирают параметры в ходе переговорного процесса. Для каждой задачи, решаемой протоколами AH и ESP, предлагается несколько схем аутентификации и шифрования — это делает IPSec очень гибким средством. Безопасная ассоциация SA представляет собой в IPSec однонаправленное логическое соединение, поэтому при двустороннем обмене данными необходимо установить две ассоциации SA. В рамках одной ассоциации SA может работать только один из протоколов защиты данных — либо AH, либо ESP, но не оба вместе.

Для идентификации каждой SA предназначен *индекс параметров безопасности SPI* (Security Parameters Index). Этот индекс включается в заголовки защищенных IPSec-пакетов, чтобы принимающая сторона смогла правильно их расшифровать и аутентифицировать, воспользовавшись указанной безопасной ассоциацией.

Система IPSec допускает применение ручного и автоматического способа установления SA. При ручном способе администратор конфигурирует каждый конечный узел таким образом, чтобы они поддерживали согласованные параметры ассоциации, включая и секретные ключи.

Для автоматического установления ассоциации необходим соответствующий протокол, в качестве которого в стандартах IPSec определен протокол IKE. Он является комбинацией протоколов ISAKMP, Oakley и SKEME. Протокол согласования параметров виртуального канала и управления ключами ISAKMP (Internet Security Association Key Management Protocol) описывает базовую технологию аутентификации, обмена ключами и согласования остальных параметров IPSec-туннеля при создании SA, однако сами протоколы аутентификации сторон и обмена ключами в нем детально не определены. Поэтому при разработке протокола IKE общие правила и процедуры протокола ISAKMP дополнены процедурами аутентификации и обмена ключами, взятыми из протоколов Oakley и SKEME. Поскольку протокол IKE использует для управления ассоциациями алгоритмы и форматы протокола ISAKMP, названия этих протоколов иногда используют как синонимы.

На основании протокола ISAKMP согласование параметров защищенного взаимодействия необходимо как при формировании IPSec-туннеля, так и при формировании в его рамках каждого защищенного однонаправленного соединения. Параметры IPSec-туннеля согласуются по протоколу ISAKMP/Oakley. Параметры каждого защищенного однонаправленного соединения согласуются в рамках сформированного IPSec-туннеля и образуют SA.

Криптографические ключи для каждого защищенного однонаправленного соединения генерируются на основе ключей, выработанных в рамках IPSec-туннеля. При этом учитываются алгоритмы аутентификации и шифрования, используемые в протоколах аутентифицирующего заголовка (AH) и инкапсулирующей защиты (ESP).

Стандарты IPSec позволяют шлюзам использовать как одну ассоциацию SA для передачи трафика всех взаимодействующих через Internet хостов, так и создавать для этой цели произвольное число ассоциаций SA, например по одной на каждое соединение TCP.

12.3.2. Базы данных SAD и SPD

IPSec предлагает различные методы защиты трафика.

В каждом узле, поддерживающем IPSec, используются БД двух типов:

- база данных безопасных ассоциаций SAD (Security Associations Database);
- база данных политики безопасности SPD (Security Policy Database).

При установлении SA две вступающие в обмен стороны принимают ряд соглашений, регламентирующих процесс передачи потока данных между ними. Соглашения представляются в виде набора параметров. Для SA такими параметрами являются, в частности, тип и режим работы протокола защиты (AH или ESP), методы шифрования, секретные ключи, значение текущего номера пакета в ассоциации и другая информация.

Объединение служебной информации в рамках SA предоставляет пользователю возможность сформировать разные классы защиты, предназначенные, например, для электронного общения с разными «собеседниками». Другими словами, применение

структур SA открывает путь к построению множества виртуальных частных сетей, различающихся своими параметрами.

Наборы текущих параметров, определяющих все активные ассоциации, хранятся на обоих оконечных узлах защищенного канала в виде SAD. Каждый узел IPSec поддерживает две базы SAD — одну для исходящих ассоциаций, другую — для входящих.

SPD задает соответствие между IP-пакетами и установленными для них правилами обработки. При обработке пакетов БД SPD используются совместно с БД SAD. SPD представляет собой упорядоченный набор правил, каждое из которых включает совокупность селекторов и допустимых политик безопасности. Селекторы служат для отбора пакетов, а политики безопасности задают требуемую обработку. Такая БД формируется и поддерживается на каждом узле, где установлено ПО IPSec.

12.4. Особенности реализации средств IPSec

Выше было рассмотрено, что протоколы AH или ESP могут защищать передаваемые данные в двух режимах: туннельном, при котором IP-пакеты защищаются целиком, включая их заголовки, и транспортном, обеспечивающим защиту только содержимого IP-пакетов.

Основным режимом является туннельный. В туннельном режиме исходный пакет помещается в новый IP-пакет и передача данных по сети выполняется на основании заголовка нового IP-пакета. При работе в этом режиме каждый обычный IP-пакет помещается целиком в криптозащищенном виде в конверт IPSec, а тот в свою очередь инкапсулируется в другой защищенный IP-пакет. Туннельный режим обычно реализуют на специально выделенных шлюзах безопасности, в роли которых могут выступать маршрутизаторы или МЭ. Между такими шлюзами и формируются защищенные туннели IPSec.

После приема на другой стороне туннеля защищенные IP-пакеты «распаковываются» и полученные исходные IP-пакеты передаются компьютерам приемной локальной сети по стандартным правилам. Туннелирование IP-пакетов полностью прозрачно для обычных компьютеров в локальных сетях, являющихся держателями туннелей. На оконечных системах туннельный режим может использоваться для поддержки удаленных и мобиль-

ных пользователей. В этом случае на компьютерах этих пользователей должно быть установлено ПО, реализующее туннельный режим IPSec.

В транспортном режиме передача IP-пакета через сеть выполняется с помощью исходного заголовка этого пакета. В конверт IPSec в криптозащищенном виде помещается только содержимое исходного IP-пакета и к полученному конверту добавляется исходный IP-заголовок. Транспортный режим быстрее туннельного и разработан для применения на оконечных системах. Этот режим может использоваться для поддержки удаленных и мобильных пользователей, а также защиты информационных потоков внутри локальных сетей. Следует отметить, что работа в транспортном режиме отражается на всех входящих в группу защищенного взаимодействия системах, и в большинстве случаев требуется перепрограммирование сетевых приложений.

12.4.1. Основные схемы применения IPSec

Применение туннельного или транспортного режима зависит от требований, предъявляемых к защите данных, а также от роли узла, в котором работает IPSec. Узлом, завершающим защищенный канал, может быть хост (конечный узел) или шлюз (промежуточный узел) [48]. Соответственно различают три основные схемы применения IPSec:

1) хост—хост;
2) шлюз—шлюз;
3) хост—шлюз.

В схеме 1 защищенный канал, или, что в данном контексте одно и то же, SA, устанавливается между двумя конечными узлами сети, т. е. хостами H1 и H2 (рис. 12.8). Протокол IPSec в этом случае работает на конечном узле и защищает данные,

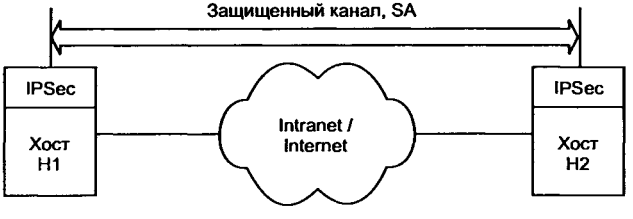


Рис. 12.8. Схема хост—хост

поступающие на него. Для хостов, поддерживающих IPSec, разрешается использовать как транспортный режим, так и туннельный.

В соответствии со схемой 2 защищенный канал устанавливается между двумя промежуточными узлами, называемыми шлюзами безопасности SG1 и SG2 (*Security Gateway*), на каждом из которых работает протокол IPSec (рис. 12.9).

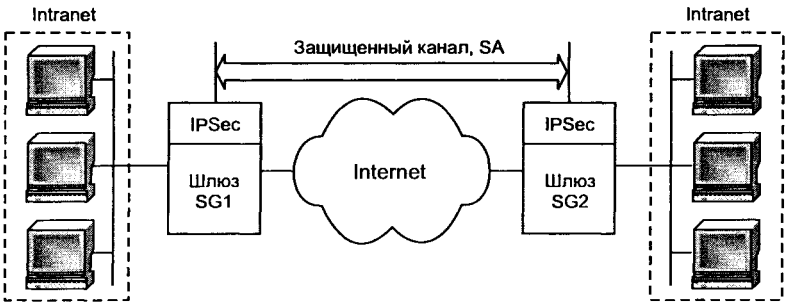


Рис. 12.9. Схема шлюз—шлюз

Защищенный обмен данными может происходить между любыми двумя конечными узлами, подключенными к сетям, которые расположены позади шлюзов безопасности. От конечных узлов поддержка протокола IPSec не требуется, они передают свой трафик в незащищенном виде через заслуживающие доверие сети Intranet предприятия. Трафик, направляемый в общедоступную сеть, проходит через шлюз безопасности, который и обеспечивает его защиту с помощью IPSec, действуя от своего имени. Шлюзам разрешается использовать только туннельный режим работы, хотя они могли бы поддерживать и транспортный режим, но он в этом случае малоэффективен.

При защищенном удаленном доступе часто применяется схема 3 хост—шлюз (рис. 12.10).

Здесь защищенный канал организуется между удаленным хостом H1, на котором работает IPSec, и шлюзом SG, защищающим трафик для всех хостов, входящих в сеть Intranet предприятия. Удаленный хост может использовать при отправке пакетов шлюзу как транспортный, так и туннельный режим, шлюз же отправляет пакеты хосту только в туннельном режиме.

Эту схему можно модифицировать, создав параллельно еще один защищенный канал — между удаленным хостом H1 и ка-

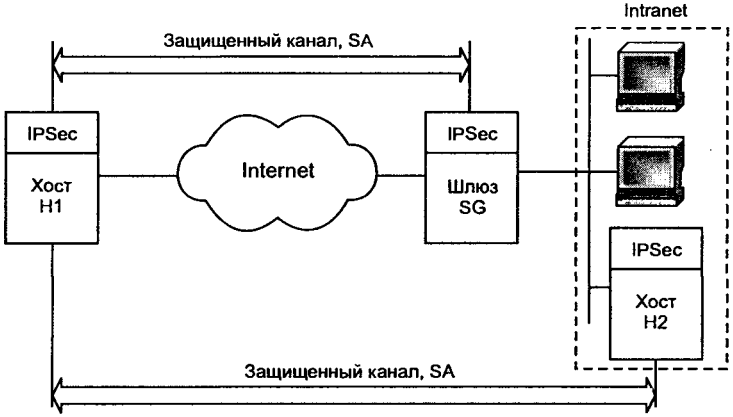


Рис. 12.10. Схема хост—шлюз, дополненная каналом хост—хост

ким-либо хостом H2, принадлежащим внутренней сети, защищаемой шлюзом. Такое комбинированное использование двух SA позволяет надежно защитить трафик и во внутренней сети.

Рассмотренные схемы построения защищенных каналов на базе IPSec широко применяются при создании разнообразных виртуальных защищенных сетей VPN. Их спектр варьируется от провайдерских сетей, позволяющих управлять обслуживанием клиентов непосредственно на их площадях, до корпоративных сетей VPN, разворачиваемых и управляемых самими компаниями. На базе IPSec успешно реализуются виртуальные защищенные сети любой архитектуры, включая VPN с удаленным доступом (Remote Access VPN), внутрикорпоративные VPN (Intranet VPN) и межкорпоративные VPN (Extranet VPN).

12.4.2. Преимущества средств безопасности IPSec

Система стандартов IPSec вобрала в себя прогрессивные методики и достижения в области сетевой безопасности, завоевала признание специалистов как надежная и легко интегрируемая система безопасности для IP-сетей. Система IPSec прочно занимает сегодня лидирующие позиции в наборе стандартов для создания VPN. Этому способствует ее открытое построение, способное включать все новые достижения в области криптографии. IPsec позволяет защитить сеть от большинства сетевых атак,

«сбрасывая» чужие пакеты еще до того, как они достигнут уровня IP на принимающем компьютере. В защищаемый компьютер или сеть могут войти только пакеты от зарегистрированных партнеров по взаимодействию.

IPsec обеспечивает:

- аутентификацию — доказательство отправки пакетов вашим партнером по взаимодействию, т. е. обладателем разделяемого секрета;
- целостность — невозможность изменения данных в пакете;
- конфиденциальность — невозможность раскрытия передаваемых данных;
- надежное управление ключами — протокол IKE вычисляет разделяемый секрет, известный только получателю и отправителю пакета;
- туннелирование — полную маскировку топологии локальной сети предприятия.

Работа в рамках стандартов IPSec обеспечивает полную защиту информационного потока данных от отправителя до получателя, закрывая трафик для наблюдателей на промежуточных узлах сети. VPN-решения на основе стека протоколов IPSec обеспечивают построение виртуальных защищенных сетей, их безопасную эксплуатацию и интеграцию с открытыми коммуникационными системами.

Глава 13
ИНФРАСТРУКТУРА ЗАЩИТЫ НА ПРИКЛАДНОМ УРОВНЕ

Развитие ИТ позволяет повысить эффективность деятельности компаний, а также открывает новые возможности для взаимодействия с потенциальными клиентами на базе общедоступных сетей, в том числе Интернета. Создание Web-сайта — своеобразного представительства предприятия в Интернете — является лишь первым шагом на этом пути. Активное ведение коммерческих операций в Сети предполагает массовый доступ потребителей электронных услуг (или Web-клиентов) к Internet-приложениям и проведение электронных транзакций миллионами пользователей Сети. Размещение Internet-приложений внутри корпоративной сети может нанести ущерб безопасности ИТ-инфраструктуры, поскольку открытие доступа через МЭ неизбежно создает потенциальную возможность для несанкционированного проникновения злоумышленников в сеть предприятия.

Обеспечение информационной безопасности должно включать решение таких задач, как безопасный доступ к Web-серверам и Web-приложениям, аутентификация и авторизация пользователей, обеспечение целостности и конфиденциальности данных, реализация электронной цифровой подписи и др.

Организации нуждаются в надежных, гибких и безопасных методах и средствах для получения и использования открытой и конфиденциальной информации многочисленными группами людей — своими сотрудниками, партнерами, клиентами и поставщиками. Проблема заключается в обеспечении доступа к такой информации только авторизованным пользователям. Целесообразно использовать интегрированную систему управления доступом пользователей к чувствительной информации в широ-

ком диапазоне точек доступа и приложений. Такая система решает многие проблемы контроля доступа, с которыми сталкиваются организации, обеспечивая при этом удобный доступ и высокую безопасность.

13.1. Управление идентификацией и доступом

Для реализации растущих потребностей электронного бизнеса необходимо построить надежную с точки зрения безопасности среду для осуществления электронного бизнеса в режиме on-line. Технологии, которые дают возможность осуществлять электронный бизнес, выполняют четыре основные функции:

- аутентификацию, или проверку подлинности пользователя;
- управление доступом, позволяющее авторизованным пользователям получать доступ к требуемым ресурсам;
- шифрование, гарантирующее, что связь между пользователем и базовой инфраструктурой защищена;
- неотказуемость, означающую, что пользователи не могут позднее отказаться от выполненной транзакции (обычно реализуется с помощью цифровой подписи и инфраструктуры открытых ключей) (рис. 13.1).

Рис. 13.1. Технологии, обеспечивающие электронный бизнес

Только решение, которое выполняет все эти четыре функции, может создать доверенную среду, способную по-настоящему обеспечить реализацию электронного бизнеса.

Управление доступом является критическим компонентом общей системы безопасности. Система управления доступом обеспечивает авторизованным пользователям доступ к надлежащим ресурсам. Проектирование этой инфраструктуры требует тонкого баланса между предоставлением доступа к критическим ресурсам только авторизованным пользователям и обеспечением необходимой безопасности этих ресурсов, известных большому числу пользователей.

13.1.1. Особенности управления доступом

В распределенной корпоративной сети обычно применяются два метода управления доступом:

- управление сетевым доступом (регулирует доступ к ресурсам внутренней сети организации);
- управление Web-доступом (регулирует доступ к Web-серверам и их содержимому).

Все запросы на доступ к ресурсам проходят через один или более *списков контроля доступа ACL* (Access Control List). ACL является набором правил доступа, которые задают для набора защищаемых ресурсов. Ресурсы с низким риском будут иметь менее строгие правила доступа, в то время как высококритичные ресурсы должны иметь более строгие правила доступа. ACL, по существу, определяют политику безопасности.

Доступ к сетевым ресурсам организации можно регулировать путем создания списков контроля доступа Login ACL, которые позволяют точно определить конкретные разрешения и условия для получения доступа к ресурсам внутренней сети.

Средства контроля и управления Web-доступом позволяют создавать и исполнять политику Web-доступа. Создавая конкретные списки контроля Web доступа Web ACL, администраторы безопасности определяют, какие пользователи могут получить доступ к Web-серверам организации и их содержимому и при каких заранее установленных условиях.

Управление доступом упрощается при применении единой централизованной инфраструктуры контроля и управления доступом, которая может разрешить пользователям «самообслуживание», поручая им такие задачи управления, как регистрация, редактирование профиля, восстановление пароля и управление подпиской. Она может также обеспечить делегирование администрирования, передачу функций управления пользователями, людям, наиболее осведомленным о конкретной группе пользователей как внутри — в бизнес-подразделениях организации, так и вне ее — у клиентов и в подразделениях бизнес-партнеров. Чтобы облегчить поддержку системы безопасности масштаба предприятия, средства управления доступом могут получать данные пользователей и политик, уже хранимых в таких существующих хранилищах данных, как каталоги LDAP и реляционные БД.

13.1.2. Функционирование системы управления доступом

Централизованные системы управления доступом выпускаются рядом компаний, в частности Secure Computing, RSA Security Inc., Baltimore и др.

Рассмотрим функционирование системы управления доступом на примере системы PremierAccess компании Secure Computing. Эта система осуществляет управление Web и сетевым доступом всех пользователей, включая внутренних пользователей, удаленных сотрудников, клиентов, поставщиков и бизнес-партнеров. Она базируется на политике безопасности, которая позволяет персонализировать права доступа пользователей. Пользователи получают доступ только к тем ресурсам, на которые было дано разрешение в соответствии с их правами доступа, через Web-доступ, VPN-доступ или удаленный доступ с использованием серверов RADIUS. В системе реализованы основанные на применении каталогов процессы аутентификации, авторизации и администрирования действий пользователей. Система поддерживает различные типы аутентификаторов — от многоразовых паролей до биометрических средств аутентификации. Предпочтение отдается методам и средствам строгой аутентификации.

Средства управления пользователями позволяют управлять большим числом пользователей. Сервер регистрации дает возможность самим пользователям регистрироваться в сети, используя стандартные Web-браузеры. В процессе регистрации пользователям назначаются *роли*. Роли являются ярлыками, идентифицирующими группы пользователей, которые разделяют одинаковые права доступа. Иначе говоря, роли определяют наборы правил доступа, применяемые к конкретным группам пользователей. Категорирование пользователей по ролям можно выполнить на основе их функциональных обязанностей.

Средства управления сетевым доступом

В системе управления доступом используются так называемые агенты. *Агент* системы — это программный модуль, инсталлированный на соответствующий сервер в рамках корпоративной сети (рис. 13.2).

В качестве таких агентов выступают агенты удаленного доступа, агенты VPN-доступа, агенты серверов RADIUS, Novel,

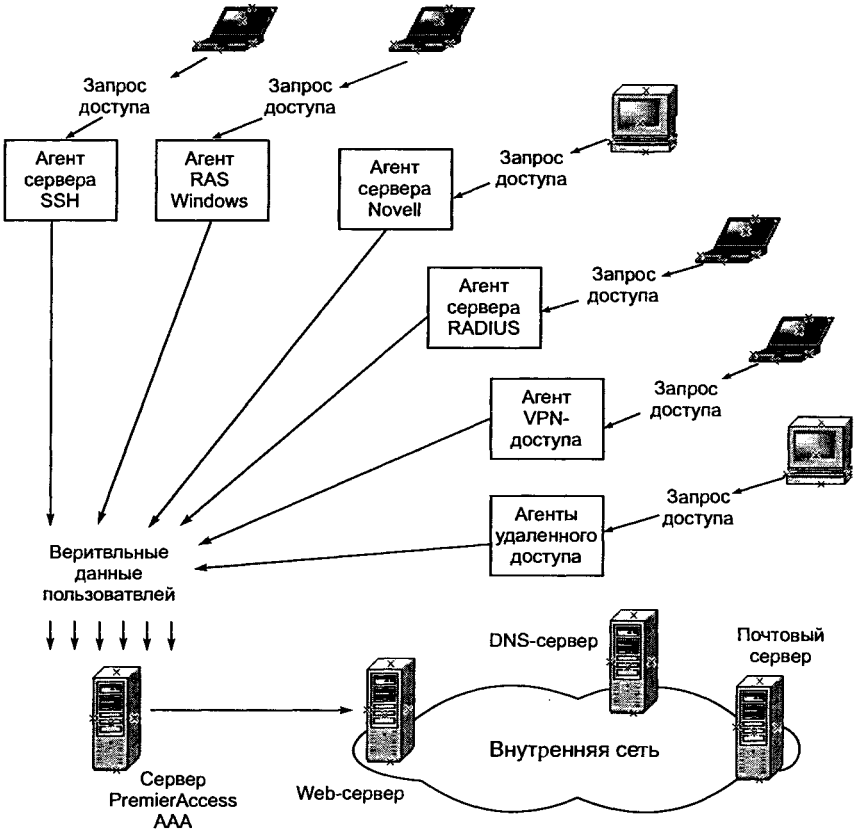


Рис. 13.2. Схема управления доступом к сети

RAS, Citrix и др. При попытке пользователя подключиться к внутренней сети, агенты системы перехватывают запрос пользователя на вход в сеть.

Агенты действуют как точки аутентификации пользователей UAPs (User Authentication Points) на линиях коммуникации с сервером PremierAccess. В ответ на запрос пользователя агент запрашивает у пользователя его верительные данные — идентификатор пользователя и аутентификатор. Отвечая на запрос агента, пользователь вводит свои данные. Эти верительные данные передаются AAA-серверу (AAA — Authentication, Authorization, Accounting).

AAA-сервер сравнивает идентификатор ID пользователя или сертификат с данными, хранимыми в каталоге LDAP, с целью

проверки их тождественности. Если идентификатор ID пользователя совпадает с хранимым, запись пользователя в БД проверяется по роли (или ролям) и ресурсам, к которым они авторизуются. Для аутентификации могут применяться фиксированный пароль, аппаратный или программный аутентификаторы. Если пользователь успешно проходит все шаги подтверждения своей подлинности, он получает доступ к ресурсу сети.

Средства управления Web-доступом

Система PremierAccess использует универсальный Web-агент UWA (Universal Web Agent), который инсталируется на хост-машине каждого защищаемого Web-сервера. В рассматриваемом примере в качестве пользователя выступает бизнес-партнер, который запрашивает доступ к защищаемому Web-ресурсу компании (рис. 13.3).

Управление Web-доступом реализуется в виде процесса, состоящего из двух этапов.

1. Пользователь пытается войти в систему, используя сервер WLS (Web Login Server). Запрос пользователя на доступ к защи-

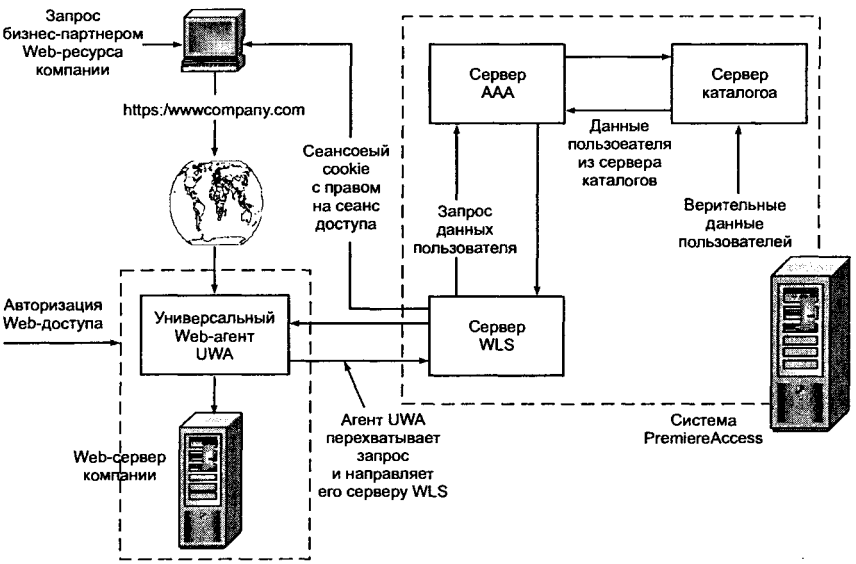


Рис. 13.3. Схема управления Web-доступом

щенному Web-ресурсу компании перехватывается агентом UWA, который для обработки этого запроса обращается к серверу WLS. Сервер WLS запрашивает результат аутентификации у сервера AAA. В случае успешной аутентификации сервер WLS генерирует сеансовый cookie, который содержит сеансовый идентификатор пользователя.

2. Пользователь пытается получить доступ к Web-ресурсу. Сервер WLS использует сеансовый идентификатор в cookie для запроса у AAA-сервера данных сеанса пользователя. Чтобы выполнить запрос на доступ, сервер WLS передает пользователю сеансовый cookie с правами на сеанс. Агент UWA получает сеансовый ID, затем получает от AAA-сервера данные сеанса. Основываясь на ролях пользователя и политике доступа, он принимает решение, давать или запретить пользователю доступ к Web-ресурсу.

При построении систем управления доступом важное значение имеют:

- средства и протоколы аутентификации удаленных пользователей;
- средства управления доступом по схеме однократного входа с авторизацией Single Sign-On;
- инфраструктуры управления открытыми ключами PKI.

Перечисленные средства и системы рассматриваются в последующих разделах данной главы.

13.2. Организация защищенного удаленного доступа

Удаленный доступ к компьютерным ресурсам стал в настоящее время таким же актуальным и значимым, как и доступ в режиме непосредственного подключения. Удаленный доступ к корпоративной сети осуществляется из незащищенного внешнего окружения через открытые сети. Поэтому средства построения защищенной корпоративной сети должны обеспечить безопасность сетевого взаимодействия при подключении к сети удаленных компьютеров.

Удаленный доступ к корпоративной сети возможен через глобальную компьютерную сеть или через среду передачи информации, образованную цепочкой из телефонной и глобальной компьютерной сетей. Доступ через глобальную сеть Internet яв-

ляется достаточно эффективным способом, причем для подключения удаленного пользователя к Internet может использоваться канал телефонной связи. Основные достоинства удаленного доступа к корпоративной сети через Internet:

- обеспечение масштабируемой поддержки удаленного доступа, позволяющей мобильным пользователям связываться с Internet-провайдером и затем через Internet входить в свою корпоративную сеть;
- сокращение расходов на информационный обмен через открытую внешнюю среду (удаленные пользователи, подключившись к Internet, связываются с сетью своей организации с минимальными затратами);
- управление трафиком удаленного доступа осуществляется так же, как любым другим трафиком Internet.

В корпоративной сети для взаимодействия с удаленными пользователями выделяется сервер удаленного доступа, который служит:

- для установки соединения с удаленным компьютером;
- аутентификации удаленного пользователя;
- управления удаленным соединением;
- посредничества при обмене данными между удаленным компьютером и корпоративной сетью.

Среди протоколов удаленного доступа к локальной сети наибольшее распространение получил протокол «точка—точка» PPP (Point-to-Point Protocol), который является открытым стандартом Internet. Протокол PPP предназначен для установления удаленного соединения и обмена информацией по установленному каналу пакетами сетевого уровня, инкапсулированными в PPP-кадры. Используемый в протоколе PPP метод формирования кадров обеспечивает одновременную работу через канал удаленной связи нескольких протоколов сетевого уровня.

Протокол PPP поддерживает следующие важные функции:

- аутентификации удаленного пользователя и сервера удаленного доступа;
- компрессии и шифрования передаваемых данных;
- обнаружения и коррекции ошибок;
- конфигурирования и проверки качества канала связи;
- динамического присвоения адресов IP и управления этими адресами.

На основе протокола PPP построены часто используемые при удаленном доступе протоколы PPTP, L2F и L2TP. Эти протоколы

позволяют создавать защищенные каналы для обмена данными между удаленными компьютерами и локальными сетями, функционирующими по различным протоколам сетевого уровня — IP, IPX или NetBEUI. Для передачи по телефонным каналам связи пакеты этих протоколов инкапсулируются в PPP-кадры. При необходимости передачи через Internet защищенные PPP-кадры инкапсулируются в IP-пакеты сети Internet. Криптозащита трафика возможна как в каналах Internet, так и на протяжении всего пути между компьютером удаленного пользователя и сервером удаленного доступа локальной сети.

13.2.1. Протоколы аутентификации удаленных пользователей

Контроль доступа пользователей к ресурсам корпоративной сети должен осуществляться в соответствии с политикой безопасности организации, которой принадлежит данная сеть. Эффективное разграничение доступа к сетевым ресурсам может быть обеспечено только при надежной аутентификации пользователей. Требования к надежности аутентификации удаленных пользователей должны быть особенно высокими, так как при взаимодействии с физически удаленными пользователями значительно сложнее обеспечить доступ к сетевым ресурсам. В отличие от локальных пользователей удаленные пользователи не проходят процедуру физического контроля при допуске на территорию организации.

При удаленном взаимодействии важна аутентификация не только пользователей, но и оборудования, поскольку подмена пользователя или маршрутизатора приводит к одним и тем же последствиям — данные из корпоративной сети передаются не тем лицам, которым они предназначены.

Для обеспечения надежной аутентификации удаленных пользователей необходимо выполнение следующих требований:

- проведение аутентификации обеих взаимодействующих сторон — как удаленного пользователя, так и сервера удаленного доступа — для исключения маскировки злоумышленников;
- оперативное согласование используемых протоколов аутентификации;

- осуществление динамической аутентификации взаимодействующих сторон в процессе работы удаленного соединения;
- применение криптозащиты передаваемых секретных паролей либо механизма одноразовых паролей для исключения перехвата и несанкционированного использования аутентифицирующей информации.

Протокол PPP имеет встроенные средства, которые могут быть использованы для организации аутентификации при удаленном взаимодействии. В стандарте RFC 1334 определены два протокола аутентификации:

- по паролю — PAP (Password Authentication Protocol);
- по рукопожатию — CHAP (Challenge Handshake Authentication Protocol).

В процессе установления удаленного соединения каждая из взаимодействующих сторон может предложить для применения один из стандартных протоколов аутентификации — PAP или CHAP [9].

Иногда компании создают собственные протоколы аутентификации удаленного доступа, работающие вместе с протоколом PPP. Эти фирменные протоколы обычно являются модификациями протоколов PAP и CHAP.

Широкое применение для аутентификации по одноразовым паролям получил протокол S/Key. В программных продуктах, обеспечивающих связь по протоколу PPP, протоколы PAP и CHAP, как правило, поддерживаются в первую очередь.

Протокол PAP

Суть работы протокола PAP довольно проста. В процессе аутентификации участвуют две стороны — проверяемая и проверяющая. Протокол PAP использует для аутентификации передачу проверяемой стороной идентификатора и пароля в виде открытого текста. Если проверяющая сторона обнаруживает совпадение идентификатора и пароля с записью, имеющейся у него в БД легальных пользователей, то процесс аутентификации считается успешно завершенным, после чего проверяемой стороне посылается соответствующее сообщение. В качестве стороны, чья подлинность проверяется, как правило, выступает удаленный пользователь, а в качестве проверяющей стороны — сервер удаленного доступа.

Для инициализации процесса аутентификации на базе протокола PAP сервер удаленного доступа после установления сеанса связи высылает удаленному компьютеру пакет LCP (Link Control Protocol) — протокол управления каналом, указывающий на необходимость применения протокола PAP. Далее осуществляется обмен пакетами PAP. Удаленный компьютер передает по каналу связи проверяющей стороне идентификатор и пароль, введенные удаленным пользователем. Сервер удаленного доступа по полученному идентификатору пользователя выбирает эталонный пароль из БД системы защиты и сравнивает его с полученным паролем. Если они совпадают, то аутентификация считается успешной, что сообщается удаленному пользователю.

Следует особо отметить, что протокол аутентификации PAP, согласно которому идентификаторы и пароли передаются по линии связи в незашифрованном виде, целесообразно применять только совместно с протоколом, ориентированным на аутентификацию по одноразовым паролям, например совместно с протоколом S/Key. В противном случае пароль, передаваемый по каналу связи, может быть перехвачен злоумышленником и использован повторно в целях маскировки под санкционированного удаленного пользователя.

Протокол CHAP

В протоколе CHAP используется секретный статический пароль. В отличие от протокола PAP, в протоколе CHAP пароль каждого пользователя для передачи по линии связи шифруется на основе случайного числа полученного от сервера. Такая технология обеспечивает не только защиту пароля от хищения, но и защиту от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем. Протокол CHAP применяется в современных сетях гораздо чаще, чем PAP, так как он использует передачу пароля по сети в защищенной форме, и, следовательно, гораздо безопаснее [9].

Шифрование пароля в соответствии с протоколом CHAP выполняется с помощью криптографического алгоритма хэширования и поэтому является необратимым. В стандарте RFC 1334 для протокола CHAP в качестве хэш-функции определен алгоритм MD5, вырабатывающий из входной последовательности любой длины 16-байтовое значение. Хотя минимальной длиной секрета является 1 байт, для повышения криптостойкости рекомендуется

использовать секрет длиной не менее 16 байт. Спецификация CHAP не исключает возможность использования других алгоритмов вычисления хэш-функций.

Для инициализации процесса аутентификации по протоколу CHAP сервер удаленного доступа после установления сеанса связи должен выслать удаленному компьютеру пакет LCP, указывающий на необходимость применения протокола CHAP, а также требуемого алгоритма хэширования. Если удаленный компьютер поддерживает предложенный алгоритм хэширования, то он должен ответить пакетом LCP о согласии с предложенными параметрами. В противном случае выполняется обмен пакетами LCP для согласования алгоритма хэширования.

После этого начинается аутентификация на основе обмена пакетами протокола CHAP.

В протоколе CHAP определены пакеты четырех типов:

- Вызов (Challenge);
- Отклик (Response);
- Подтверждение (Success);
- Отказ (Failure).

Протокол CHAP использует для аутентификации удаленного пользователя результат шифрования произвольного слова-вызова с помощью уникального секрета. Этот секрет имеется как у проверяющей, так и у проверяемой стороны. Процедура аутентификации начинается с отправки сервером удаленного доступа пакета Вызов (рис. 13.4).

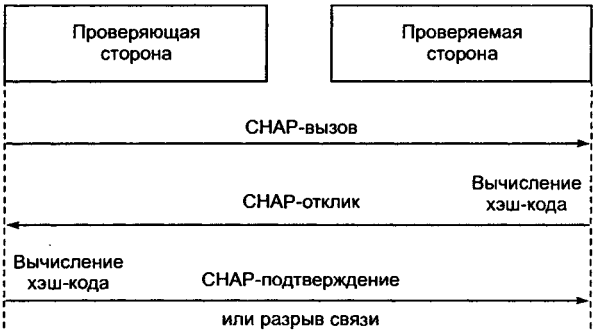


Рис. 13.4. Шаги процесса аутентификации по протоколу CHAP

Удаленный компьютер, получив пакет Вызов, зашифровывает его с помощью односторонней функции и известного ему

секрета, получая в результате дайджест. Дайджест возвращается проверяющей стороне в виде пакета Отклик.

Так как используется односторонняя хэш-функция, то по перехваченным пакетам Вызов и Отклик вычислить пароль удаленного пользователя практически невозможно.

Получив пакет Отклик, сервер удаленного доступа сравнивает содержимое результата из полученного пакета Отклик с результатом, вычисленным самостоятельно. Если эти результаты совпадают, то аутентификация считается успешной и сервер высылает удаленному компьютеру пакет Подтверждение.

В противном случае сервер удаленного доступа высылает пакет Отказ и разрывает сеанс связи.

Пакет Вызов должен быть отправлен сервером повторно, если в ответ на него не был получен пакет Отклик. Кроме того, пакет Вызов может отправляться периодически в течение сеанса удаленной связи для проведения динамической аутентификации, чтобы убедиться, что противоположная сторона не была подменена. Соответственно пакет Отклик должен отправляться проверяемой стороной в ответ на каждый принятый пакет Вызов.

Протокол S/Key

Одним из наиболее распространенных протоколов аутентификации на основе одноразовых паролей является стандартизованный в Интернете протокол S/Key (RFC 1760) [9, 32]. Этот протокол реализован во многих системах, требующих проверки подлинности удаленных пользователей, в частности в системе TACACS+ компании Cisco.

Перехват одноразового пароля, передаваемого по сети в процессе аутентификации, не предоставляет злоумышленнику возможности повторно использовать этот пароль, так как при следующей проверке подлинности необходимо предъявлять уже другой пароль. Поэтому схема аутентификации на основе одноразовых паролей, в частности S/Key, позволяет передавать по сети одноразовый пароль в открытом виде и, таким образом, компенсирует основной недостаток протокола аутентификации PAP.

Однако следует отметить, что протокол S/Key не исключает необходимость задания секретного пароля для каждого пользователя. Этот секретный пароль используется только для генерации одноразовых паролей. Для того чтобы злоумышленник не смог по перехваченному одноразовому паролю вычислить сек-

ретный исходный пароль, генерация одноразовых паролей выполняется с помощью односторонней, т. е. необратимой, функции. В качестве такой односторонней функции в спецификации протокола S/Key определен алгоритм хэширования MD4 (Message Digest Algorithm 4). Некоторые реализации протокола S/Key в качестве односторонней функции используют алгоритм хэширования MD5 (Message Digest Algorithm 5).

Поясним основную идею протокола S/Key на следующем примере.

Пусть удаленному пользователю (проверяемой стороне) для регулярного прохождения аутентификации необходим набор из 100 одноразовых паролей.

Проверяемой стороне заранее назначается генерируемый случайный ключ K в качестве ее секретного постоянного пароля. Затем проверяющая сторона выполняет процедуру инициализации списка одноразовых $N = 100$ паролей. В ходе данной процедуры проверяющая сторона с помощью односторонней функции h вычисляет по ключу K проверочное значение w_{101} для 1-го одноразового пароля. Для вычисления значения w_{101} ключ K подставляют в качестве аргумента функции h и данная функция рекурсивно выполняется 101 раз:

$$w_1 = h(K),\ w_2 = h(h(K)),\ w_3 = h(h(h(K))),\ \ldots,$$

$$w_{101} = h(h(h(\ldots h(K)\ldots))) = h^{101}(K).$$

Идентификатор пользователя и соответствующий этому пользователю секретный ключ K, а также несекретные числа N и w_{101} сохраняются в БД проверяющей стороны. Число N является номером одноразового пароля для очередной аутентификации из списка одноразовых паролей. Следует отметить, что после использования каждого такого одноразового пароля номер N уменьшается на единицу.

В процессе очередной аутентификации, проводимой после инициализации, проверяемая сторона предоставляет проверяющей стороне свой идентификатор, а та возвращает соответствующее этому идентификатору число N. В нашем примере $N = 100$. Затем проверяемая сторона вычисляет по своему секретному ключу K одноразовый пароль

$$w'_{100} = h(h(h(\ldots h(K))\ldots))) = h^{100}(K)$$

и посылает его проверяющей стороне.

Получив значение w'_{100}, проверяющая сторона выполняет над ним 1 раз одностороннюю функцию $w'_{101} = h(w'_{100})$. Далее проверяющая сторона сравнивает полученное значение w'_{101} со значением w_{101} из БД. Если они совпадают, то это означает, что и $w'_{100} = w_{100}$ и, следовательно, аутентификация является успешной.

В случае успешной аутентификации проверяющая сторона заменяет в БД для проверяемой стороны число w_{101} на полученное от нее число w'_{100}, а число N на $N = N - 1$. С учетом того, что при успешной аутентификации номер одноразового пароля N для очередной аутентификации уменьшился на 1, в БД проверяющей стороны совместно с идентификатором и секретным ключом K проверяемой стороны будут храниться числа $(N - 1)$ и w_{100}. Здесь под w_{100} понимается полученный от проверяемой стороны при успешной аутентификации последний одноразовый пароль. После использования очередного списка одноразовых паролей процедура инициализации должна выполняться снова.

Иногда желательно, чтобы пользователь имел возможность сам назначать секретный постоянный пароль. Для осуществления такой возможности спецификация S/Key предусматривает режим вычисления одноразовых паролей не только на основе секретного пароля, но и на основе генерируемого проверяющей стороной случайного числа. Таким образом, в соответствии с протоколом S/Key за каждым пользователем закрепляется идентификатор и секретный постоянный пароль.

Перед тем как проходить аутентификацию, каждый пользователь должен сначала пройти процедуру инициализации очередного списка одноразовых паролей, т. е. фазу парольной инициализации. Данная фаза выполняется по запросу пользователя на сервере удаленного доступа.

Для ускорения процедуры аутентификации определенное число одноразовых паролей, например несколько десятков, может быть вычислено заранее и храниться на удаленном компьютере в зашифрованном виде.

Протокол аутентификации на основе одноразовых паролей S/Key применяют, в частности, для улучшения характеристик протоколов централизованного контроля доступа к сети удаленных пользователей TACACS и RADIUS.

13.2.2. Централизованный контроль удаленного доступа

Для управления удаленными соединениями небольшой локальной сети вполне достаточно одного сервера удаленного доступа. Однако если локальная сеть объединяет относительно большие сегменты и число удаленных пользователей существенно возрастает, то одного сервера удаленного доступа недостаточно.

При использовании в одной локальной сети нескольких серверов удаленного доступа требуется централизованный контроль доступа к компьютерным ресурсам.

Рассмотрим, как решается задача контроля доступа к сети удаленных пользователей в соответствии с обычной схемой, когда удаленные пользователи пытаются получить доступ к сетевым ресурсам, которые находятся под управлением нескольких разных ОС. Пользователь дозванивается до своего сервера удаленного доступа, и RAS выполняет для него процедуру аутентификации, например по протоколу CHAP. Пользователь логически входит в сеть и обращается к нужному серверу, где снова проходит аутентификацию и авторизацию, в результате чего получает или не получает разрешение на выполнение запрошенной операции.

Нетрудно заметить, что такая схема неудобна пользователю, поскольку ему приходится несколько раз выполнять аутентификацию — при входе в сеть на сервере удаленного доступа, а потом еще каждый раз при обращении к каждому ресурсному серверу сети. Пользователь вынужден запоминать несколько разных паролей. Кроме того, он должен знать порядок прохождения разных процедур аутентификации в разных ОС. Возникают также трудности с администрированием такой сети. Администратор должен заводить учетную информацию о каждом пользователе на каждом сервере. Эти разрозненные БД трудно поддерживать в корректном состоянии. При увольнении сотрудника сложно исключить его из всех списков. Возникают проблемы при назначении паролей, существенно затрудняется аудит.

Отмеченные трудности преодолеваются при установке в сети централизованной службы аутентификации и авторизации. Для централизованного контроля доступа выделяется отдельный сервер, называемый *сервером аутентификации*. Этот сервер служит для проверки подлинности удаленных пользователей, определе-

ния их полномочий, а также фиксации и накопления регистрационной информации, связанной с удаленным доступом. Надежность защиты повышается, если сервер удаленного доступа запрашивает необходимую для аутентификации информацию непосредственно у сервера, на котором хранится общая БД системы защиты компьютерной сети.

Однако в большинстве случаев серверы удаленного доступа нуждаются в посреднике для взаимодействия с центральной БД системы защиты, например со службой каталогов.

Большинство сетевых ОС и служб каталогов сохраняют эталонные пароли пользователей с использованием одностороннего хэширования, что не позволяет серверам удаленного доступа, стандартно реализующим протоколы PAP и CHAP, извлечь открытый эталонный пароль для проверки ответа.

Роль посредника во взаимодействии между серверами удаленного доступа и центральной БД системы защиты может быть возложена на сервер аутентификации. Централизованный контроль удаленного доступа к компьютерным ресурсам с помощью сервера аутентификации выполняется на основе специализированных протоколов. Эти протоколы позволяют объединять используемые серверы удаленного доступа и сервер аутентификации в одну подсистему, выполняющую все функции контроля удаленных соединений на основе взаимодействия с центральной БД системы защиты. Сервер аутентификации создает единую точку наблюдения и проверки всех удаленных пользователей и контролирует доступ к компьютерным ресурсам в соответствии с установленными правилами.

К наиболее популярным протоколам централизованного контроля доступа к сети удаленных пользователей относятся протоколы TACACS (Terminal Access Controller Access Control System) и RADIUS (Remote Authentication Dial-In User Service). Они предназначены в первую очередь для организаций, в центральной сети которых используется несколько серверов удаленного доступа. В этих системах администратор может управлять БД идентификаторов и паролей пользователей, предоставлять им привилегии доступа и вести учет обращений к системным ресурсам [9].

Протоколы TACACS и RADIUS требуют применения отдельного сервера аутентификации, который для проверки подлинности пользователей и определения их полномочий может использовать не только собственную БД, но и взаимодействовать с со-

временными службами каталогов, например с NDS (Novell Directory Services) и Microsoft Windows NT Directory Service. Серверы TACACS и RADIUS выступают в качестве посредников между серверами удаленного доступа, принимающими звонки от пользователей, с одной стороны, и сетевыми ресурсными серверами — с другой. Реализации TACACS и RADIUS могут также служить посредниками для внешних систем аутентификации.

Рассмотрим особенности централизованного контроля удаленного доступа на примере протокола TACACS (рис. 13.5).

Система TACACS выполнена в архитектуре клиент—сервер [32]. В компьютерной сети, включающей несколько серверов удаленного доступа, устанавливается один сервер аутентификации, который называют сервером TACACS (обычно это программа, работающая в среде универсальной ОС, чаще всего Unix).

На сервере TACACS формируется центральная база учетной информации об удаленных пользователях, включающая их имена, пароли и полномочия. В полномочиях каждого пользователя задаются подсети, компьютеры и сервисы, с которыми он может

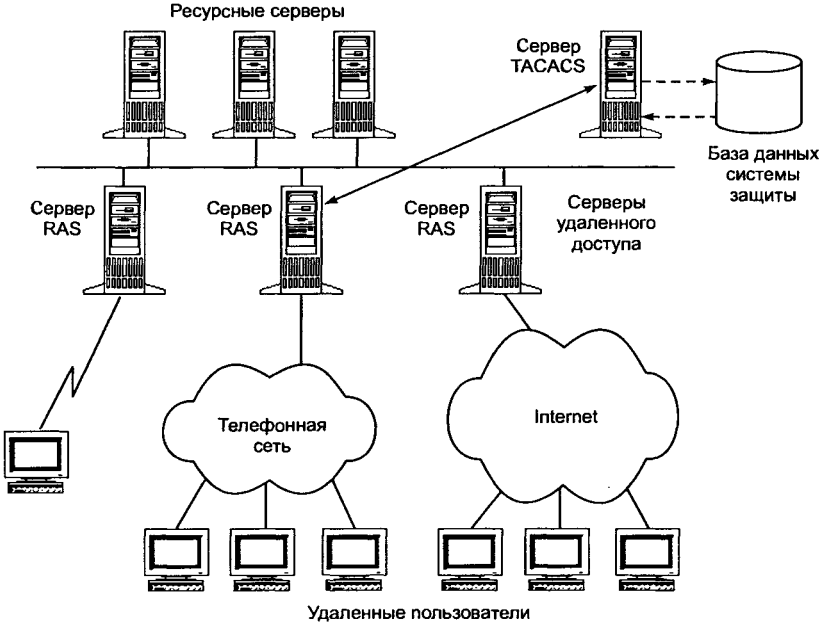


Рис. 13.5. Схема централизованного контроля удаленного доступа

работать, а также различные виды ограничений, например временные ограничения. На этом сервере ведется БД аудита, в которой накапливается регистрационная информация о каждом логическом входе, продолжительности сессии, а также времени использования ресурсов сети.

Клиентами сервера TACACS являются серверы удаленного доступа, принимающие запросы на доступ к ресурсам сети от удаленных пользователей. В каждый такой сервер встроено ПО, реализующее стандартный протокол, по которому они взаимодействуют с сервером TACACS. Этот протокол также называется TACACS.

Протокол TACACS стандартизует схему взаимодействия серверов удаленного доступа с сервером TACACS на основе задания возможных типов запросов, ответов и соединений. Определены запросы, с которыми клиенты могут обращаться к серверу TACACS. Сервер на каждый запрос должен ответить соответствующим сообщением. Протокол задает несколько типов соединений, каждое из которых определяется как последовательность пар запрос—ответ, ориентированная на решение отдельной задачи.

Определено три типа соединений:

- AUTH — выполняется только аутентификация;
- LOGIN — выполняется аутентификация и фиксируется логическое соединение с пользователем;
- SLIP — выполняется аутентификация, фиксируется логическое соединение, подтверждается IP-адрес клиента.

С помощью соединения AUTH серверы удаленного доступа перенаправляют серверу TACACS поток запросов на логическое подключение пользователей к сети в целом. Соединение LOGIN служит для перенаправления запросов серверу TACACS на логическое подключение пользователей к отдельным компьютерам локальной сети.

При соединении AUTH сервер удаленного доступа посылает на сервер TACACS только одно сообщение — пакет AUTH, на который сервер TACACS отвечает сообщением REPLY.

Сервер TACACS на основании имеющихся у него данных проверяет пароль и возвращает ответ в виде пакета REPLY, где сообщает об успехе или неуспехе аутентификации. В соответствии с протоколом TACACS пароль передается между сервером удаленного доступа и сервером аутентификации в открытом виде. Поэтому протокол TACACS необходимо применять совместно с

протоколом аутентификации по одноразовым паролям, например с протоколом S/Key.

На основании полученных от сервера TACACS указаний сервер удаленного доступа выполняет процедуру аутентификации и разрешает или не разрешает удаленному пользователю логически войти в сеть.

Сервер TACACS может выполнять аутентификацию и авторизацию удаленных пользователей различными способами:

- использовать встроенный механизм аутентификации той ОС, под управлением которой работает сервер;
- использовать централизованные справочные системы ОС;
- использовать системы аутентификации, основанные на одноразовых паролях, например систему SecurID;
- передавать запросы другим системам аутентификации, например, системе Kerberos.

Следует отметить, что недостатки протокола TACACS, связанные с открытой передачей пароля по сети, устранены компанией Cisco в версии, названной TACACS+. В соответствии с протоколом TACACS+ пароль для передачи по сети шифруется с помощью алгоритма MD5. TACACS+ предусматривает раздельное хранение БД аутентификационной, авторизационной и учетной информации, в том числе и на разных серверах. Улучшено взаимодействие с системой Kerberos.

Другой распространенной системой централизованной аутентификации при удаленном доступе является система RADIUS. По своим функциональным возможностям протоколы TACACS и RADIUS практически эквивалентны и являются открытыми стандартами, однако протокол RADIUS стал более популярен среди производителей систем централизованного контроля удаленного доступа. Это связано с тем, что основанное на нем серверное ПО распространяется бесплатно. Кроме того, протокол RADIUS менее сложен в реализации.

13.3. Управление доступом по схеме однократного входа с авторизацией Single Sign-On (SSO)

Большинство пользователей информационных средств и систем используют компьютеры для доступа к ряду сервисов, будь это несколько локальных приложений или сложные прило-

жения, которые включают одну или более удаленных систем, к которым машина пользователя подсоединяется через сеть. В целях обеспечения безопасности многие приложения требуют проведения аутентификации пользователя, прежде чем ему дадут доступ к сервисам и данным, предоставляемым приложением.

Конечные пользователи обычно воспринимают такие требования системы безопасности как дополнительную нагрузку, которая заставляет поддерживать и помнить многочисленные входные идентификаторы и пароли и использовать их каждый день по несколько раз, чтобы иметь возможность выполнять свою обычную работу. Довольно обычна ситуация, когда один пользователь имеет 5 и более таких пользовательских accounts, все на различных платформах, с различными правилами для длин паролей, а также с различной частотой их замены. Пользователь должен либо заучивать их, либо записывать, подвергая тем самым безопасность серьезному риску, так как их и могут найти неавторизованные пользователи.

С увеличением числа требующих запоминания паролей, возрастает вероятность того, что эти пароли будут забываться, а это потребует от администраторов дополнительных усилий по их восстановлению. Эту проблему часто называют «проблемой многих входов». Ее позволяет решить схема *однократного входа с авторизацией SSO* (Single Sign-On).

Управление доступом по схеме SSO дает возможность пользователям корпоративной сети при их входе в сеть пройти одну аутентификацию, предъявив только один раз пароль (или иной требуемый аутентификатор), и затем без дополнительной аутентификации получить доступ ко всем авторизованным сетевым ресурсам, которые нужны для выполнения их работы. Такими сетевыми ресурсами могут быть принтеры, приложения, файлы и другие данные, размещаемые по всему предприятию на серверах различных типов, работающих на базе различных ОС. Управление доступом по схеме SSO позволяет повысить производительность труда пользователей сети, уменьшить стоимость сетевых операций и улучшить сетевую безопасность.

С функционированием схемы SSO непосредственно связаны процессы аутентификации и авторизации. С помощью аутентификации система проверяет подлинность пользователя, в то время как авторизация определяет, что именно разрешается делать пользователю (обычно основываясь на его роли в организации). Большинство подходов SSO централизованно осуществляют ау-

тентификацию пользователя. Авторизацию обычно выполняют на ресурсах целевых объектов, хотя некоторые продвинутые SSO-решения централизованно осуществляют и авторизацию, при этом используются продукты централизованного администрирования безопасности, которые осуществляют администрирование полномочий пользователей.

Схему SSO поддерживают такие средства, как протокол LDAP (Lightweight Directory Access Protocol), протокол SSL (Secure Sockets Layer), система Kerberos и инфраструктура управления открытыми ключами PKI (Public Key Infrastructure), а также средства интеграции сервисов каталогов и безопасности. Эти средства и технологии образуют вместе фундамент для применения схемы SSO при обработке данных системами, использующими различные комбинации клиентов, серверов, сервисов и приложений.

Существующие решения схемы SSO простираются от простых средств до SSO-сервисов на базе сетевых ОС NOS (Network Operating System), многофункциональных приложений и SSO уровня предприятия [9].

Простые средства SSO включают кэш паролей Windows и кэш паролей, встроенный в продукты, подобные Internet Explorer и другие пакеты.

NOS-based SSO-сервисы дают возможность пользователю входить в такие сетевые ОС, как Windows NT/2000/XP, NetWare или Solaris, и таким образом получать доступ ко многим или ко всем приложениям, работающим на базе NOS.

Продукты SSO уровня предприятия, такие как IBM's Global Sign-On и др., обычно применяют комбинированные подходы к sign-on, основанные на использовании клиентов и proxy, технологии и стандарты кратной аутентификации, включая ввод ID пользователя и пароля.

13.3.1. Простая система однократного входа SSO

Простое SSO-решение состоит в том, чтобы просто автоматизировать процесс предъявления пароля. Для многих из продуктов SSO информация входа (т. е. имя пользователя и пароль) и любые необходимые записи хранятся в специальном сервере аутентификации. Используя клиентское ПО, пользователь предъявляет серверу аутентификации пароль, и этот сервер сообщает клиентско-

му ПО, к каким ресурсам может получить доступ пользователь (рис. 13.6). Клиентское ПО представляет пользователю допустимые опции. Когда пользователь выберет ресурс, клиентское ПО использует мандат входа и scripts, предоставленные сервером аутентификации, чтобы установить от имени пользователя соединение с соответствующим ресурсом целевого объекта (сервера, хоста, домена или приложения).

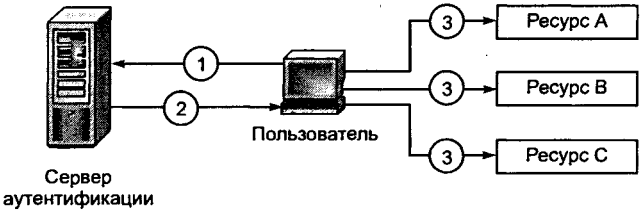


Рис. 13.6. Простое SSO-решение — автоматизация входа

При автоматизации процедуры входа выполняются следующие шаги.

1. Пользователь предъявляет серверу аутентификации пароль, используя специальное клиентское ПО на своем персональном компьютере.

2. Сервер аутентификации проверяет, к каким ресурсам может получить доступ этот пользователь и отправляет эту информацию обратно на клиентское SSO-приложение совместно с необходимым мандатом входа и scripts для соединения с каждым разрешенным ресурсом.

3. Клиентское SSO-приложение представляет пользователю доступные ресурсы и входит от имени пользователя в выбранные приложения.

Автоматизация процедуры входа позволяет получить простую схему SSO, но при этом еще больше децентрализуется администрирование безопасностью. Ряд поставщиков предлагает дополнительные средства централизованного администрирования безопасностью. Эти средства используют агентов в целевых системах и обеспечивают основанное на ролях (role-based) централизованное администрирование учетных записей пользователей и информации об их полномочиях. В некоторых случаях эти средства администрирования полностью отделены от схемы SSO; в других — интегрированы с SSO.

Первоначальной целью SSO было сокращение числа используемых многоразовых паролей для получения пользователями доступа к сетевым ресурсам. При формировании современного решения SSO применяются также такие средства аутентификации пользователя, как токены, цифровые сертификаты PKI, смарт-карты и биометрические устройства. Более совершенный подход к аутентификации обычно основан на использовании токенов. Наиболее известной системой аутентификации является Kerberos.

Продвинутые SSO-решения предоставляют больше контроля над полномочиями пользователя, поддерживаемыми обычно на прикладном уровне. В продуктах SSO могут быть также поддержаны нетокенные механизмы аутентификации, основанные на сертификатах PKI (в частности, RSA ClearTrust поддерживает PKI).

13.3.2. SSO-продукты уровня предприятия

SSO-продукты уровня предприятия проектируются для больших компаний с гетерогенной распределенной компьютерной средой, состоящей из многих систем и приложений.

Характерным представителем SSO-продуктов уровня предприятия является продукт IBM Global Sign-On for Multiplatforms (далее называемый GSO). Продукт GSO представляет безопасное, простое решение, позволяющее получать доступ к сетевым компьютерным ресурсам, используя однократный вход в систему. GSO освобождает пользователя от необходимости вводить различные идентификаторы и пароли для всех его целевых объектов, которые включают ОС, программные средства коллективного пользования, БД или приложения другого вида [9].

Было бы идеально, если бы GSO мог действовать как универсальный безопасный, надежный механизм аутентификации для любого целевого объекта. К сожалению, такое решение унифицированной аутентификации создать невозможно, потому что большинство продуктов, которым требуется сервис аутентификации, выполняют процедуру аутентификации различными способами. Чтобы сделать реальностью такой идеальный подход, поставщики должны модифицировать свои продукты таким образом, чтобы обеспечить выполнение требований общего стандарта X/Open Single Sign-On (XSSO).

Поэтому GSO придерживается реального подхода, основанного на том факте, что продукты поставщиков не поддерживают доверенную внешнюю аутентификацию. Для аутентификации эти продукты чаще всего требуют идентификатор ID и пароль каждого пользователя. GSO осуществляет безопасное хранение пользовательских идентификаторов IDs и паролей, а также обеспечение ими целевых объектов, когда пользователю нужно предъявить пароль при входе. Это освобождает пользователя от необходимости помнить и вводить IDs и пароль каждый день для каждого целевого объекта.

Ячейка GSO содержит, по крайней мере, сервер GSO и одну рабочую станцию пользователя, называемую также клиентом GSO. В ячейке GSO может быть более одного сервера GSO и множество клиентов (рис. 13.7).

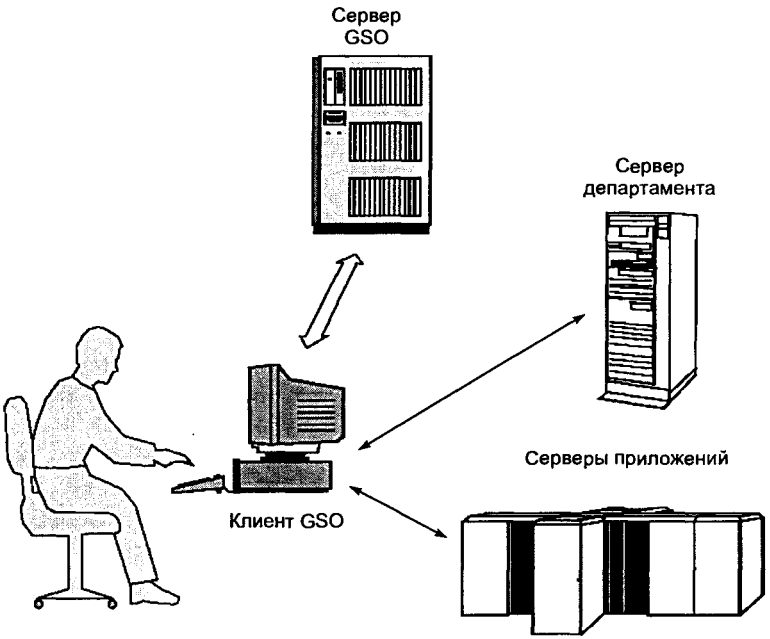


Рис. 13.7. Базовые компоненты GSO

Пользователь взаимодействует со своей рабочей станцией и некоторыми целевыми объектами (приложениями), которые могут выполняться на этой рабочей станции или на каком-либо

другом компьютере, например сервере департамента или серверах приложений.

Перед тем как начать работу, пользователь должен войти в свою рабочую станцию. Он предъявляет пароль именно GSO, а не приложению или другим серверам. GSO выполняет аутентификацию, основанную на идентификаторе ID и пароле пользователя (иногда поддерживаемых смарт-картой или считывателем отпечатков пальцев). Сервер GSO включается в процесс аутентификации, для того чтобы проверить пароль пользователя и извлечь его мандат (credentials).

Затем GSO вводит пользователя в целевые объекты (приложения или серверы), с которыми этот пользователь должен работать. GSO использует для входа пользователя методы, предоставляемые целевыми объектами. В большинстве случаев GSO имитирует вход пользователя, передавая целевому объекту ID и пароль пользователя, как будто вводит их сам пользователь. Важное различие, очевидно, состоит в том, что теперь пользователю не нужно запоминать эти идентификаторы ID и пароли, поскольку заботу о них принимает на себя GSO.

GSO является клиент/серверным приложением. В дополнение к серверу GSO существует программа клиента (сегмент программного кода), выполняемая на рабочей станции пользователя, которая взаимодействует с сервером GSO [9].

SSO-продукты уровня предприятия обладают следующими достоинствами:

- допускают использование многих целевых платформ со своими собственными механизмами аутентификации;
- безопасно хранят в БД учетную информацию пользователей (такую как идентификатор ID, пароль и некоторую дополнительную информацию) на каждую целевую платформу и каждого пользователя;
- радикально уменьшают долю забываемых паролей, поскольку пароли пользователей хранятся безопасно и надежно;
- используют методы и средства безопасной аутентификации и коммуникации; чувствительная пользовательская информация хранится и передается по сети только в зашифрованном виде.

Недостатками SSO-продуктов уровня предприятия является их относительно большая стоимость и высокие требования к квалификации обслуживающего персонала.

13.4. Протокол Kerberos

Протокол Kerberos используется в системах клиент—сервер для аутентификации и обмена ключевой информацией, предназначенной для установления защищенного канала связи между абонентами, работающими как в локальной сети, так и глобальных сетях. Данный протокол встроен в качестве основного протокола аутентификации в Microsoft Windows 2000 и в UNIX BSD.

Kerberos обеспечивает аутентификацию в открытых сетях, т. е. при работе Kerberos подразумевается, что злоумышленники могут производить следующие действия:

- выдавать себя за одну из легитимных сторон сетевого соединения;
- иметь физический доступ к одному из участвующих в соединении компьютеров;
- перехватывать любые пакеты, модифицировать их и (или) передавать повторно.

Соответственно, обеспечение безопасности в Kerberos построено таким образом, чтобы нейтрализовать любые потенциальные проблемы, которые могут возникнуть из-за указанных действий злоумышленников.

Kerberos разработан для сетей TCP/IP и построен на основе доверия участников протокола к третьей (доверенной) стороне. Служба Kerberos, работающая в сети, действует как доверенный посредник, обеспечивая надежную аутентификацию в сети с последующей авторизацией доступа клиента (клиентского приложения) к ресурсам сети. Защищенность установленных в рамках сессии Kerberos соединений обуславливается применением симметричных алгоритмов шифрования. Служба Kerberos разделяет отдельный секретный ключ с каждым субъектом сети, и знание такого секретного ключа равносильно доказательству подлинности субъекта сети.

Основу Kerberos составляет протокол аутентификации и распределения ключей Нидхэма — Шредера с третьей доверенной стороной [9]. Рассмотрим эту версию протокола. В протоколе Kerberos (версия 5) участвуют две взаимодействующие стороны и доверенный сервер KS, выполняющий роль Центра распределения ключей.

Вызывающий (исходный) объект обозначается через *A*, а вызываемый (объект назначения) — через *B*. Участники сеанса *A* и

B имеют уникальные идентификаторы Id_A и Id_B соответственно. Стороны *A* и *B*, каждая по отдельности, разделяют свой секретный ключ с сервером KS.

Пусть сторона *A* хочет получить сеансовый ключ для информационного обмена со стороной *B*.

Сторона *A* инициирует фазу распределения ключей, посылая по сети серверу KS идентификаторы Id_A и Id_B:

$$A \rightarrow \text{KS: } Id_A, Id_B. \quad (1)$$

Сервер KS генерирует сообщение с временно́й отметкой *T*, сроком действия *L*, случайным сеансовым ключом *K* и идентификатором Id_A. Он шифрует это сообщение секретным ключом, который разделяет со стороной *B*.

Затем сервер KS берет временну́ю отметку *T*, срок действия *L*, сеансовый ключ *K*, идентификатор Id_B стороны *B* и шифрует все это секретным ключом, который разделяет со стороной *A*. Оба эти зашифрованные сообщения он отправляет стороне *A*:

$$\text{KS} \rightarrow A\text{: } E_A(T, L, K, Id_B), E_B(T, L, K, Id_A). \quad (2)$$

Сторона *A* расшифровывает сообщение своим секретным ключом, проверяет отметку времени *T*, чтобы убедиться, что это сообщение не является повторением предыдущей процедуры распределения ключей. Затем сторона *A* генерирует сообщение со своим идентификатором Id_A и отметкой времени *T*, шифрует его сеансовым ключом *K* и отправляет стороне *B*. Кроме того, *A* отправляет для *B* сообщение от KS, зашифрованное ключом стороны *B*:

$$A \rightarrow B\text{: } E_K(Id_A, T), E_B(T, L, K, Id_A). \quad (3)$$

Только сторона *B* может расшифровать сообщение (3). Сторона *B* получает отметку времени *T*, срок действия *L*, сеансовый ключ *K* и идентификатор Id_A. Затем сторона *B* расшифровывает сеансовым ключом *K* вторую часть сообщения (3). Совпадение значений *T* и Id_A в двух частях сообщения подтверждают подлинность *A* по отношению к *B*.

Для взаимного подтверждения подлинности сторона *B* создает сообщение, состоящее из отметки времени *T* плюс 1, шифрует его ключом *K* и отправляет стороне *A*:

$$B \rightarrow A\text{: } E_K(T+1). \quad (4)$$

Если после расшифрования сообщения (4) сторона *A* получает ожидаемый результат, она знает, что на другом конце линии связи находится действительно *B*.

Этот протокол успешно работает при условии, что часы каждого участника синхронизированы с часами сервера KS. Следует отметить, что в этом протоколе необходим обмен с KS для получения сеансового ключа каждый раз, когда *A* желает установить связь с *B*. Протокол обеспечивает надежное соединение объектов *A* и *B* при условии, что ни один из ключей не скомпрометирован и сервер KS защищен.

Система Kerberos имеет структуру типа клиент—сервер и состоит из клиентских частей C, установленных на всех рабочих станциях пользователей и серверах сети, и сервера Kerberos KS, располагающегося на каком-либо (не обязательно выделенном) компьютере (см. рис. 13.8). Клиентами могут быть пользователи, а также независимые программы, выполняющие такие действия, как загрузка удаленных файлов, отправка сообщений, доступ к БД, доступ к принтерам, получение привилегий у администратора и т. п.

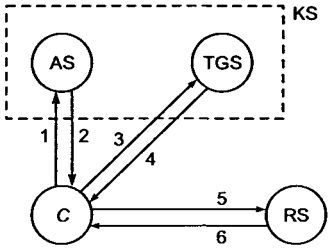
Сервер Kerberos KS, можно разделить на две части: сервер аутентификации AS (Authentication Server) и сервер службы выдачи мандатов TGS (Ticket Granting Service). Физически эти серверы могут быть совмещены. Информационными ресурсами, необходимыми клиентам C, управляет сервер информационных ресурсов RS. Предполагается, что серверы службы Kerberos надежно защищены от физического доступа злоумышленников.

Сетевые службы, требующие проверки подлинности, и клиенты, которые хотят использовать эти службы, регистрируют в Kerberos свои секретные ключи. Kerberos хранит БД о клиентах и их секретных ключах. Наличие в этой БД секретных ключей каждого пользователя и ресурсов сети, поддерживающих этот протокол, позволяет создавать зашифрованные сообщения, направляемые клиенту или серверу; успешное расшифрование этих сообщений и является гарантией прохождения аутентификации всеми участниками протокола.

Kerberos также создает *сеансовые ключи* (*session key*), которые выдаются клиенту и серверу (или двум клиентам) и никому больше. Сеансовый ключ используется для шифрования сообщений, которыми обмениваются две стороны, и уничтожается после окончания сеанса.

Область действия системы Kerberos распространяется на тот участок сети, все пользователи которого зарегистрированы под своими именами и паролями в БД сервера Kerberos.

Укрупненно процесс идентификации и аутентификации пользователя в системе Kerberos версии 5 можно описать следующим образом (рис. 13.8).



Обозначения:

KS — сервер системы Kerberos
AS — сервер аутентификации
TGS — сервер службы выделения мандатов
RS — сервер информационных ресурсов
C — клиент системы Kerberos

Рис. 13.8. Схема работы протокола Kerberos

Клиент *C*, желая получить доступ к ресурсу сети, направляет запрос серверу аутентификации AS. Сервер AS идентифицирует пользователя с помощью его имени и пароля и высылает клиенту *мандат* (*ticket*) на доступ к серверу службы выделения мандатов TGS (Ticket-Granting Service).

Для использования конкретного целевого сервера информационных ресурсов RS клиент *C* запрашивает у TGS мандат на обращение к целевому серверу RS. Если все в порядке, TGS разрешает использование необходимых ресурсов сети и посылает соответствующий мандат клиенту *C*.

Основные шаги работы системы Kerberos (см. рис. 13.10):

1. *C* → AS — запрос клиента *C* к серверу AS разрешить обратиться к службе TGS.

2. AS → *C* — разрешение (мандат) от сервера AS клиенту *C* обратиться к службе TGS.

3. *C* → TGS — запрос клиента *C* к службе TGS на получение допуска (мандата) к серверу ресурсов RS.

4. TGS → *C* — разрешение (мандат) от службы TGS клиенту *C* для обращения к серверу ресурсов RS.

5. *C* → RS — запрос информационного ресурса (услуги) у сервера RS.

6. RS → *C* — подтверждение подлинности сервера RS и предоставление информационного ресурса (услуги) клиенту *C*.

Данная модель взаимодействия клиента с серверами может функционировать только при условии обеспечения конфиденциальности и целостности передаваемой управляющей информации. Без строгого обеспечения информационной безопасности клиент *C* не может отправлять серверам AS, TGS и RS свои запросы и получать разрешения на доступ к обслуживанию в сети.

Чтобы избежать возможности перехвата и несанкционированного использования информации, Kerberos применяет при передаче любой управляющей информации в сети систему многократного шифрования с использованием комплекса секретных ключей (секретный ключ клиента, секретный ключ сервера, секретные сеансовые ключи пары клиент—сервер). Kerberos может использовать различные симметричные алгоритмы шифрования и хэш-функции.

На сегодняшний день протокол Kerberos является широко распространенным средством аутентификации. Kerberos может использоваться в сочетании с различными криптографическими схемами, включая шифрование с открытым ключом.

13.5. Инфраструктура управления открытыми ключами PKI

Исторически в задачи любого центра управления информационной безопасностью всегда входил набор задач по управлению ключами, используемыми различными средствами защиты информации (СЗИ). В этот набор входят выдача, обновление, отмена и распространение ключей.

В случае использования симметричной криптографии задача распространения секретных ключей представляла наиболее трудную проблему, поскольку:

- для N пользователей необходимо распространить в защищенном режиме $N(N-1)/2$ ключей, что обременительно при N порядка нескольких сотен;
- система распространения ключей сложна (много ключей и закрытый канал распространения), что приводит к появлению уязвимых мест.

Асимметричная криптография позволяет обойти эту проблему, предложив к использованию только N секретных ключей. При этом у каждого пользователя только один секретный ключ

и один открытый, полученный по специальному алгоритму из секретного.

Из открытого ключа практически невозможно получить секретный, поэтому открытый ключ можно распространять открытым способом всем участникам взаимодействия. На основании своего закрытого ключа и открытого ключа своего партнера по взаимодействию любой участник может выполнять любые криптографические операции: электронно-цифровую подпись, расчет разделяемого секрета, защиту конфиденциальности и целостности сообщения.

В результате решаются две главные проблемы симметричной криптографии:

- перегруженность количеством ключей — их теперь всего N;
- сложность распространения — их можно распространять открыто.

Однако у этой технологии есть один недостаток — подверженность атаке man-in-the-middle (человек-в-середине), когда атакующий злоумышленник расположен между участниками взаимодействия. В этом случае появляется риск подмены передаваемых открытых ключей.

Инфраструктура управления открытыми ключами PKI (Public Key Infrastructure) позволяет преодолеть этот недостаток и обеспечить эффективную защиту от атаки man-in-the-middle.

13.5.1. Принципы функционирования PKI

Инфраструктура открытых ключей PKI предназначена для надежного функционирования КИС и позволяет как внутренним, так и внешним пользователям безопасно обмениваться информацией с помощью цепочки доверительных отношений. Инфраструктура открытых ключей основывается на цифровых сертификатах, которые действуют подобно электронным паспортам, связывающим индивидуальный секретный ключ пользователя с его открытым ключом.

Защита от атаки man-in-the-middle

При осуществлении атаки man-in-the-middle атакующий может незаметно заменить передаваемые по открытому каналу открытые ключи законных участников взаимодействия на свой от-

крытый ключ, создать разделяемые секреты с каждым из законных участников и затем перехватывать и расшифровывать все их сообщения.

Поясним на примере (рис. 13.9) действия атакующего и способ защиты от этой атаки. Предположим, что пользователь 1 и пользователь 2 решили установить защищенное соединение, рассчитав общий для них разделяемый секрет по схеме Диффи — Хеллмана. Однако в момент передачи по открытому каналу открытых ключей K_1^0 и K_2^0 пользователей 1 и 2 злоумышленник @ перехватил эти ключи, не дав им дойти до адресатов. Создав свои закрытый и открытый ключи, злоумышленник @ передает свой открытый ключ $K_@^0$ пользователям 1 и 2, незаметно подменив своим ключом $K_@^0$ их подлинные открытые ключи K_1^0 и K_2^0. В результате пользователи 1 и 2 создадут разделяемые секреты не между собою, а между 1 ↔ @ и 2 ↔ @, поскольку они будут использовать свои закрытые ключи K_1^C и K_2^C и открытый ключ $K_@^0$ злоумышленника @.

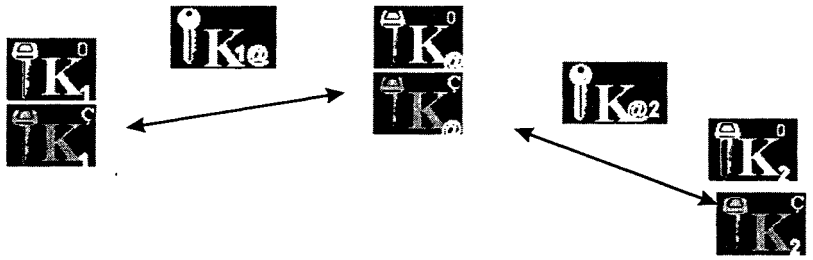


Рис. 13.9. Осуществление атаки man-in-the-middle

Когда пользователь 1 будет отправлять пользователю 2 зашифрованную информацию, злоумышленник @ может ее перехватить и расшифровать (у него с пользователем 1 свой разделяемый секрет $K_{@1}$). Затем злоумышленник @ зашифрует информацию (возможно, измененную) заново, используя второй разделяемый секрет $K_{@2}$, рассчитанный им и пользователем 2. В результате пользователь 2 будет получать, расшифровывать и использовать информацию, отправленную злоумышленником @, полагая, что он имеет защищенный канал с пользователем 1.

Эта простая, но результативная атака является расплатой за изящное решение задачи распределения ключей, предложенное асимметричной криптографией.

Проблема подмены открытых ключей успешно решается путем использования сертификатов открытых ключей.

Сертификаты открытых ключей

Сертификаты открытых ключей играют важную роль в криптографии открытых ключей. Их основное назначение — сделать доступным и достоверным открытый ключ пользователя.

В основу формирования сертификатов открытых ключей положены принципы строгой аутентификации, рекомендованные стандартом X.509 и базирующиеся на свойствах криптосистем с открытым ключом.

Криптосистемы с открытым ключом предполагают наличие у пользователя парных ключей — секретного и открытого (общедоступного). Каждый пользователь идентифицируется с помощью своего секретного ключа. С помощью парного открытого ключа любой другой пользователь имеет возможность определить, является ли его партнер по связи подлинным владельцем секретного ключа.

Процедура, позволяющая каждому пользователю устанавливать однозначное и достоверное соответствие между открытым ключом и его владельцем, обеспечивается с помощью механизма сертификации открытых ключей.

Степень достоверности факта установления подлинности (аутентификации) пользователя зависит от надежности хранения секретного ключа и надежности источника поставки открытых ключей пользователей. Чтобы пользователь мог доверять процессу аутентификации, он должен извлекать открытый ключ другого пользователя из надежного источника, которому он доверяет. Таким источником согласно стандарту X.509 является *Центр сертификации CA* (*Certification Authority*). Его называют также *Удостоверяющий центр* — УЦ; последний термин используется, в частности, в отечественном «Законе об ЭЦП» [62].

Центр сертификации CA является *доверенной третьей стороной*, обеспечивающей аутентификацию открытых ключей, содержащихся в сертификатах. CA имеет собственную пару ключей (открытый/секретный), где секретный ключ CA используется для подписывания сертификатов, а открытый ключ CA публикуется и используется пользователями для проверки подлинности открытого ключа, содержащегося в сертификате.

Сертификация открытого ключа — это подтверждение подлинности открытого ключа и хранимой совместно с ним служебной информацией, в частности о принадлежности ключа. Сертификация ключа выполняется путем вычисления ЭЦП сертифицируемого ключа и служебной информации с помощью специального секретного ключа-сертификата, доступного только СА. Иными словами, сертификация открытого ключа — это подписывание открытого ключа электронной подписью, вычисленной на секретном ключе СА.

Открытый ключ совместно с сертифицирующей его ЭЦП часто называют *сертификатом открытого ключа* или просто *сертификатом.*

СА формирует сертификат открытого ключа пользователя путем заверения цифровой подписью СА определенного набора данных.

В соответствии с форматом X.509 в этот набор данных включаются:

- период действия открытого ключа, состоящий из двух дат: начала и конца периода;
- номер и серия ключа;
- уникальное имя пользователя;
- информация об открытом ключе пользователя: идентификатор алгоритма, для которого предназначен данный ключ, и собственно открытый ключ;
- ЭЦП и информация, используемая при проведении процедуры проверки ЭЦП (например, идентификатор алгоритма генерации ЭЦП);
- уникальное имя сертификационного центра.

Таким образом, цифровой сертификат содержит три главные составляющие:

- информацию о пользователе — владельце сертификата;
- открытый ключ пользователя;
- сертифицирующую ЭЦП двух предыдущих составляющих, вычисленную на секретном ключе СА.

Сертификат открытого ключа обладает следующими свойствами:

- каждый пользователь, имеющий доступ к открытому ключу СА, может извлечь открытый ключ, включенный в сертификат;

- ни одна сторона, помимо CA, не может изменить сертификат так, чтобы это не было обнаружено (сертификаты нельзя подделать).

Так как сертификаты не могут быть подделаны, то их можно опубликовать, поместив в общедоступный справочник не предпринимая специальных усилий по защите этих сертификатов.

Создание сертификата открытого ключа начинается с создания пары ключей (открытый/секретный).

Процедура генерации ключей может осуществляться двумя способами.

1. CA создает пару ключей. Открытый ключ заносится в сертификат, а парный ему секретный ключ передается пользователю с обеспечением аутентификации пользователя и конфиденциальности передачи ключа.

2. Пользователь сам создает пару ключей. Секретный ключ сохраняется у пользователя, а открытый ключ передается по защищенному каналу в CA.

Каждый пользователь может быть владельцем одного или нескольких сертификатов, сформированных сертификационным центром CA пользователя. Пользователь может владеть сертификатами, полученными из нескольких разных сертификационных центров.

На практике часто возникает потребность аутентифицировать пользователя, который получает сертификаты в другом сертификационном центре. Принципы распределенного администрирования рассматриваются ниже.

Базовые модели сертификации

Концепция инфраструктуры открытых ключей PKI подразумевает, что все сертификаты конкретной PKI (своя PKI может быть у любой организации или организационной единицы) организованы в определенную структуру.

В PKI различают четыре типа сертификатов.

1. *Сертификат конечного пользователя* (описанный выше).

2. *Сертификат CA.* Должен быть доступен для проверки ЭЦП сертификата конечного пользователя и подписан секретным ключом CA верхнего уровня, причем эта ЭЦП также должна проверяться, для чего должен быть доступен сертификат CA верхнего уровня, и т. д.

3. *Самоподписанный сертификат.* Является *корневым* для всей PKI и доверенным по определению — в результате проверки цепочки сертификатов CA выяснится, что один из них подписан корневым секретным ключом, после чего процесс проверки ЭЦП сертификатов заканчивается.

4. *Кросс-сертификат.* Позволяет расширить действие конкретной PKI путем взаимоподписания корневых сертификатов двух разных PKI.

Существуют три *базовые модели сертификации*:

- иерархическая модель, основанная на иерархической цепи сертификатов;
- модель кросс-сертификации (подразумевает взаимную сертификацию);
- сетевая (гибридная) модель, включающая элементы иерархической и взаимной сертификации [9].

Обобщенные схемы иерархической и сетевой архитектуры систем управления сертификатами приведены на рис. 13.10.

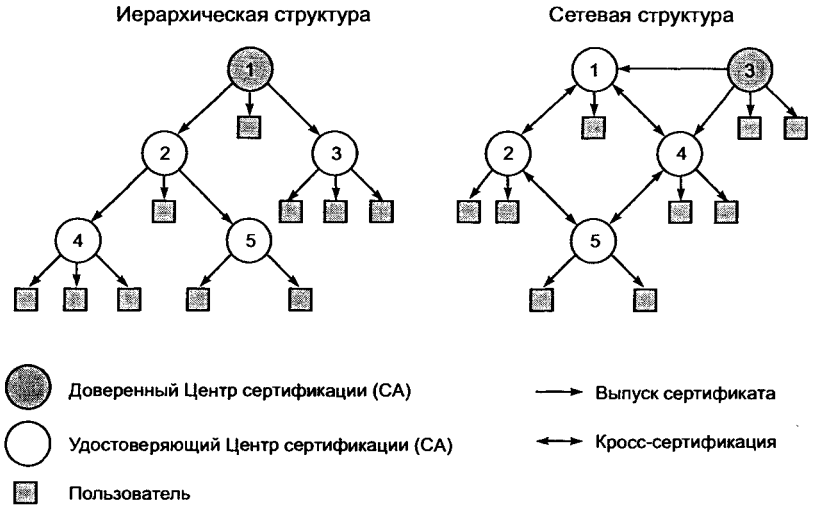


Рис. 13.10. Иерархическая и сетевая архитектуры систем управления сертификатами

В *иерархической модели* CA расположены в иерархическом подчинении доверенному (корневому) CA, предоставляющему сертификаты другим CA.

Достоинства иерархической архитектуры системы управления сертификатами:

- аналогична существующим федеральным и ведомственным организационно-управляющим структурам и может строиться с учетом этого;
- определяет простой алгоритм поиска, построения и верификации цепочек сертификатов для всех взаимодействующих сторон;
- для обеспечения взаимодействия двух пользователей одному из них достаточно предоставить другому свою цепочку сертификатов, что уменьшает проблемы, связанные с их взаимодействием.

Недостаток иерархической архитектуры: для обеспечения взаимодействия всех конечных пользователей должен быть только один корневой доверенный СА.

В *модели кросс-сертификации* независимые СА, не находящиеся на одной ветви иерархии, взаимно сертифицируют друг друга в сети СА. Кросс-сертификация является предметом двустороннего соглашения между СА. Следует отметить, что модель кросс-сертификации является частным случаем *сетевой архитектуры* системы управления сертификатами.

Достоинства сетевой архитектуры системы управления сертификатами:

- гибкость, что способствует установлению непосредственных доверенных взаимоотношений, существующих в современном бизнесе;
- отношения доверия в системе: конечный пользователь должен доверять, по крайней мере, только центру, издавшему его сертификат;
- возможность непосредственной кросс-сертификации различных удостоверяющих СА, пользователи которых часто взаимодействуют между собой, что сокращает процесс верификации цепочек.

Недостатки сетевой архитектуры управления сертификатами:

- сложность алгоритма поиска и построения цепочек сертификатов для всех взаимодействующих сторон;
- невозможность предоставления пользователем цепочки, которая обеспечивает проверку его сертификата всеми остальными пользователями.

Вероятно, в недалеком будущем на самом высоком уровне иерархии сертификации должен оказаться государственный нотариус, который обеспечит связь цепочек доверия разных организаций.

13.5.2. Логическая структура и компоненты PKI

Инфраструктура открытых ключей PKI (Public Key Infrastructure) — это набор агентов и правил, предназначенных для управления ключами, политикой безопасности и собственно обменом защищенными сообщениями [9, 50].

Основные задачи PKI:

- поддержка жизненного цикла цифровых ключей и сертификатов (т. е. генерация ключей, создание и подпись сертификатов, их распределение и пр.);
- регистрация фактов компрометации и публикация «черных» списков отозванных сертификатов;
- поддержка процессов идентификации и аутентификации пользователей таким образом, чтобы сократить, по возможности, время допуска каждого пользователя в систему;
- реализация механизма интеграции (основанного на PKI) существующих приложений и всех компонентов подсистемы безопасности;
- предоставление возможности использования единственного «токена» безопасности, единообразного для всех пользователей и приложений, содержащего все необходимые ключевые компоненты и сертификаты.

Токен безопасности — это индивидуальное средство безопасности, определяющее все права и окружение пользователя в системе, например смарт-карта.

Приложение, требующее систему управления ключами, должно взаимодействовать с системой PKI в ряде точек (передача сертификата на подпись, получение сертификата и «черного» списка при установлении взаимодействия и т. п.). Очевидно, что это взаимодействие с чуждой по отношению к данному приложению системой может осуществляться только при условии полной поддержки международных стандартов, которым удовлетворяет большинство современных PKI-систем (например, Baltimore, Entrust, Verisign).

Для предоставления удаленного доступа мобильным пользователям центр управления должен допускать подключение компьютеров, IP-адрес которых ему заранее неизвестен. Участники информационного обмена опознаются по их криптографическим сертификатам. Так как криптографический сертификат пользователя является электронным паспортом, он, как и любой паспорт, должен соответствовать определенным стандартам. В криптографии это стандарт X.509.

На рис. 13.11 приведена логическая структура и основные компоненты инфраструктуры управления открытыми ключами PKI.

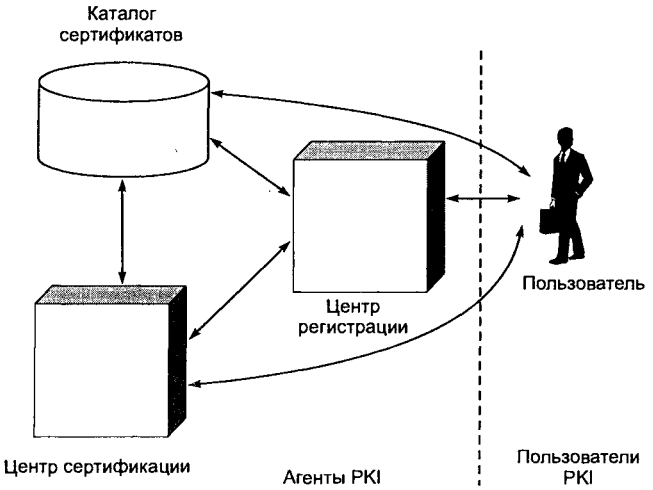


Рис. 13.11. Структура PKI

Компоненты этой структуры имеют следующее назначение.

Каталог сертификатов — общедоступное хранилище сертификатов пользователей. Доступ к сертификатам производится обычно по стандартизованному протоколу доступа к каталогам LDAP (Lightweight Directory Access Protocol).

Центр регистрации RA (Registration Authority) — организационная единица, назначение которой — регистрация пользователей системы.

Пользователь — владелец какого-либо сертификата (такой пользователь подлежит регистрации) или любой пользователь, запрашивающий сертификат, хранящийся в каталоге сертификатов.

Центр сертификации CA (Certification Authority) — организационная единица, назначение которой — сертификация открытых ключей пользователей (здесь из открытого ключа получается сертификат формата X.509) и их опубликование в каталоге сертификатов.

Общая схема работы CA выглядит следующим образом:

- CA генерирует собственные ключи и формирует сертификаты CA, предназначенные для проверки сертификатов пользователей;
- пользователи формируют запросы на сертификацию и доставляют их CA тем или иным способом;
- CA на основе запросов пользователей формирует сертификаты пользователей;
- CA формирует и периодически обновляет списки отмененных сертификатов CRL (Certificate Revocation List);
- сертификаты пользователей, сертификаты CA и списки отмены CRL публикуются CA (рассылаются пользователям либо помещаются в общедоступный справочник).

Инфраструктуру открытых ключей PKI поддерживает ряд ОС, приложений и стандартов.

В свою очередь инфраструктура открытых ключей PKI может интегрировать перечисленные функциональные области. В результате можно создавать комплексную систему информационной безопасности путем интеграции инфраструктуры открытых ключей в ИС компании и использования единых стандартов и сертификатов открытых ключей.

Часть 4
ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Еще несколько лет назад можно было надежно обеспечить безопасность ИС, используя такие традиционные средства защиты как идентификация и аутентификация, разграничение доступа, шифрование и т. п. Однако с появлением и развитием открытых компьютерных сетей ситуация резко изменилась. Количество уязвимостей сетевых ОС, прикладных программ и возможных атак на КИС постоянно растет. Системы анализа защищенности и системы обнаружения компьютерных атак являются важными элементами системы безопасности сетей любого современного предприятия.

Сегодня уже никого не надо убеждать в необходимости построения антивирусной защиты любой достаточно ответственной ИС. По оценкам западных аналитиков, ежегодный общемировой ущерб от вторжений вирусов, сетевых червей, троянских коней и прочих вредоносных программ составляет миллиарды долларов. Ежедневно в мире появляются от 2 до 10 новых вирусов. В условиях, когда компьютерные системы становятся основой бизнеса, а БД главным капиталом многих компаний, антивирусная защита прочно встает рядом с вопросами информационной и экономической безопасности организации.

Эффективность защиты КИС зависит от принятия правильных решений, которые поддерживают защиту, адаптирующуюся к изменяющимся условиям сетевого окружения. Решение проблем безопасности КИС требует применения адаптивного механизма, работающего в реальном режиме времени и обладающего высокой чувствительностью к изменениям в информационной инфраструктуре.

Глава 14
АНАЛИЗ ЗАЩИЩЕННОСТИ И ОБНАРУЖЕНИЕ АТАК

Ряд ведущих зарубежных организаций, занимающихся сетевой безопасностью, разработали подходы, позволяющие не только распознавать существующие уязвимости и атаки, но и выявлять изменившиеся старые или появившиеся новые уязвимости и противопоставлять им соответствующие средства защиты. В частности, компания ISS (Internet Security Systems) уточнила и развила эти подходы и разработала *Модель адаптивного управления безопасностью ANS* (*Adaptive Network Security*). Эти подходы развиваются и некоторыми другими компаниями, известными на рынке средств информационной безопасности. В России работами по адаптивному управлению безопасностью занимается НИП «Информзащита».

14.1. Концепция адаптивного управления безопасностью

Атакой на КИС считается любое действие, выполняемое нарушителем для реализации угрозы путем использования уязвимостей КИС. Под *уязвимостью* КИС понимается любая характеристика или элемент КИС, использование которых нарушителем может привести к реализации угрозы.

Архитектура КИС включает в себя четыре уровня.

1. Уровень прикладного программного обеспечения (ПО), отвечающий за взаимодействие с пользователем. Примером элементов ИС, работающих на этом уровне, можно назвать текстовый редактор WinWord, редактор электронных таблиц Excel, почтовую программу Outlook и т. д.

2. Уровень системы управления базами данных (СУБД), отвечающий за хранение и обработку данных ИС. Примером элементов ИС, работающих на этом уровне, можно назвать СУБД Oracle, MS SQL Server, Sybase и MS Access.

3. Уровень операционной системы (ОС), отвечающий за обслуживание СУБД и прикладного ПО. Примером элементов ИС, работающих на этом уровне, можно назвать ОС Microsoft Windows NT/2000/XP, Sun Solaris, Novell Netware.

4. Уровень сети, отвечающий за взаимодействие узлов ИС. Примером элементов ИС, работающих на этом уровне, можно назвать стеки протоколов TCP/IP, IPS/SPX и SMB/NetBIOS.

Злоумышленник располагает широким спектром возможностей для нарушения безопасности КИС. Эти возможности могут быть реализованы на всех четырех перечисленных выше уровнях КИС. Например, для получения НСД к финансовой информации в СУБД MS SQL Server злоумышленник может реализовать одну из следующих возможностей:

- перехватить передаваемые по сети данные (уровень сети);
- прочитать файлы БД, обращаясь непосредственно к файловой системе (уровень ОС);
- прочитать нужные данные средствами самой СУБД (уровень СУБД);
- прочитать записи БД при помощи SQL-запросов через программу MS Query, которая позволяет получать доступ к записям СУБД (уровень прикладного ПО).

При построении большинства традиционных компьютерных средств защиты использовались классические модели разграничения доступа, разработанные еще в 1970—80-е гг. Недостаточная эффективность таких традиционных механизмов защиты, как разграничение доступа, аутентификация, фильтрация и другие, обусловлена тем, что при их создании не учтены многие аспекты, связанные с современными атаками.

Рассмотрим этапы осуществления атаки на КИС (рис. 14.1) [40].

Первый, подготовительный, этап заключается в поиске злоумышленником предпосылок для осуществления той или иной атаки. На этом этапе злоумышленник ищет уязвимости в систе-

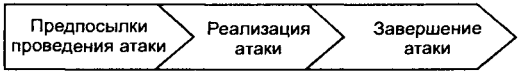


Рис. 14.1. Этапы осуществления атаки

ме. На втором, основном этапе — реализации атаки — осуществляется использование найденных уязвимостей. На третьем, заключительном, этапе злоумышленник завершает атаку и старается скрыть следы вторжения. В принципе первый и третий этапы сами по себе могут являться атаками. Например, поиск злоумышленником уязвимостей при помощи сканеров безопасности сам по себе считается атакой.

Следует отметить, что существующие механизмы защиты, реализованные в МЭ, серверах аутентификации, системах разграничения доступа, работают только на этапе реализации атаки. По существу эти механизмы защищают от атак, которые находятся уже в процессе осуществления. Более эффективным было бы упреждение атак, т. е. предотвращение самих предпосылок реализации вторжения. Комплексная система обеспечения информационной безопасности должна эффективно работать на всех трех этапах осуществления атаки.

В организациях часто не учитывается тот факт, что администраторы и пользователи регулярно изменяют конфигурацию ИС. В результате этих изменений могут появляться новые уязвимости, связанные с ОС и приложениями. Кроме того, очень быстро изменяются информационные и сетевые технологии, регулярно появляется новое ПО. Непрерывное развитие сетевых технологий при отсутствии постоянно проводимого анализа их безопасности и нехватке ресурсов для обеспечения защиты приводит к тому, что с течением времени защищенность КИС падает, так как появляются новые неучтенные угрозы и уязвимости системы.

В большинстве случаев для решения возникающих проблем с защитой в организациях используются частичные подходы. Эти подходы обычно обусловлены прежде всего текущим уровнем доступных ресурсов. Кроме того, администраторы безопасности имеют тенденцию реагировать только на те риски безопасности, которые им понятны. Фактически таких рисков может быть существенно больше. Только строгий текущий контроль защищенности КИС и комплексный подход, обеспечивающий единую политику безопасности, позволяют существенно снизить риски безопасности.

Адаптивный подход к безопасности позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, используя правильно спроектированные и хорошо управляемые процессы и средства.

Адаптивная безопасность сети состоит из трех основных элементов [40]:

- технологии анализа защищенности (security assessment);
- технологии обнаружения атак (intrusion detection);
- технологии управления рисками (risk management).

Оценка риска состоит в выявлении и ранжировании уязвимостей (по степени серьезности ущерба потенциальных воздействий), подсистем сети (по степени критичности), угроз (исходя из вероятности их реализации) и т. д. Поскольку конфигурация сети постоянно изменяется, то и процесс оценки риска должен проводиться постоянно. С оценки рисков должно начинаться построение системы защиты КИС.

Анализ защищенности — это поиск уязвимых мест в сети. Сеть состоит из соединений, узлов, хостов, рабочих станций, приложений и БД. Все они нуждаются как в оценке эффективности их защиты, так и в поиске неизвестных уязвимостей в них. Технологии анализа защищенности исследуют сеть и ищут «слабые» места в ней, обобщают эти сведения и печатают по ним отчет. Если система, реализующая эту технологию, содержит и адаптивный компонент, то устранение найденной уязвимости будет осуществляться не вручную, а автоматически. Технология анализа защищенности является действенным методом, позволяющим реализовать политику сетевой безопасности прежде, чем осуществится попытка ее нарушения снаружи или изнутри организации.

Перечислим некоторые из проблем, идентифицируемых технологией анализа защищенности:

- «люки» в системах (back door) и программы типа «троянский конь»;
- слабые пароли;
- восприимчивость к проникновению из незащищенных систем и атакам типа «отказ в обслуживании»;
- отсутствие необходимых обновлений (patch, hotfix) ОС;
- неправильная настройка МЭ, Web-серверов и БД;
- и многие другие.

Обнаружение атак является процессом оценки подозрительных действий, которые происходят в корпоративной сети. Обнаружение атак реализуется посредством анализа или журналов регистрации ОС и приложения или сетевого трафика в реальном времени. Компоненты обнаружения атак, размещенные на узлах или сегментах сети, оценивают различные события и дей-

ствия, в том числе и действия, использующие известные уязвимости (рис. 14.2).

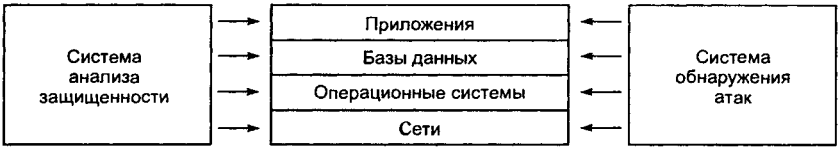


Рис. 14.2. Взаимодействие систем анализа защищенности и обнаружения атак

Адаптивный компонент модели адаптивного управления безопасностью (ANS) отвечает за модификацию процесса анализа защищенности, предоставляя ему самую последнюю информацию о новых уязвимостях. Он также модифицирует компонент обнаружения атак, дополняя его последней информацией об атаках. В качестве примера адаптивного компонента можно указать механизм обновления БД антивирусных программ для обнаружения новых вирусов. Управляющий компонент должен быть способен к генерации отчетов и анализу тенденций, связанных с формированием системы защиты организации.

Адаптация данных может заключаться в различных формах реагирования, которые могут включать:

- отправление уведомлений системам сетевого управления по протоколу SNMP, по электронной почте или на пейджер администратору;
- автоматическое завершение сессии с атакующим узлом или пользователем, реконфигурация МЭ или иных сетевых устройств (например, маршрутизаторов);
- выработка рекомендаций администратору, позволяющих своевременно устранить обнаруженные уязвимости в сетях, приложениях или иных компонентах ИС организации [40].

Использование модели адаптивной безопасности сети (рис. 14.3) позволяет контролировать практически все угрозы и своевременно реагировать на них высокоэффективным способом, позволяющим не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к появлению уязвимостей.

Модель адаптивной безопасности сети позволяет также уменьшить злоупотребления в сети, повысить осведомленность пользователей, администраторов и руководства компании о событиях безопасности в сети. Следует отметить, что эта модель не

Рис. 14.3. Модель адаптивной безопасности

отбрасывает уже используемые механизмы защиты (разграничение доступа, аутентификация и т. д.). Она расширяет их функциональность за счет новых технологий.

Для того чтобы привести свою систему обеспечения информационной безопасности в соответствие современным требованиям, организациям необходимо дополнить имеющиеся решения компонентами, отвечающими за анализ защищенности, обнаружение атак и управление рисками.

14.2. Технология анализа защищенности

В организации, использующей КИС, приходится регулярно проверять, насколько реализованные или используемые механизмы защиты информации соответствует положениям принятой в организации политики безопасности. Такая задача периодически возникает при изменении и обновлении компонентов ИС, изменении конфигурации ОС и т. п. [9, 40].

Однако администраторы сетей не имеют достаточно времени на проведение такого рода проверок для всех узлов корпоративной сети. Поэтому специалисты отделов защиты информации нуждаются в средствах, облегчающих анализ защищенности используемых механизмов обеспечения информационной безопасности. Этот процесс помогают автоматизировать средства анализа защищенности, часто называемые *сканерами безопасности* (*security scanners*).

Использование средств анализа защищенности позволяет определить уязвимости на узлах корпоративной сети и устранить их до того, как ими воспользуются злоумышленники. По существу, действия системы анализа защищенности аналогичны действиям охранника, периодически обходящего все этажи охраняемого здания в поисках открытых дверей, незакрытых окон и других проблем. Только в качестве здания выступает корпоративная сеть, а в качестве незакрытых окон и дверей — уязвимости.

Средства анализа защищенности работают на первом этапе осуществления атаки. Обнаруживая и своевременно устраняя уязвимости, они тем самым предотвращают саму возможность реализации атаки, что позволяет снизить затраты на эксплуатацию средств защиты.

Средства анализа защищенности могут функционировать на сетевом уровне, уровне ОС и уровне приложения. Они могут проводить поиск уязвимостей, постепенно наращивая число проверок и «углубляясь» в ИС, исследуя все ее уровни.

Наибольшее распространение получили средства анализа защищенности сетевых сервисов и протоколов. Обусловлено это, в первую очередь, универсальностью используемых протоколов. Изученность и повсеместное использование таких протоколов, как IP, TCP, HTTP, FTP, SMTP и т. п., позволяют с высокой степенью эффективности проверять защищенность ИС, работающей в сетевом окружении.

Вторыми по распространенности являются средства анализа защищенности ОС. Обусловлено это также универсальностью и распространенностью некоторых ОС (например, UNIX и Windows NT).

Средства анализа защищенности приложений пока существуют только для широко распространенных прикладных систем типа Web-браузеры и СУБД.

Применение средств анализа защищенности позволяет быстро определить все узлы корпоративной сети, доступные в момент проведения тестирования, выявить все используемые в сети сервисы и протоколы, их настройки и возможности для несанкционированного воздействия (как изнутри корпоративной сети, так и снаружи). По результатам сканирования эти средства вырабатывают рекомендации и пошаговые меры, позволяющие устранить выявленные недостатки.

Данный метод контроля нарушений политики безопасности не может заменить специалиста по информационной безопасности. Средства анализа защищенности могут лишь автоматизировать поиск некоторых известных уязвимостей.

14.2.1. Средства анализа защищенности сетевых протоколов и сервисов

Взаимодействие абонентов в любой сети базируется на использовании сетевых протоколов и сервисов, определяющих процедуру обмена информацией между двумя и более узлами. При разработке сетевых протоколов и сервисов к ним предъявлялись требования (обычно явно недостаточные) по обеспечению безопасности обрабатываемой информации. Поэтому постоянно появляются сообщения об обнаруженных в сетевых протоколах уязвимостях. В результате возникает потребность в постоянной проверке всех используемых в корпоративной сети протоколов и сервисов.

Системы анализа защищенности выполняют серию тестов по обнаружению уязвимостей. Эти тесты аналогичны применяемым злоумышленниками при осуществлении атак на корпоративные сети.

Сканирование с целью обнаружения уязвимостей начинается с получения предварительной информации о проверяемой системе. Заканчивается сканирование попытками имитации проникновения, используя широко известные атаки, например подбор пароля методом полного перебора (brute force — «грубая сила»).

При помощи средств анализа защищенности на уровне сети можно тестировать не только возможность НСД в корпоративную сеть из сети Internet. Эти средства могут быть использованы как для оценки уровня безопасности организации, так и для контроля эффективности настройки сетевого программного и аппаратного обеспечения.

В настоящее время известно более десятка различных средств, автоматизирующих поиск уязвимостей сетевых протоколов и сервисов. Среди коммерческих систем анализа защищенности можно назвать Internet Scanner компании Internet Security Systems, Inc., NetSonar компании Cisco, CyberCop Scanner компании Network Associates и ряд других.

Типичная схема проведения анализа защищенности (на примере системы Internet Scanner) приведена на рис. 14.4.

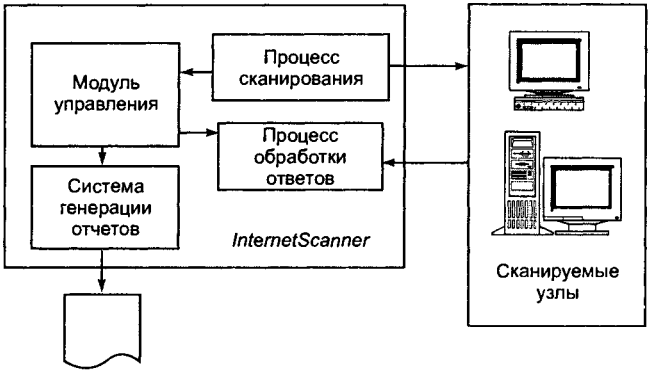


Рис. 14.4. Схема проведения анализа защищенности (на примере системы Internet Scanner)

Средства анализа защищенности данного класса анализируют не только уязвимость сетевых сервисов и протоколов, но и системного и прикладного ПО, отвечающего за работу с сетью. К такому обеспечению можно отнести Web-, FTP- и почтовые серверы, МЭ, браузеры и т. п.

14.2.2. Средства анализа защищенности ОС

Средства этого класса предназначены для проверки настроек ОС, влияющих на ее защищенность. К таким настройкам можно отнести:

- учетные записи пользователей (account), например длину пароля и срок его действия;
- права пользователей на доступ к критичным системным файлам;
- уязвимые системные файлы;
- установленные патчи (patch) и т. п.

Системы анализа защищенности на уровне ОС могут быть использованы также для контроля конфигурации ОС.

В отличие от средств анализа защищенности сетевого уровня данные системы проводят сканирование не снаружи, а изнутри анализируемой системы, т. е. они не имитируют атаки

внешних злоумышленников. Кроме возможностей по обнаружению уязвимостей, некоторые системы анализа защищенности на уровне ОС (например, System Scanner компании Internet Security Systems) позволяют автоматически устранять часть обнаруженных проблем или корректировать параметры системы, не удовлетворяющие политике безопасности, принятой в организации.

14.3. Технологии обнаружения атак

Сетевые и информационные технологии меняются настолько быстро, что статичные защитные механизмы, к которым относятся системы разграничения доступа, МЭ, системы аутентификации во многих случаях не могут обеспечить эффективной защиты. Поэтому требуются динамические методы, позволяющие оперативно обнаруживать и предотвращать нарушения безопасности. Одной из технологий, позволяющей обнаруживать нарушения, которые не могут быть идентифицированы при помощи традиционных моделей контроля доступа, является технология обнаружения атак.

По существу, процесс обнаружения атак является процессом оценки подозрительных действий, которые происходят в корпоративной сети. Иначе говоря, *обнаружение атак* (intrusion detection) — это процесс идентификации и реагирования на подозрительную деятельность, направленную на вычислительные или сетевые ресурсы.

14.3.1. Методы анализа сетевой информации

Эффективность системы обнаружения атак во многом зависит от применяемых методов анализа полученной информации. В первых системах обнаружения атак, разработанных в начале 1980-х гг., использовались статистические методы обнаружения атак. В настоящее время к статистическому анализу добавился ряд новых методик, начиная с экспертных систем и нечеткой логики и заканчивая использованием нейронных сетей [9, 40].

Статистический метод. Основные преимущества статистического подхода — использование уже разработанного и зареко-

мендовавшего себя аппарата математической статистики и адаптация к поведению субъекта.

Сначала для всех субъектов анализируемой системы определяются профили. Любое отклонение используемого профиля от эталонного считается несанкционированной деятельностью. Статистические методы универсальны, поскольку для проведения анализа не требуется знания о возможных атаках и используемых ими уязвимостях. Однако при использовании этих методик возникают и проблемы:

- «статистические» системы не чувствительны к порядку следования событий; в некоторых случаях одни и те же события в зависимости от порядка их следования могут характеризовать аномальную или нормальную деятельность;
- трудно задать граничные (пороговые) значения отслеживаемых системой обнаружения атак характеристик, чтобы адекватно идентифицировать аномальную деятельность;
- «статистические» системы могут быть с течением времени «обучены» нарушителями так, чтобы атакующие действия рассматривались как нормальные.

Следует также учитывать, что статистические методы не применимы в тех случаях, когда для пользователя отсутствует шаблон типичного поведения или когда для пользователя типичны несанкционированные действия.

Экспертные системы состоят из набора правил, которые охватывают знания человека-эксперта. Использование экспертных систем представляет собой распространенный метод обнаружения атак, при котором информация об атаках формулируется в виде правил. Эти правила могут быть записаны, например, в виде последовательности действий или в виде сигнатуры. При выполнении любого из этих правил принимается решение о наличии несанкционированной деятельности. Важным достоинством такого подхода является практически полное отсутствие ложных тревог.

БД экспертной системы должна содержать сценарии большинства известных на сегодняшний день атак. Для того чтобы оставаться постоянно актуальными, экспертные системы требуют постоянного обновления БД. Хотя экспертные системы предлагают хорошую возможность для просмотра данных в журналах регистрации, требуемые обновления могут либо игнорироваться, либо выполняться администратором вручную. Как минимум, это приводит к экспертной системе с ослабленными возможностя-

ми. В худшем случае отсутствие надлежащего сопровождения снижает степень защищенности всей сети, вводя ее пользователей в заблуждение относительно действительного уровня защищенности.

Основным недостатком является невозможность отражения неизвестных атак. При этом даже небольшое изменение уже известной атаки может стать серьезным препятствием для функционирования системы обнаружения атак.

Нейронные сети. Большинство современных методов обнаружения атак используют некоторую форму анализа контролируемого пространства на основе правил или статистического подхода. В качестве контролируемого пространства могут выступать журналы регистрации или сетевой трафик. Анализ опирается на набор заранее определенных правил, которые создаются администратором или самой системой обнаружения атак.

Любое разделение атаки во времени или среди нескольких злоумышленников является трудным для обнаружения при помощи экспертных систем. Из-за большого разнообразия атак и хакеров даже специальные постоянные обновления БД правил экспертной системы никогда не дадут гарантии точной идентификации всего диапазона атак.

Использование нейронных сетей является одним из способов преодоления указанных проблем экспертных систем. В отличие от экспертных систем, которые могут дать пользователю определенный ответ о соответствии рассматриваемых характеристик заложенным в БД правилам, нейронная сеть проводит анализ информации и предоставляет возможность оценить, согласуются ли данные с характеристиками, которые она научена распознавать. В то время как степень соответствия нейросетевого представления может достигать 100 %, достоверность выбора полностью зависит от качества системы в анализе примеров поставленной задачи.

Сначала нейросеть обучают правильной идентификации на предварительно подобранной выборке примеров предметной области. Реакция нейросети анализируется и система настраивается таким образом, чтобы достичь удовлетворительных результатов. В дополнение к начальному периоду обучения, нейросеть набирается опыта с течением времени, по мере того, как она проводит анализ данных, связанных с предметной областью.

Важным преимуществом нейронных сетей при обнаружении злоупотреблений является их способность «изучать» характери-

стики умышленных атак и идентифицировать элементы, которые не похожи на те, что наблюдались в сети прежде.

Каждый из описанных методов обладает рядом достоинств и недостатков, поэтому сейчас практически трудно встретить систему, реализующую только один из описанных методов. Как правило, эти методы используются в совокупности.

14.3.2. Классификация систем обнаружения атак IDS

Механизмы, применяемые в современных системах обнаружения атак IDS (Intrusion Detection System), основаны на нескольких общих методах, которые не являются взаимоисключающими. Во многих системах используются их комбинации.

Классификация IDS может быть выполнена:

- по способу реагирования;
- способу выявления атаки;
- способу сбора информации об атаке.

По способу реагирования различают пассивные и активные IDS. *Пассивные* IDS просто фиксируют факт атаки, записывают данные в файл журнала и выдают предупреждения. *Активные* IDS пытаются противодействовать атаке, например, путем реконфигурации МЭ или генерации списков доступа маршрутизатора.

По способу выявления атаки системы IDS принято делить на две категории:

- обнаружение аномального поведения (anomaly-based);
- обнаружение злоупотреблений (misuse detection или signature-based).

Технология *обнаружения аномального поведения* основана на следующем. Аномальное поведение пользователя (т. е. атака или какое-нибудь враждебное действие) часто проявляется как отклонение от нормального поведения. Примером аномального поведения может служить большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора и т. п.

Если можно было бы однозначно описать профиль нормального поведения пользователя, то любое отклонение от него можно идентифицировать как аномальное поведение. Однако аномальное поведение не всегда является атакой. Например, одно-

временную посылку большого числа запросов от администратора сети система обнаружения атак может идентифицировать как атаку типа «отказ в обслуживании» («denial of service»).

При использовании системы с такой технологией возможны два случая:

- обнаружение аномального поведения, которое не является атакой, и отнесение его к классу атак;
- пропуск атаки, которая не подпадает под определение аномального поведения. Этот случай более опасен, чем ложное отнесение аномального поведения к классу атак.

Технология обнаружения аномалий ориентирована на выявление новых типов атак. Однако недостаток ее — необходимость постоянного обучения. Пока эта технология не получила широкого распространения. Связано это с тем, что она трудно реализуема на практике.

Обнаружение злоупотреблений заключается в описании атаки в виде сигнатуры (signature) и поиска данной сигнатуры в контролируемом пространстве (сетевом трафике или журнале регистрации). В качестве сигнатуры атаки может выступать шаблон действий или строка символов, характеризующие аномальную деятельность. Эти сигнатуры хранятся в БД, аналогичной той, которая используется в антивирусных системах. Данная технология обнаружения атак очень похожа на технологию обнаружения вирусов, при этом система может обнаружить все известные атаки. Однако системы данного типа не могут обнаруживать новые, еще неизвестные виды атак.

Подход, реализованный в таких системах, достаточно прост и именно на нем основаны практически все предлагаемые сегодня на рынке системы обнаружения атак.

Наиболее популярна классификация **по способу сбора информации об атаке**:

- обнаружение атак на уровне сети (network-based);
- обнаружение атак на уровне хоста (host-based);
- обнаружение атак на уровне приложения (application-based).

Система *network-based* работает по типу сниффера, «прослушивая» трафик в сети и определяя возможные действия злоумышленников. Такие системы анализируют сетевой трафик, используя, как правило, сигнатуры атак и анализ «на лету». Метод анализа «на лету» заключается в мониторинге сетевого трафика в реальном или близком к реальному времени и использовании соответствующих алгоритмов обнаружения.

Системы *host-based* предназначены для мониторинга, детектирования и реагирования на действия злоумышленников на определенном хосте. Располагаясь на защищаемом хосте, они проверяют и выявляют направленные против него действия. Эти системы анализируют регистрационные журналы ОС или приложения.

Как правило, анализ журналов регистрации является дополнением к другим методам обнаружения атак, в частности к обнаружению атак «на лету». Использование этого метода позволяет проводить «разбор полетов» уже после того, как была зафиксирована атака, для того чтобы выработать эффективные меры предотвращения аналогичных атак в будущем.

Система *application-based* основана на поиске проблем в определенном приложении.

Каждый из этих типов систем обнаружения атак (на уровне сети, на уровне хоста и на уровне приложения) имеет свои достоинства и недостатки. Гибридные IDS, представляющие собой комбинацию различных типов систем, как правило, включают в себя возможности нескольких категорий.

14.3.3. Компоненты и архитектура IDS

На основе анализа существующих решений можно привести перечень компонентов, из которых состоит типичная система обнаружения атак [40].

Модуль слежения обеспечивает сбор данных из контролируемого пространства (журнала регистрации или сетевого трафика). Разные производители дают этому модулю следующие названия: *сенсор* (sensor), *монитор* (monitor), *зонд* (probe) и т. д.

В зависимости от архитектуры построения системы обнаружения атак модуль слежения может быть физически отделен от других компонентов, т. е. находиться на другом компьютере.

Подсистема обнаружения атак — основной модуль системы обнаружения атак. Она осуществляет анализ информации, получаемой от модуля слежения. По результатам этого анализа данная подсистема может идентифицировать атаки, принимать решения относительно вариантов реагирования, сохранять сведения об атаке в хранилище данных и т. д.

База знаний в зависимости от методов, используемых в системе обнаружения атак, может содержать профили пользователей и

вычислительной системы, сигнатуры атак или подозрительные строки, характеризующие несанкционированную деятельность. База знаний может пополняться производителем системы обнаружения атак, пользователем системы или третьей стороной, например аутсорсинговой компанией, осуществляющей поддержку этой системы.

Хранилище данных обеспечивает хранение данных, собранных в процессе функционирования системы обнаружения атак.

Графический интерфейс. Даже очень мощное и эффективное средство не будет использоваться, если у него отсутствует дружественный интерфейс. В зависимости от ОС, под управлением которой функционирует система обнаружения атак, графический интерфейс должен соответствовать стандартам де-факто для Windows и Unix.

Подсистема реагирования осуществляет реагирование на обнаруженные атаки и иные контролируемые события. Варианты реагирования будут описаны более подробно ниже.

Подсистема управления компонентами предназначена для управления различными компонентами системы обнаружения атак. Под термином «управление» понимается возможность изменения политики безопасности для различных компонентов системы обнаружения атак (например, модулей слежения), а также получение информации от этих компонентов (например, сведения о зарегистрированной атаке). Управление может осуществляться как при помощи внутренних протоколов и интерфейсов, так и при помощи уже разработанных стандартов, например SNMP.

Системы обнаружения атак строятся на основе двух архитектур: «автономный агент» и «агент—менеджер». В первом случае на каждый защищаемый узел или сегмент сети устанавливаются агенты системы, которые не могут обмениваться информацией между собой, а также не могут управляться централизовано с единой консоли. Этих недостатков лишена архитектура «агент—менеджер». В этом случае в *распределенной системе обнаружения атак dIDS* (distributed IDS), состоящей из множества IDS, расположенных в различных участках большой сети, серверы сбора данных и центральный анализирующий сервер осуществляют централизованный сбор и анализ регистрируемых данных. Управление модулями dIDS осуществляется с центральной консоли управления [39]. Для крупных организаций, в которых филиалы

разнесены по разным территориям и даже городам, использование такой архитектуры имеет принципиальное значение.

Общая схема функционирования dIDS приведена на рис. 14.5.

Такая система позволяет усилить защищенность корпоративной подсети благодаря централизации информации об атаке от различных IDS. Распределенная система обнаружения атак dIDS состоит из следующих подсистем: консоли управления, анализирующих серверов, агентов сети, серверов сбора информации об атаке. Центральный анализирующий сервер обычно состоит из БД и Web-сервера, что позволяет сохранять информацию об атаках и манипулировать данными с помощью удобного Web-интерфейса. Агент сети — один из наиболее важных компонентов dIDS. Он представляет собой небольшую программу, цель которой — сообщать об атаке на центральный анализирующий сервер. Сервер сбора информации об атаке — часть системы dIDS, логически базирующаяся на центральном анализирующем сервере. Сервер определяет параметры, по которым группируются

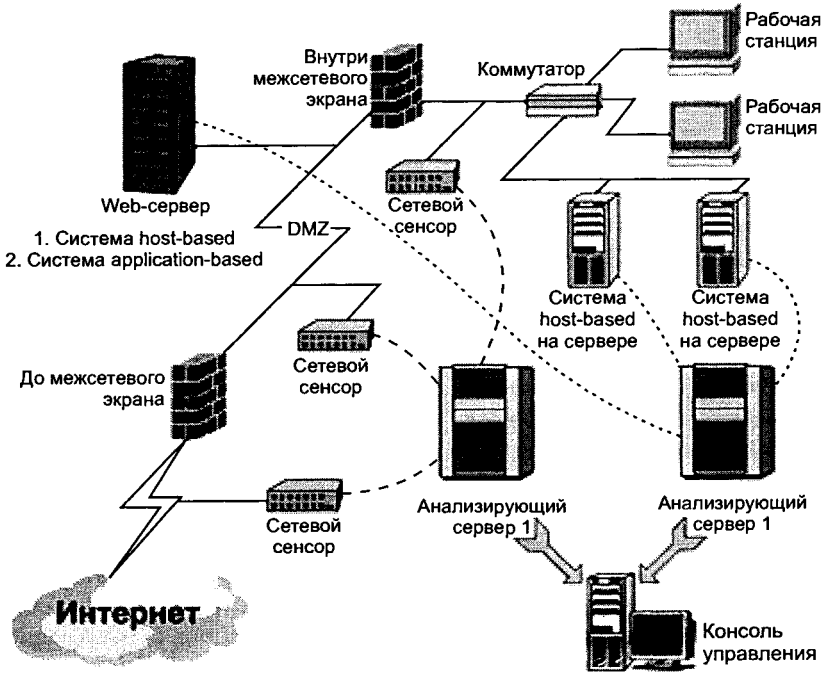


Рис. 14.5. Общая схема функционирования распределенной dIDS

данные, полученные от агентов сети. Группировка данных может осуществляться по следующим параметрам:

- IP-адресу атакующего;
- порту получателя;
- номеру агента;
- дате, времени;
- протоколу;
- типу атаки и т. д.

14.3.4. Методы реагирования

Атака не только должна быть обнаружена, но и необходимо правильно и своевременно среагировать на нее. В существующих системах применяется широкий спектр методов реагирования, которые можно разделить на три категории [9, 40]:

- уведомление;
- сохранение;
- активное реагирование.

Применение той или иной реакции зависит от многих факторов.

Уведомление. Самым простым и широко распространенным методом уведомления является отправление администратору безопасности сообщений об атаке на консоль системы обнаружения атак. Такая консоль может быть установлена не у каждого сотрудника, отвечающего в организации за безопасность, кроме того, этих сотрудников могут интересовать не все события безопасности, поэтому необходимо применение иных механизмов уведомления. Этими механизмами могут быть отправление сообщений по электронной почте, на пейджер, по факсу или по телефону.

К категории «уведомление» относится также посылка управляющих последовательностей к другим системам, например к системам сетевого управления или к МЭ.

Сохранение. К категории «сохранение» относятся два варианта реагирования:

- регистрация события в БД;
- воспроизведение атаки в реальном масштабе времени.

Первый вариант широко распространен и в других системах защиты. Для реализации второго варианта бывает необходимо «пропустить» атакующего в сеть компании и зафиксировать все его действия. Это позволяет администратору безопасности затем

воспроизводить в реальном масштабе времени (или с заданной скоростью) все действия, осуществленные атакующим, анализировать «успешные» атаки и предотвращать их в дальнейшем, а также использовать собранные данные в процессе разбирательства.

Активное реагирование. К этой категории относятся следующие варианты реагирования:

- блокировка работы атакующего;
- завершение сессии с атакующим узлом;
- управлением сетевым оборудованием и средствами защиты.

IDS могут предложить такие конкретные варианты реагирования: блокировка учетной записи атакующего пользователя, автоматическое завершение сессии с атакующим узлом, реконфигурация МЭ и маршрутизаторов и т. д. Эта категория механизмов реагирования, с одной стороны, достаточно эффективна, а с другой стороны, требует аккуратного использования, так как неправильное применение может привести к нарушению работоспособности всей КИС.

Глава 15
ЗАЩИТА ОТ ВИРУСОВ

Компьютерный вирус — это своеобразное явление, возникшее в процессе развития компьютерной техники и ИТ. Суть его состоит в том, что программы-вирусы обладают свойствами, присущими живым организмам, — они рождаются, размножаются и умирают. Термин «компьютерный вирус» впервые употребил сотрудник Университета Южной Калифорнии Фред Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. Этим термином был назван вредоносный фрагмент программного кода. Конечно, это была всего лишь метафора. Фрагмент программного кода похож на настоящий вирус не больше, чем человек на робота. Однако это один из тех редких случаев, когда значение метафоры становилось со временем менее метафорическим и более буквальным.

Компьютерные вирусы способны делать практически то же, что и настоящие вирусы: переходить с одного объекта на другой, изменять способы атаки и мутировать. Проникнув в ИС, компьютерный вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае ИС, пораженная вирусом, окажется под полным контролем злоумышленника. Сегодня компьютерам доверяют решение многих критических задач. Поэтому выход из строя ИС может иметь весьма тяжелые последствия, вплоть до человеческих жертв.

15.1. Компьютерные вирусы и проблемы антивирусной защиты

Существует много определений компьютерного вируса. Исторически первое определение было дано в 1984 г. Фредом Коэном: «Компьютерный вирус — это программа, которая может заражать

другие программы, модифицируя их посредством включения в них своей, возможно измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Ключевыми понятиями в этом определении являются *способность вируса к саморазмножению* и *способность к модификации вычислительного процесса*. Указанные свойства компьютерного вируса аналогичны паразитированию биологического вируса в живой природе. С тех пор острота проблемы вирусов многократно возросла — к концу XX в. в мире насчитывалось более 14 300 модификаций вирусов.

В настоящее время под компьютерным вирусом принято понимать программный код, обладающий следующими свойствами:

- способностью к созданию собственных копий, не обязательно совпадающих с оригиналом, но обладающих свойствами оригинала (самовоспроизведение);
- наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

Следует отметить, что эти свойства являются необходимыми, но не достаточными. Указанные свойства следует дополнить свойствами деструктивности и скрытности действий данной вредоносной программы в вычислительной среде.

15.1.1. Классификация компьютерных вирусов

На сегодняшний день известны десятки тысяч различных компьютерных вирусов. Несмотря на такое изобилие, число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, достаточно ограничено. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Вирусы можно разделить на классы [38, 85]:

- по среде обитания;
- операционной системе (ОС);
- особенностям алгоритма работы;
- деструктивным возможностям.

Основной и наиболее распространенной классификацией компьютерных вирусов является классификация *по среде обитания*, или *по типам объектов* компьютерной системы, в которые

внедряются вирусы (рис. 15.1). По среде обитания компьютерные вирусы можно разделить:

- на файловые;
- загрузочные;
- макровирусы;
- сетевые.

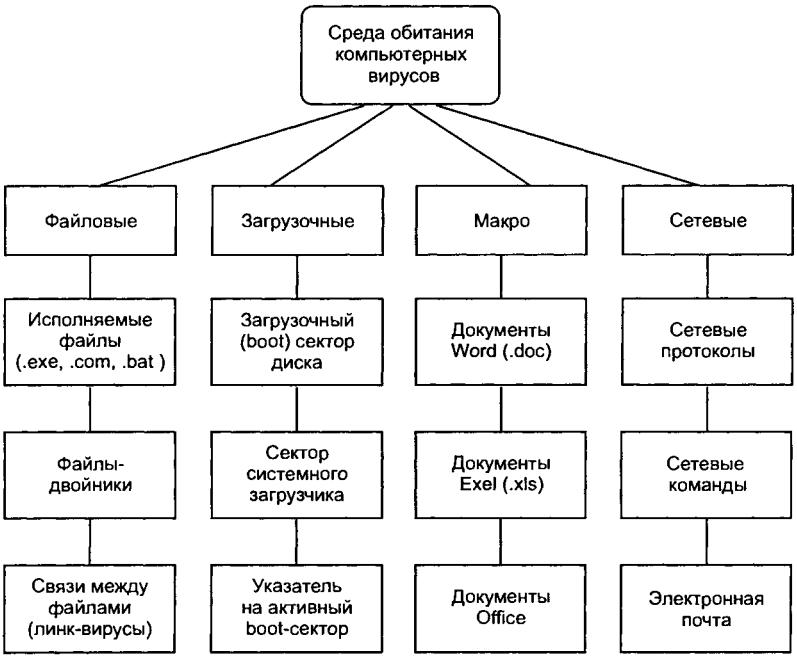


Рис. 15.1. Классификация компьютерных вирусов по среде обитания

Файловые вирусы либо внедряются в выполняемые файлы (наиболее распространенный тип вирусов) различными способами, либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record). Загрузочные вирусы замещают код программы, получающей управление при загрузке системы. В результате при перезагрузке управление передается вирусу. При этом оригинальный boot-сектор обычно переносит-

ся в какой-либо другой сектор диска. Иногда загрузочные вирусы называют *бутовыми вирусами*.

Макровирусы заражают макропрограммы и файлы документов современных систем обработки информации, в частности файлы-документы и электронные таблицы популярных редакторов Microsoft Word, Microsoft Excel и др. Для размножения макровирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла в другие. Вирусы этого типа получают управление при открытии зараженного файла и инфицируют файлы, к которым впоследствии идет обращение из соответствующего офисного приложения.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Иногда сетевые вирусы называют программами типа «червь». Сетевые черви подразделяются на Internet-черви (распространяются по Internet), LAN-черви (распространяются по локальной сети), IRC-черви Internet Relay Chat (распространяются через чаты). Существуют также смешанные типы, которые совмещают в себе сразу несколько технологий.

Существуют много комбинированных типов компьютерных вирусов, например, известен сетевой макро-вирус, который заражает редактируемые документы, а также рассылает свои копии по электронной почте. В качестве другого примера вирусов комбинированного типа можно указать файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков. Такие вирусы имеют усложненный алгоритм работы и применяют своеобразные методы проникновения в систему.

Другим признаком деления компьютерных вирусов на классы является *операционная система*, объекты которой подвергаются заражению. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких ОС — DOS, Windows 95/98, Windows NT/2000 и т. д. Макро-вирусы заражают файлы форматов Word, Excel, Microsoft Office. На определенные форматы расположения системных данных в загрузочных секторах дисков также ориентированы загрузочные вирусы.

Естественно, эти схемы классификации не являются единственно возможными, существуют много различных схем типизации вирусов. Однако ограничимся пока классификацией компьютерных вирусов по среде обитания, поскольку она является базовой, и перейдем к рассмотрению общих принципов функционирования вирусов. Анализ основных этапов «жизненного

цикла» этих вредоносных программ позволяет выделить их различные признаки и особенности, которые могут быть положены в основу дополнительных классификаций.

15.1.2. Жизненный цикл вирусов

Как и у любой программы, у компьютерных вирусов можно выделить две основные стадии жизненного цикла — хранение и исполнение.

Стадия хранения соответствует периоду, когда вирус просто хранится на диске совместно с объектом, в который он внедрен. На этой стадии вирус является наиболее уязвимым со стороны антивирусного ПО, так как он не активен и не может контролировать работу ОС с целью самозащиты.

Некоторые вирусы на этой стадии используют механизмы защиты своего кода от обнаружения. Наиболее распространенным способом защиты является шифрование большей части тела вируса. Его использование совместно с механизмами мутации кода (об этом идет речь ниже) делает невозможным выделение сигнатур — устойчивых характеристических фрагментов кода вирусов.

Стадия исполнения компьютерных вирусов, как правило, включает пять этапов:

1) загрузка вируса в память;
2) поиск жертвы;
3) заражение найденной жертвы;
4) выполнение деструктивных функций;
5) передача управления программе-носителю вируса.

Рассмотрим эти этапы подробнее [38, 70].

1. Загрузка вируса. Загрузка вируса в память осуществляется ОС одновременно с загрузкой исполняемого объекта, в который вирус внедрен. Например, если пользователь запустил на исполнение программный файл, содержащий вирус, то, очевидно, вирусный код будет загружен в память как часть этого файла. В простейшем случае процесс загрузки вируса представляет собой не что иное, как копирование с диска в оперативную память, сопровождаемое иногда настройкой адресов, после чего происходит передача управления коду тела вируса. Эти действия выполняются ОС, а сам вирус находится в пассивном состоянии. В более сложных ситуациях вирус может после получения управления выполнять дополнительные действия, которые необ-

ходимы для его функционирования. В связи с этим рассматриваются два аспекта.

Первый аспект связан с максимальным усложнением процедуры обнаружения вирусов. Для обеспечения защиты на стадии хранения некоторые вирусы используют достаточно сложные алгоритмы. К таким усложнениям можно отнести шифрование основного тела вируса. Однако использование только шифрования является полумерой, так как в открытом виде должна храниться та часть вируса, которая обеспечивает расшифрование вируса на стадии загрузки. Для избежания подобной ситуации разработчики вирусов используют механизмы «мутаций» кода расшифровщика. Суть этого метода состоит в том, что при внедрении в объект копии вируса часть ее кода, относящаяся к расшифровщику, модифицируется так, чтобы возникли текстуальные различия с оригиналом, но результаты работы остались неизменными. Обычно применяют следующие приемы модификации кода:

- изменение порядка независимых инструкций;
- замену некоторых инструкций на эквивалентные по результату работы;
- замену используемых в инструкциях регистров на другие;
- введение случайным образом зашумляющих инструкций.

Вирусы, использующие подобные механизмы мутации кода, получили название *полиморфных вирусов*. При совместном использовании механизмов шифрования и мутации внедряемая копия вируса окажется отличной от оригинала, так как одна ее часть будет изменена, а другая окажется зашифрованной на ключе, сгенерированном специально для этой копии вируса. А это существенно осложняет выявление вируса в вычислительной системе.

Полиморфные вирусы (polymorphic) — это трудно обнаруживаемые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Полиморфизм встречается в вирусах всех типов — файловых, загрузочных и макровирусах.

Дополнительные действия, которые выполняют полиморфные вирусы на этапе загрузки, состоят в расшифровывании основного тела вируса.

При использовании стелс-алгоритмов вирусы могут полностью или частично скрыть себя в системе. Наиболее распростра-

ненный стелс-алгоритм осуществляет перехват системных запросов с целью контроля действий ОС. Вирусы, использующие стелс-алгоритмы, называются стелс-вирусами.

Стелс-вирусы (Stealth) способны скрывать свое присутствие в системе и избегать обнаружения антивирусными программами. Эти вирусы могут перехватывать запросы ОС на чтение/запись зараженных файлов, при этом они либо временно лечат эти файлы, либо «подставляют» вместо себя незараженные участки информации, эмулируя «чистоту» зараженных файлов.

В случае макровирусов наиболее популярным способом является запрет вызовов меню просмотра макросов. Одним из первых файловых стелс-вирусов был вирус «Frodo», первым загрузочным стелс-вирусом был вирус «Brain».

Нередко в вирусах используются различные нестандартные приемы с целью глубже спрятаться в ядре ОС, либо защитить от обнаружения свою резидентную копию, либо затруднить лечение от вируса и т. п.

Второй аспект связан с так называемыми *резидентными вирусами*. Поскольку вирус и объект, в который он внедрен, являются для ОС единым целым, то после загрузки они располагаются, естественно, в едином адресном пространстве. После завершения работы объекта он выгружается из оперативной памяти, при этом одновременно выгружается и вирус, переходя в пассивную стадию хранения. Однако некоторые типы вирусов способны сохраняться в памяти и оставаться активными после окончания работы вирусоносителя. Эти вирусы получили название резидентных.

Резидентные вирусы при инфицировании компьютера оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.

Резидентными можно считать макровирусы, так как для большинства из них выполняются основные требования — постоянное присутствие в памяти компьютера на все время работы зараженного редактора и перехват функций, используемых при работе с документами. При этом роль ОС берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.

Следует отметить, что деление вирусов на резидентные и нерезидентные справедливо в основном для файловых вирусов. Загрузочные вирусы, как и макровирусы, относятся к резидентным вирусам.

2. Поиск жертвы. По способу поиска жертвы вирусы можно разделить два два класса.

К **первому классу** относятся вирусы, осуществляющие «активный» поиск с использованием функций ОС. Примером являются файловые вирусы, использующие механизм поиска исполняемых файлов в текущем каталоге.

Второй класс составляют вирусы, реализующие «пассивный» механизм поиска, т. е. вирусы, расставляющие «ловушки» дпя программных файлов. Как правило, файловые вирусы устраивают такие ловушки путем перехвата функции *Exec* ОС, а макровирусы — с помощью перехвата команд типа *Save as* из меню *File*.

3. Заражение жертвы. В простейшем случае заражение представляет собой самокопирование кода вируса в выбранный в качестве жертвы объект. Классификация вирусов на этом этапе связана с анализом особенностей этого копирования и способов модификации заражаемых объектов.

Особенности заражения файловыми вирусами. По способу инфицирования жертвы вирусы можно разделить на два класса.

К **первому классу** относятся вирусы, которые не внедряют свой код непосредственно в программный файл, а изменяют имя файла и создают новый, содержащий тело вируса.

Второй класс составляют вирусы, внедряющиеся непосредственно в файлы-жертвы. Они характеризуются местом внедрения. Возможны следующие варианты.

Внедрение в начало файла. Этот способ является наиболее удобным для COM-файлов MS-DOS, так как данный формат не предусматривает наличие служебных заголовков. При внедрении этим способом вирусы могут либо производить конкатенацию собственного кода и кода программы-жертвы, либо переписывать начальный фрагмент файла в конец, освобождая место для себя.

Внедрение в конец файла. Это — наиболее распространенный тип внедрения. Передача управления коду вирусов обеспечивается модификацией первых команд программы (COM) или заголовка файла (EXE).

Внедрение в середину файла. Как правило, этот способ используется вирусами применительно к файлам с заранее известной структурой (например, к файлу COMMAND.COM) или же к файлам, содержащим последовательность байтов с одинаковыми значениями, длина которой достаточна для размещения вируса. Во втором случае вирусы архивируют найденную последовательность и замещают собственным кодом. Помимо этого вирусы могут внедряться в середину файла, освобождая себе место путем переноса фрагментов кода программы в конец файла или же «раздвигая» файл.

Особенности заражения загрузочными вирусами определяются особенностями объектов, в которые они внедряются, — загрузочными секторами гибких и жестких дисков и главной загрузочной записью (MBR) жестких дисков. Основной проблемой является ограниченный размер этих объектов. В связи с этим вирусам необходимо сохранить на диске ту свою часть, которая не уместилась на месте жертвы, а также перенести оригинальный код инфицированного загрузчика. Существуют различные способы решения этой задачи. Ниже приводится классификация, предложенная Е. Касперским [38, 85].

Используются псевдосбойные секторы. Вирус переносит необходимый код в свободные секторы диска и помечает их как сбойные, защищая тем самым себя и загрузчик от перезаписи.

Используются редко применяемые секторы в конце раздела. Вирус переносит необходимый код в эти свободные секторы в конце диска. С точки зрения ОС эти секторы выглядят как свободные.

Используются зарезервированные области разделов. Вирус переносит необходимый код в области диска, зарезервированные под нужды ОС, а потому неиспользуемые.

Короткие вирусы могут уместиться в один сектор загрузчика и полностью взять на себя функции MBR или загрузочного сектора.

Особенности заражения макровирусами. Процесс заражения сводится к сохранению вирусного макрокода в выбранном документе-жертве. Для некоторых систем обработки информации это сделать не просто, так как формат файлов документов может не предусматривать возможность сохранения макропрограмм. В ка-

честве примера приведем Microsoft Word 6.0. Сохранение макрокода для этой системы возможно только в файлах шаблонов (имеющих по умолчанию расширение .DOT). Поэтому для своего сохранения вирус должен контролировать обработку команды *Save as* из меню *File*, которая вызывается всякий раз, когда происходит первое сохранение документа на диск. Этот контроль необходим, чтобы в момент сохранения изменить тип файла-документа (имеющего по умолчанию расширение .DOC) на тип файла-шаблона. В этом случае на диске окажутся и макрокод вируса, и содержимое документа.

Помимо простого копирования кода вируса в заражаемый объект на этом этапе могут использоваться более сложные алгоритмы, обеспечивающие защиту вируса на стадии хранения. К числу таких вирусов относятся описанные выше полиморфные вирусы.

4. Выполнение деструктивных функций. Вирусы могут выполнять помимо самокопирования деструктивные функции.

По деструктивным возможностям вирусы можно разделить на безвредные, неопасные, опасные и очень опасные [85].

Безвредные вирусы — это вирусы, в которых реализован только механизм самораспространения. Они не наносят вред системе, за исключением расхода свободной памяти на диске в результате своего распространения.

Неопасные вирусы — это вирусы, присутствие которых в системе связано с различными эффектами (звуковыми, видео) и уменьшением свободной памяти на диске, но которые не наносят вред программам и данным.

Опасные вирусы — это вирусы, которые могут привести к серьезным сбоям в работе компьютера. Последствием сбоя может стать разрушение программ и данных.

Очень опасные вирусы — это вирусы, в алгоритм работы которых заведомо заложены процедуры, непосредственно приводящие к разрушениям программ и данных, а также к стиранию информации, записанной в системных областях памяти и необходимой для работы компьютера.

На «степень опасности» вирусов оказывает существенное влияние та среда, под управлением которой вирусы работают.

Так, вирусы, созданные для работы в MS-D0S, обладают практически неограниченными потенциальными возможностями.

Распространение вирусов под управлением Windows NT/2000 ограничивается развитой системой разграничения доступа.

Возможности макровирусов напрямую определяются возможностями макроязыков, на которых они написаны. В частности, язык Word Basic позволяет создать мощные макровирусы, способные доставить пользователям серьезные неприятности.

Дополняя эту классификацию, можно отметить также деление вирусов на вирусы, наносящие вред системе вообще, и вирусы, предназначенные для целенаправленных атак на определенные объекты.

5. Передача управления программе-носителю вируса. Здесь следует указать на деление вирусов на разрушающие и неразрушающие.

Разрушающие вирусы не заботятся о сохранении работоспособности инфицированных программ, поэтому для них этот этап функционирования отсутствует.

Для *неразрушающих вирусов* этот этап связан с восстановлением в памяти программы в том виде, в котором она должна корректно исполняться, и передачей управления программе-носителю вируса.

Вредоносные программы других типов

Кроме вирусов принято выделять еще несколько видов вредоносных программ. Это троянские программы, логические бомбы, хакерские утилиты скрытого администрирования удаленных компьютеров, программы, ворующие пароли доступа к ресурсам Интернет и прочую конфиденциальную информацию. Четкого разделения между ними не существует: троянские программы могут содержать вирусы, в вирусы могут быть встроены логические бомбы и т. д.

Троянские программы не размножаются и не рассылаются сами. Внешне они выглядят совершенно безобидно и даже предлагают полезные функции. Но когда пользователь загрузит такую программу в свой компьютер и запустит ее, она может незаметно выполнять вредоносные функции. Чаще всего троянские программы используются для первоначального распространения вирусов, для получения удаленного доступа к компьютеру через Интернет, кражи данных или их уничтожения.

Логической бомбой называется программа или ее отдельные модули, которые при определенных условиях выполняют вредо-

носные действия. Логическая бомба может, например, сработать по достижении определенной даты или тогда, когда в БД появится или исчезнет запись, и т. п. Такая бомба может быть встроена в вирусы, троянские программы и даже в обычные программы.

15.1.3. Основные каналы распространения вирусов и других вредоносных программ

Для того чтобы создать эффективную систему антивирусной защиты компьютеров и корпоративных сетей, необходимо четко представлять себе, откуда грозит опасность. Вирусы находят самые разные каналы распространения, причем к старым способам постоянно добавляются новые.

Классические способы распространения

Файловые вирусы распространяются вместе с файлами программ в результате обмена дискетами и программами, загрузки программ из сетевых каталогов, с Web- или ftp-серверов. *Загрузочные вирусы* попадают на компьютер, когда пользователь забывает зараженную дискету в дисководе, а затем перезагружает ОС. Загрузочный вирус также может быть занесен на компьютер вирусами других типов. *Макрокомандные вирусы* распространяются в результате обмена зараженными файлами офисных документов, такими как файлы Microsoft Word, Excel, Access.

Если зараженный компьютер подключен к локальной сети, вирус легко может оказаться на дисках файл-сервера, а оттуда через каталоги, доступные для записи, попасть на все остальные компьютеры сети. Так начинается вирусная эпидемия. Системному администратору следует помнить, что вирус имеет в сети такие же права, что и пользователь, на компьютер которого этот вирус пробрался. Поэтому он может попасть во все сетевые каталоги, доступные пользователю. Если же вирус завелся на рабочей станции администратора сети, последствия могут быть очень тяжелыми.

Электронная почта

В настоящее время глобальная сеть Internet является основным источником вирусов. Большое число заражений вирусами происходит при обмене письмами по электронной почте в фор-

матах Microsoft Word. Электронная почта служит каналом распространения макрокомандных вирусов, так как вместе с сообщениями часто отправляются офисные документы.

Заражения вирусами могут осуществляться как непреднамеренно, так и по злому умыслу. Например, пользователь зараженного макровирусом редактора, сам того не подозревая, может рассылать зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т. д. С другой стороны, злоумышленник может преднамеренно послать по электронной почте вместе с вложенным файлом исполняемый модуль вирусной или троянской программы, вредоносный программный сценарий Visual Basic Script, зараженную или троянскую программу сохранения экрана монитора, словом — любой опасный программный код.

Распространители вирусов часто пользуются для маскировки тем фактом, что диалоговая оболочка Microsoft Windows по умолчанию не отображает расширения зарегистрированных файлов. Например, файл с именем FreeCreditCard.txt.exe, будет показан пользователю как FreeCreditCard.txt. Если пользователь попытается открыть такой файл, будет запущена вредоносная программа.

Сообщения электронной почты часто приходят в виде документов HTML, которые могут включать ссылки на элементы управления ActiveX, апплеты Java и другие активные компоненты. Из-за ошибок в почтовых клиентах злоумышленники могут воспользоваться такими активными компонентами для внедрения вирусов и троянских программ на компьютеры пользователей. При получении сообщения в формате HTML почтовый клиент показывает его содержимое в своем окне. Если сообщение содержит вредоносные активные компоненты, они сразу же запускаются и выполняют заложенные в них функции. Чаще всего таким способом распространяются троянские программы и черви.

Троянские Web-сайты

Пользователи могут «получить» вирус или троянскую программу во время простого серфинга сайтов Интернета, посетив троянский Web-сайт. Ошибки в браузерах пользователей зачастую приводят к тому, что активные компоненты троянских Web-сайтов (элементы управления ActiveX или апплеты Java) внедряют на

компьютеры пользователей вредоносные программы. Здесь используется тот же самый механизм, что и при получении сообщений электронной почты в формате HTML. Но заражение происходит незаметно: активные компоненты Web-страниц могут внешне никак себя не проявлять. Приглашение посетить троянский сайт пользователь может получить в обычном электронном письме.

Локальные сети

Локальные сети также представляют собой путь быстрого заражения. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в локальную сеть заражает один или несколько служебных файлов на сервере. В качестве таких файлов могут выступать служебный файл LOGIN.COM, Excel-таблицы и стандартные документы-шаблоны, применяемые в фирме. Пользователи при входе в эту сеть запускают зараженные файлы с сервера, и в результате вирус получает доступ на компьютеры пользователей.

Другие каналы распространения вредоносных программ

Одним из серьезных каналов распространения вирусов являются пиратские копии ПО. Часто нелегальные копии на дискетах и CD-дисках содержат файлы, зараженные разнообразными типами вирусов. К источникам распространения вирусов следует также отнести электронные конференции и файл-серверы ftp и BBS. Часто авторы вирусов закладывают зараженные файлы сразу на несколько файл-серверов ftp/BBS или рассылают одновременно по нескольким электронным конференциям, причем зараженные файлы обычно маскируют под новые версии программных продуктов и даже антивирусов. Компьютеры, установленные в учебных заведениях и Интернет-центрах и работающие в режиме общего пользования, также могут легко оказаться источниками распространения вирусов. Если один из таких компьютеров оказался зараженным вирусом с дискеты очередного пользователя, тогда дискеты и всех остальных пользователей, работающих на этом компьютере, окажутся зараженными.

По мере развития компьютерных технологий совершенствуются и компьютерные вирусы, приспосабливаясь к новым для себя сферам обитания. В любой момент может появиться компьютерный вирус, троянская программа или «червь» нового, неиз-

вестного ранее типа, либо известного типа, но нацеленного на новое компьютерное оборудование. Новые вирусы могут использовать неизвестные или не существовавшие ранее каналы распространения, а также новые технологии внедрения в компьютерные системы. Чтобы исключить угрозу вирусного заражения, системный администратор корпоративной сети должен внедрять методики антивирусной защиты и постоянно отслеживать новости в мире компьютерных вирусов.

15.2. Антивирусные программы и комплексы

Для защиты от компьютерных вирусов могут использоваться:

- общие методы и средства защиты информации;
- специализированные программы для защиты от вирусов;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусами.

Общие средства защиты информации полезны не только для защиты от вирусов. Они используются также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя. Существуют две основные разновидности этих средств:

- средства копирования информации (применяются для создания копий файлов и системных областей дисков);
- средства разграничения доступа (предотвращают несанкционированное использование информации, в частности обеспечивают защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей).

При заражении компьютера вирусом важно его обнаружить. К внешним признакам проявления деятельности вирусов можно отнести следующие:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- изменение даты и времени модификации файлов;
- исчезновение файлов и каталогов или искажение их содержимого;
- частые зависания и сбои в работе компьютера;
- медленная работа компьютера;
- невозможность загрузки ОС;

- существенное уменьшение размера свободной оперативной памяти;
- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске.

Однако следует заметить, что перечисленные выше явления необязательно вызываются действиями вируса, они могут быть следствием и других причин. Поэтому правильная диагностика состояния компьютера всегда затруднена и обычно требует привлечения специализированных программ.

Антивирусные программы

Для обнаружения и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать компьютерные вирусы. Такие программы называются *антивирусными*. Практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов. Антивирусные программы используют различные методы обнаружения вирусов.

Методы обнаружения вирусов

К основным методам обнаружения компьютерных вирусов можно отнести следующие:

- метод сравнения с эталоном;
- эвристический анализ;
- антивирусный мониторинг;
- метод обнаружения изменений;
- встраивание антивирусов в BIOS компьютера и др. [85].

Метод сравнения с эталоном. Самый простой метод обнаружения заключается в том, что для поиска известных вирусов используются так называемые *маски*. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Антивирусная программа последовательно просматривает (сканирует) проверяемые файлы в поиске масок известных вирусов. Антивирусные сканеры способны найти только уже известные вирусы, для которых определена маска.

Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Применение простых сканеров не защищает компьютер от проникновения новых вирусов. Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить маску, поэтому антивирусные сканеры их не обнаруживают.

Эвристический анализ. Для того чтобы размножаться, компьютерный вирус должен совершать какие-то конкретные действия: копирование в память, запись в секторы и т. д. Эвристический анализатор (который является частью антивирусного ядра) содержит список таких действий и проверяет программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов. Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполнимый файл программы. Обнаружив зараженный файл, анализатор обычно выводит сообщение на экране монитора и делает запись в собственном или системном журнале. В зависимости от настроек, антивирус может также направлять сообщение об обнаруженном вирусе администратору сети. Эвристический анализ позволяет обнаруживать неизвестные ранее вирусы. Первый эвристический анализатор появился в начале 1990-х гг. Практически все современные антивирусные программы реализуют собственные методы эвристического анализа. В качестве примера такой программы можно указать сканер McAffee VirusScan.

Антивирусный мониторинг. Суть данного метода состоит в том, что в памяти компьютера постоянно находится антивирусная программа, осуществляющая мониторинг всех подозрительных действий, выполняемых другими программами. Антивирусный мониторинг позволяет проверять все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты либо компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие. Пример такой программы — сторож Spider Guard, который входит в комплект сканера Doctor Web и выполняет функции антивирусного монитора.

Метод обнаружения изменений. При реализации этого метода антивирусные программы, называемые *ревизорами* диска, запо-

минают предварительно характеристики всех областей диска, которые могут подвергнуться нападению, а затем периодически проверяют их. Заражая компьютер, вирус изменяет содержимое жесткого диска: например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл AUTOEXEC.BAT, изменяет загрузочный сектор, создает файл-спутник. При сопоставлении значений характеристик областей диска антивирусная программа может обнаружить изменения, сделанные как известным, так и неизвестным вирусом.

Встраивание антивирусов в BIOS компьютера. В системные платы компьютеров встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо программа пытается изменить содержимое загрузочных секторов, срабатывает защита, и пользователь получает соответствующее предупреждение. Однако эта защита не очень надежна. Известны вирусы, которые пытаются отключить антивирусный контроль BIOS, изменяя некоторые ячейки в энергонезависимой памяти (CMOS-памяти) компьютера.

Виды антивирусных программ

Различают следующие виды антивирусных программ [85]:
- программы-фаги (сканеры);
- программы-ревизоры (CRC-сканеры);
- программы-блокировщики;
- программы-иммунизаторы.

Программы-фаги (сканеры) используют для обнаружения вирусов метод сравнения с эталоном, метод эвристического анализа и некоторые другие методы. Программы-фаги осуществляют поиск характерной для конкретного вируса маски путем сканирования в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Программы-фаги не только находят зараженные вирусами файлы, но и «лечат» их, т. е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале работы программы-фаги сканируют оперативную память, обнаруживают вирусы и уничтожают их и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги — программы-фаги, предназначенные для поиска и уничтожения большого числа вирусов.

Программы-фаги можно разделить на две категории — универсальные и специализированные сканеры. *Универсальные сканеры* рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от ОС, на работу в которой рассчитан сканер. *Специализированные сканеры* предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов. Специализированные сканеры, рассчитанные только на макровирусы, оказываются более удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Программы-фаги делятся также на *резидентные мониторы*, производящие сканирование «на лету», и *нерезидентные сканеры*, обеспечивающие проверку системы только по запросу. Резидентные мониторы обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как нерезидентный сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам программ-фагов всех типов относится их универсальность. К недостаткам следует отнести относительно небольшую скорость поиска вирусов и относительно большие размеры антивирусных баз.

Наиболее известные программы-фаги: Aidstest, Scan, Norton AntiVirus, Doctor Web. Учитывая, что постоянно появляются новые вирусы, программы-фаги быстро устаревают, и требуется регулярное обновление версий.

Программы-ревизоры (CRC-сканеры) используют для поиска вирусов метод обнаружения изменений. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (кодов циклического контроля) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) затем сохраняются в БД антивируса. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в БД, с реально подсчитанными значениями. Если информация о файле, записанная в БД, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. Как правило, сравнение состояний производят сразу после загрузки ОС.

CRC-сканеры, использующие алгоритмы анти-стелс, являются довольно мощным средством против вирусов: практически 100 % вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у CRC-сканеров имеется

недостаток, заметно снижающий их эффективность: они не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их БД отсутствует информация об этих файлах.

К числу CRC-сканеров относится широко распространенная в России программа ADinf (Advanced Diskinfoscope) и ревизор AVP Inspector. Вместе с ADinf применяется лечащий модуль ADinf Cure Module (ADinfExt), который использует собранную ранее информацию о файлах для их восстановления после поражения неизвестными вирусами. В состав ревизора AVP Inspector также входит лечащий модуль, способный удалять вирусы.

Программы-блокировщики реализуют метод антивирусного мониторинга. Антивирусные блокировщики — это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом пользователю. К «вирусо-опасным» ситуациям относятся вызовы, которые характерны для вирусов в моменты их размножения (вызовы на открытие для записи в выполняемые файлы, запись в загрузочные секторы дисков или MBR винчестера, попытки программ остаться резидентно и т. п.).

При попытке какой-либо программы произвести указанные действия блокировщик посылает пользователю сообщение и предлагает запретить соответствующее действие. К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что бывает особенно полезно в случаях, когда регулярно появляется давно известный вирус. Однако они не «лечат» файлы и диски. Для уничтожения вирусов требуется применять другие программы, например фаги. К недостаткам блокировщиков можно отнести существование путей обхода их защиты и их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла).

Следует отметить, что созданы антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера. Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера.

Программы-иммунизаторы — это программы, предотвращающие заражение файлов. Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммуниза-

торы, блокирующие заражение каким-либо типом вируса. Иммунизаторы первого типа обычно записываются в конец файлов и при запуске файла каждый раз проверяют его на изменение. У таких иммунизаторов имеется один серьезный недостаток — они не могут обнаружить заражение стелс-вирусом. Поэтому этот тип иммунизаторов практически не используются в настоящее время.

Иммунизатор второго типа защищает систему от поражения вирусом определенного вида. Он модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, вирус при этом воспринимает их зараженными и поэтому не внедряется. Такой тип иммунизации не может быть универсальным, поскольку нельзя иммунизировать файлы от всех известных вирусов. Однако в качестве полумеры подобные иммунизаторы могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

Критерии качества антивирусной программы

Качество антивирусной программы можно оценить по нескольким критериям [85]:

- надежность и удобство работы — отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки;
- качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц (MS Word, Excel, Office), упакованных и архивированных файлов; возможность лечения зараженных объектов;
- существование версий антивируса под все популярные платформы (DOS, Windows NT, Novell NetWare, OS/2, Alpha, Linux и т. д.); наличие режимов сканирования «по запросу» и «на лету», существование серверных версий с возможностью администрирования сети;
- скорость работы и другие полезные особенности.

Надежность работы антивируса является наиболее важным критерием, поскольку даже «абсолютный» антивирус может оказаться бесполезным, если он не в состоянии довести процесс сканирования до конца, т. е. «повиснет» и не проверит часть

дисков и файлов и, в результате, вирус останется незамеченным в системе.

Качество обнаружения вирусов стоит на следующем месте по вполне естественной причине. Главная обязанность антивирусных программ — обнаруживать 100 % вирусов и лечить их. При этом антивирусная программа не должна иметь высокий уровень ложных срабатываний.

Следующий по важности критерий — многоплатформенность антивируса, поскольку только программа, рассчитанная на конкретную ОС, может полностью использовать функции этой системы. Моментальная и принудительная проверка приходящих на компьютер файлов и вставляемых дискет — это практически 100%-я гарантия от заражения вирусом. Если в серверном варианте антивируса присутствует возможность антивирусного администрирования сети, то его ценность еще более возрастает.

Скорость работы также является важным критерием качества антивирусной программы. В разных антивирусах используются различные алгоритмы поиска вирусов, один алгоритм может оказаться более быстрым и качественным, другой — медленным и менее качественным.

Профилактические меры защиты

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры. Абсолютно надежных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Важным методом борьбы с компьютерными вирусами является своевременная профилактика. Чтобы существенно уменьшить вероятность заражения вирусом и обеспечить надежное хранение информации на дисках, необходимо выполнять следующие меры профилактики:

- применять только лицензионное ПО;
- оснастить компьютер современными антивирусными программами и постоянно возобновлять их версии;
- всегда проверять дискеты на наличие вирусов (запуская антивирусные программы своего компьютера) перед считыванием с них информации, записанной на других компьютерах;

- при переносе на свой компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;
- периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив ОС с защищенной от записи системной дискеты;
- всегда защищать свои дискеты от записи при работе на других компьютерах, если на них не будет производиться запись информации;
- обязательно делать на дискетах архивные копии ценной для пользователя информации;
- не оставлять в кармане дисковода А дискеты при включении или перезагрузке ОС, чтобы исключить заражение компьютера загрузочными вирусами;
- использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей.

Антивирусные программные комплексы

У каждого типа антивирусных программ есть свои достоинства и недостатки. Только комплексное использование нескольких типов антивирусных программ может привести к приемлемому результату. Программные средства защиты представляют собой комплекс алгоритмов и программ, нацеленных на контроль и исключение проникновения несанкционированной информации.

Существует спектр программных комплексов, предназначенных для профилактики заражения вирусом, обнаружения и уничтожения вирусов [9]. Они обладают универсальностью, гибкостью, адаптивностью и др.

Перечислим наиболее распространенные антивирусные программные комплексы:

- антивирус Касперского (AVP) Personal;
- антивирус Dr.Web;
- антивирус Symantec Antivirus;
- антивирус McAfee;
- антивирус AntiVir Personal Edition.

15.3. Построение системы антивирусной защиты корпоративной сети

Проблема антивирусной защиты — одна из приоритетных проблем безопасности корпоративных информационных ресурсов организации. Ее актуальность объясняется:

- лавинообразным ростом числа компьютерных вирусов;
- неудовлетворительным состоянием антивирусной защиты в существующих корпоративных компьютерных сетях. Сегодня сети компаний находятся в постоянном развитии. Однако вместе с ним постоянно растет и число точек проникновения вирусов в корпоративные сети Интернет/интранет. Как правило, такими точками являются: шлюзы и серверы Интернет, серверы файл-приложений, серверы групповой работы и электронной почты, рабочие станции.

Для небольших предприятий, использующих до 10 узлов, целесообразны решения по антивирусной защите, имеющие удобный графический интерфейс и допускающие локальное конфигурирование без применения централизованного управления. Для крупных предприятий предпочтительнее системы антивирусной защиты с несколькими консолями и менеджерами управления, подчиненными некоторому единому общему центру. Такие решения позволяют обеспечить оперативное централизованное управление локальными антивирусными клиентами и дают возможность при необходимости интегрироваться с другими решениями в области безопасности корпоративных сетей.

Часть 5
УПРАВЛЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ

Система информационной безопасности должна оградить информационные ресурсы сети от наиболее распространенных внешних и внутренних атак, направленных на вывод из строя серверов и уничтожение данных, от нежелательного проникновения в локальные вычислительные сети через «дыры» в ОС, от целенаправленного вторжения в систему для получения конфиденциальной информации.

Для успешного использования современных ИТ необходимо надежное и эффективное управление не только самими сетями, но и средствами сетевой безопасности. И если раньше задача заключалась в управлении отдельными серверами, сетями и маршрутизаторами, то сейчас требуется обеспечить информационную безопасность корпоративных бизнес-процессов. Все это предъявляет жесткие требования к управлению средствами сетевой безопасности.

Глава 16
МЕТОДЫ УПРАВЛЕНИЯ СРЕДСТВАМИ СЕТЕВОЙ БЕЗОПАСНОСТИ

Важнейшим компонентом системы управления корпоративной сетью является система информационной безопасности. Эта система должна:

- централизованно и оперативно осуществлять управляющие воздействия на средства сетевой безопасности;
- проводить регулярный аудит и мониторинг, дающие объективную информацию о состоянии информационной безопасности для принятия оперативных решений.

16.1. Задачи управления системой сетевой безопасности

Сформулируем основные задачи управления системой сетевой безопасности масштаба предприятия. Функционально система управления средствами защиты информации в распределенной сети масштаба предприятия должна решать следующие задачи:

- управление *глобальной политикой безопасности* (ГПБ) в рамках сети предприятия, формирование *локальных политик безопасности* (ЛПБ) отдельных устройств и доведения ЛПБ до всех устройств защиты информации;
- управление конфигурацией объектов и субъектов доступа; включает управление составом, версиями, компонентами устройств и ПО защиты, а также управление пэтчами (patch), которые служат для закрытия дыр, обнаруженных в поставленных продуктах обеспечения безопасности;

- предоставление сервисов защиты распределенным прикладным системам, а также регистрацию защищенных приложений и их ресурсов. Приложения этой группы должны обеспечивать, прежде всего, интерфейс (API) для обеспечения управления сервисами защиты со стороны прикладных систем;
- управление криптосредствами, в частности — ключевое управление (ключевая инфраструктура). Ключевая инфраструктура должна функционировать в составе инфраструктурных (системообразующих) служб;
- событийное протоколирование; включает настройку выдачи логов на разные устройства, управление уровнем детализации логов, управление составом событий, по которым ведется протоколирование;
- аудит безопасности ИС; обеспечивает получение и оценку объективных данных о текущем состоянии защищенности ИС, иногда под аудитом безопасности понимают анализ логов, поиск нарушителей и дыр в существующей системе, однако эти функции покрываются, скорее, задачами управления логами;
- мониторинг безопасности системы; обеспечивает получение информации в реальном времени о состоянии, активности устройств и о событиях с контекстом безопасности, происходящих в устройствах, например о потенциальных атаках;
- обеспечение работы специальных защищенных приложений, например нотариального надзора за операциями, поддержка регламентных мероприятий (смена ключей, паролей, устройств защиты, выпуск смарт-карт и др.);
- обеспечение работы проектно-инвентаризационной группы приложений; эта группа приложений должна осуществлять:
  - определение точек установки средств защиты в сети предприятия;
  - учет применяемых средств защиты;
  - контроль модульного состава средств защиты;
  - контроль состояния средств защиты и др.

Существует проблема комплексирования и организации взаимодействия традиционных систем управления сетями и систем управления средствами защиты информации в сети. Для решения этой проблемы применяются два основных подхода.

Первый подход заключается в интеграции средств сетевого или системного управления с механизмами управления средств

защиты. Средства сетевого и системного управления ориентированы, в первую очередь, на управление сетью или ИС, т. е. поддерживают традиционные действия и услуги: управление учетными записями пользователей, управление ресурсами и событиями, маршрутизацию, производительность и т. п. Ряд компаний — Cisco Systems, Computer Associates, Hewlett Packard, Tivoli Systems — пошли по пути интеграции механизмов управления средств защиты в традиционные системы управления сетями. Однако такие комплексные системы управления часто отличаются высокой стоимостью и, кроме того, некоторые аспекты управления безопасностью остаются за пределами внимания этих систем.

Второй подход заключается в использовании средств, предназначенных для решения только задачи управления безопасностью. Например, Open Security Manager (OSM) от Check Point Software Technologies дает возможность централизованно управлять корпоративной политикой безопасности и инсталлировать ее на сетевые устройства по всей компании. Продукт OSM является одним из основных компонентов технологии OPSEC (Open Platform for Secure Enterprise Connectivity), разработанной компанией CheckPoint, он создает интерфейс для управления устройствами сетевой безопасности различных производителей (например, Cisco, Bay, 3Com).

16.2. Архитектура управления средствами сетевой безопасности

Для обеспечения безопасности информационных ресурсов предприятия средства защиты информации обычно размещаются непосредственно в корпоративной сети. МЭ контролируют доступ к корпоративным ресурсам, отражая атаки злоумышленников извне, а шлюзы виртуальных частных сетей (VPN) обеспечивают конфиденциальную передачу информации через открытые глобальные сети, в частности Интернет. Для создания надежной эшелонированной защиты в настоящее время применяются также такие средства безопасности, как системы обнаружения вторжений IDS (Intrusion Detection Systems), средства контроля доступа по содержанию информации, антивирусные системы и др.

Большинство КИС построены на основе программных и аппаратных средств, поставляемых различными производителями.

Каждое из этих средств требует тщательного и специфического конфигурирования, отражающего взаимосвязи между пользователями и доступными им ресурсами. Чтобы обеспечить в гетерогенной КИС надежную защиту информации, нужна рационально организованная система управления безопасностью КИС, которая обеспечила бы безопасность и правильную настройку каждого компонента КИС, постоянно отслеживала происходящие изменения, устанавливала «заплатки» на найденные в системе бреши, контролировала работу пользователей. Очевидно, что чем разнороднее ИС, тем сложнее обеспечить управление ее безопасностью.

16.2.1. Основные понятия

Опыт ведущих предприятий-производителей средств сетевой безопасности показывает, что компания сможет успешно реализовать свою политику безопасности в распределенной КИС, если управление безопасностью будет централизованным и не будет зависеть от используемых ОС и прикладных систем. Кроме того, система регистрации событий, происходящих в КИС (события НСД, изменение привилегий пользователей и т. д.), должна быть единой, чтобы администратор смог составить полную картину происходящих в КИС изменений.

Для решения ряда задач управления безопасностью требуется применение единых вертикальных инфраструктур типа каталога X.500. Например, политика сетевого доступа требует знания идентификаторов пользователей. Эта информация нужна и другим приложениям, например в системе кадрового учета, в системе однократного доступа к приложениям (Single Sign-On) и т. д. Дублирование одних и тех же данных приводит к необходимости синхронизации, увеличению трудоемкости и возможной путанице. Поэтому, чтобы избежать такого дублирования, часто используют *единые вертикальные инфраструктуры.*

К таким вертикальным структурам, используемым различными пользовательскими подсистемами, работающими на разных уровнях OSI/ISO, относятся:

- *инфраструктуры управления открытыми ключами PKI.* Следует отметить интересный аспект, пока не получивший широкого распространения, но важный для управления. Сей-

час в основном используются цифровые сертификаты в виде так называемых «удостоверений личности» (identity certificates), но уже развиваются и кое-где применяются цифровые сертификаты в виде так называемых «верительных грамот» (credential certificates); выдавая и отзывая такие «верительные грамоты», можно более гибко управлять доступом;

- *каталоги* (например, идентификаторов пользователей и других сведений о пользователях, необходимых в системах управления доступом); примечательно, что каталоги часто используются не только как хранилища данных — в них также часто располагаются политики доступа, сертификаты, списки доступа и др.;
- *системы аутентификации* (обычно RADIUS, серверы TACACS, TACACS+);
- *системы событийного протоколирования, мониторинга и аудита*. Следует отметить, что эти системы не всегда вертикальны, часто специализируются и работают автономно в интересах конкретных подсистем.

Концепция глобального управления безопасностью, позволяющая построить эффективную систему иерархического управления безопасностью гетерогенной сети компании, разработана компанией TrustWorks Systems [9]. Организация централизованного управления безопасностью КИС основана на следующих принципах:

- управление безопасностью корпоративной сети должно осуществляться на уровне ГПБ — набора правил безопасности для множества взаимодействий между объектами корпоративной сети, а также между объектами корпоративной сети и внешними объектами;
- ГПБ должна соответствовать бизнес-процессам компании. Для этого свойства безопасности объектов и требуемые сервисы безопасности должны быть описаны с учетом их бизнес-ролей в структуре компании.
- для отдельных средств защиты формируются ЛПБ. Трансляция ЛПБ должна осуществляться автоматически на основе анализа правил ГПБ и топологии защищаемой сети.

Учитывая, что методология централизованного управления сетевой безопасностью достаточно полно отражает современные тенденции развития технологий безопасности, рассмотрим подробнее эту методологию и некоторые аспекты ее реализации.

16.2.2. Концепция глобального управления безопасностью

В основе централизованного управления безопасностью КИС лежит концепция *глобального управления безопасностью GSM* (Global Security Management). Концепция GSM позволяет построить комплексную систему управления и защиты информационных ресурсов предприятия со следующими свойствами:

- управление всеми существующими средствами защиты на базе политики безопасности предприятия, обеспечивающее целостность, непротиворечивость и полноту набора правил защиты для всех ресурсов предприятия (объектов политики безопасности) и согласованное исполнение политики безопасности средствами защиты, поставляемыми разными производителями;
- определение всех информационных ресурсов предприятия через единый (распределенный) каталог среды предприятия, который может актуализироваться как за счет собственных средств описания ресурсов, так и посредством связи с другими каталогами предприятия (в том числе по протоколу LDAP);
- централизованное, основанное на политике безопасности (policy-based) управление локальными средствами защиты информации;
- строгая аутентификация объектов политики в среде предприятия с использованием PKCS#11 токенов и инфраструктуры открытых ключей PKI, включая возможность применения дополнительных локальных средств аутентификации LAS (по выбору потребителя);
- расширенные возможности администрирования доступа к определенным в каталоге ресурсам предприятия или частям всего каталога (с поддержкой понятий групп пользователей, доменов, департаментов предприятия), управление ролями как набором прав доступа к ресурсам предприятия, введение в политику безопасности элементов косвенного определения прав через атрибуты прав доступа (credentials);
- обеспечение подотчетности (регистрации всех операций взаимодействий распределенных объектов системы в масштабах корпоративной сети) и аудита, мониторинга безопасности, тревожной сигнализации;

- интеграция с системами общего управления, инфраструктурными системами безопасности (PKI, LAS, IDS).

В рамках данной концепции *управление, основанное на политике безопасности* — PBM (Policy based management) — определяется как реализация набора правил управления, сформулированных для бизнес-объектов предприятия, которая гарантирует полноту охвата бизнес-области объектами и непротиворечивость используемых правил управления.

Система управления GSM, ориентированная на управление безопасностью предприятия на принципах PBM, удовлетворяет следующим требованиям:

- политика безопасности предприятия представляет собой логически и семантически связанную, формируемую, редактируемую и анализируемую как единое целое структуру данных;
- политика безопасности предприятия определяется в едином контексте для всех уровней защиты как единое целое сетевой политики безопасности и политики безопасности информационных ресурсов предприятия;
- для облегчения администрирования ресурсов и политики безопасности предприятия число параметров политики минимизируется.

Для того чтобы минимизировать число параметров политики, используются следующие приемы:

1) групповые определения объектов безопасности;

2) косвенные определения, например определения на основе верительных (credential) атрибутов;

3) мандатное управление доступом (в дополнение к фиксированному доступу), когда решение о доступе определяется на основе сопоставления уровня доступа, которым обладает субъект, и уровня конфиденциальности (критичности) ресурса, к которому осуществляется доступ.

Система управления GSM обеспечивает разнообразные механизмы анализа политики безопасности за счет средств многокритериальной проверки соответствия политики безопасности формальным моделям концепции безопасности предприятия.

Ниже приводится концепция определения ГПБ (GSP — Global Security Policy) сети предприятия и описание построенной на базе ГПБ системы управления безопасностью (policy based security management).

16.2.3. Глобальная и локальная политики безопасности

Глобальная политика безопасности корпоративной сети представляет собой конечное множество правил безопасности (security rules) (рис. 16.1), которые описывают параметры взаимодействия объектов корпоративной сети в контексте информационной безопасности:

- необходимый для соединения сервис безопасности (правила обработки, защиты и фильтрации трафика);
- направление предоставления сервиса безопасности;
- правила аутентификации объектов;
- правила обмена ключами;
- правила записи результатов событий безопасности в системный журнал;
- правила сигнализации о тревожных событиях и др.

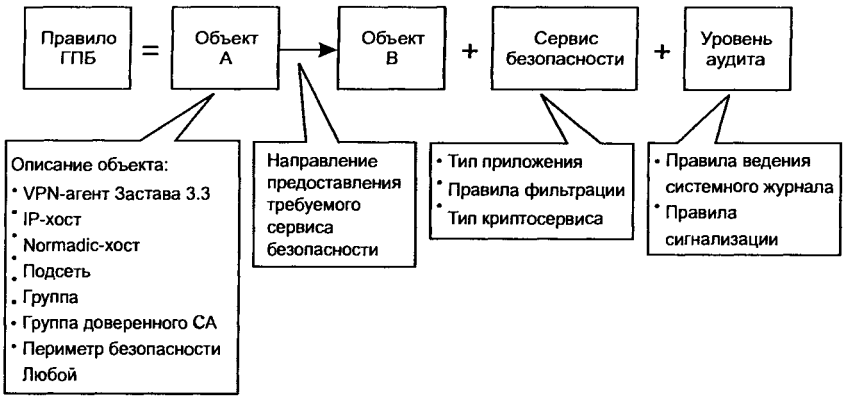


Рис. 16.1. Структура правила глобальной политики безопасности

При этом объектами ГПБ могут быть как отдельные рабочие станции и подсети, так и группы объектов, которые могут включать в себя целые структурные подразделения компании (например, отдел маркетинга или финансовый департамент) или даже отдельные компании (входящие, например, в холдинг). Политика безопасности для каждого объекта в группе автоматически реплицируется всем объектам группы.

Задачи защиты бизнес-объектов распределенной корпоративной системы можно сформулировать в терминах правил, поскольку сетевое взаимодействие можно представить как простую

передачу информации между субъектом Subj и объектом Obj доступа на основе некоторого сетевого сервиса защиты SecSrv, настроенного при помощи параметров *P*. В результате глобальная политика безопасности предприятия представляется как набор правил вида

(Subj, Obj, SecSrv (*P*)).

При этом отсутствие правила для объекта Obj означает запрет любого доступа к данному Obj.

Для простоты определения целей безопасности предприятия в GSM предусмотрено два типа объектов, выступающих в качестве Subj и Obj. Это — пользователь (*U*) и ресурс (*R*).

Ресурс *R* может быть информационным (*IR*) или сетевым (*NR*).

Пользователь и ресурс могут выступать в любой из форм агрегации, поддерживаемых в системе: группы, домены, роли, департаменты, разделы каталога.

Пример: правило (*U*, *IR*, *S*1) представляет собой правило защиты *S*1, обеспечиваемое при доступе пользователя *U* к информационному ресурсу *IR*. Правило (*IR*1, *IR*2, *S*2) означает разрешение сетевого взаимодействия двух информационных модулей (программ) с необходимостью обеспечения свойств защиты *S*2.

Политика по умолчанию для доступа к любому защищаемому объекту корпоративной системы представляет собой запретительное правило: *все, что не разрешено явно — запрещено*. Такое правило обеспечивает полноту защиты информации в сети предприятия и априорное отсутствие «дыр» в безопасности.

Чтобы обеспечить взаимодействие устройств в сети, для них создается и доставляется (в общем случае не по каналам сети) *стартовая конфигурация*, содержащая необходимые правила настройки устройств только для их централизованного управления — стартовая политика безопасности устройства.

Правила ГПБ могут быть распространены как на сетевые взаимодействия, так и на функции контроля и управления самой системы.

Функционально правила ГПБ разбиты по группам:

- *правила VPN*. Правила данного тира реализуются при помощи протоколов IPSec; агентом исполнения правила является драйвер VPN в стеке клиентского устройства или шлюза безопасности (*IP*1, *IP*2, VPNRule);

- *правила пакетной фильтрации.* Они обеспечивают пакетную фильтрацию типа stateful и stateless; исполнение этих правил обеспечивают те же агенты, что исполняют VPN-правила (*IP*1, *IP*2, PacketRule);
- *proxy-правила, включая антивирусную защиту «на лету».* Эти правила отвечают за фильтрацию трафика, передаваемого под управлением заданных прикладных протоколов; их исполнительным агентом является proxy-агент, например (User, Protocol, ProxyRule) или (Application, Protocol, ProxyRule);
- *правила аутентифицированного/авторизованного доступа, включая правила Single Sign-On.* Управление доступом Single Sign-On обеспечивает данному пользователю работу на едином пароле или другой аутентификационной информации со многими информационными ресурсами; понятно, что символическая запись правила сетевого доступа легко распространяется на Single Sign-On (User, Application, Authentication Scheme). Правила этой группы могут комбинированно исполняться агентами различного уровня, от VPN-драйвера до proxy-агентов; кроме того, агентами исполнения таких правил могут быть системы аутентификации запрос—отклик и продукты третьих разработчиков;
- *правила, отвечающие за сигнализацию и событийное протоколирование.* Политика протоколирования может оперативно и централизованно управляться агентом протоколирования; исполнителями правил являются все компоненты системы.

Набор правил ГПБ является логически целостным и семантически полным описанием политики безопасности в масштабах сети, на основе которой может строиться локальная политика безопасности отдельных устройств.

Локальная политика безопасности. Любому средству защиты, реализующему какой-либо сервис информационной безопасности, необходима для выполнения его работы ЛПБ — точное описание настроек для корректной реализации правил аутентификации пользователей, управления доступом, защиты трафика и др. При традиционном подходе администратору приходится отдельно настраивать каждое средство защиты или реплицировать какие-то простейшие настройки на большое число узлов с последующей их корректировкой. Очевидно, что это неизбежно при-

водит к большому числу ошибок администрирования и, как следствие, существенному снижению уровня защищенности корпоративной сети.

После формирования администратором ГПБ Центр управления на основе интерпретации ГПБ автоматически вычисляет и, если это необходимо, корректирует отдельные ЛПБ для каждого средства защиты и автоматически загружает нужные настройки в управляющие модули соответствующих средств защиты.

В целом, ЛПБ сетевого устройства включает в себя полный набор *правил* разрешенных соединений данного устройства, исполняемых для обеспечения какой-либо информационной услуги с требуемыми свойствами защиты информации.

Различие между правилами, реализующими ГПБ в сети, и правилами, реализующими ЛПБ конкретного устройства, заключается в том, что в правилах группы ГПБ объекты и субъекты доступа могут быть распределены произвольным образом в пределах сети, а правила группы ЛПБ, включая субъекты и объекты ЛПБ, предназначены и доступны только в пределах пространства одного из сетевых устройств.

16.3. Функционирование системы управления средствами безопасности

Структурными элементами системы управления средствами безопасности TrustWorks являются агенты безопасности (Trusted Agent), Центр управления (Trusted GSM Server) и Консоль управления (Trusted GSM Console) (рис. 16.2).

Назначение основных средств безопасности

Агент безопасности (Trusted Agent), установленный на *персональном компьютере клиента*, ориентирован на защиту индивидуального пользователя, выступающего, как правило, клиентом в приложениях клиент—сервер.

Агент безопасности, установленный на *сервере приложений*, ориентирован на обеспечение защиты серверных компонентов распределенных приложений.

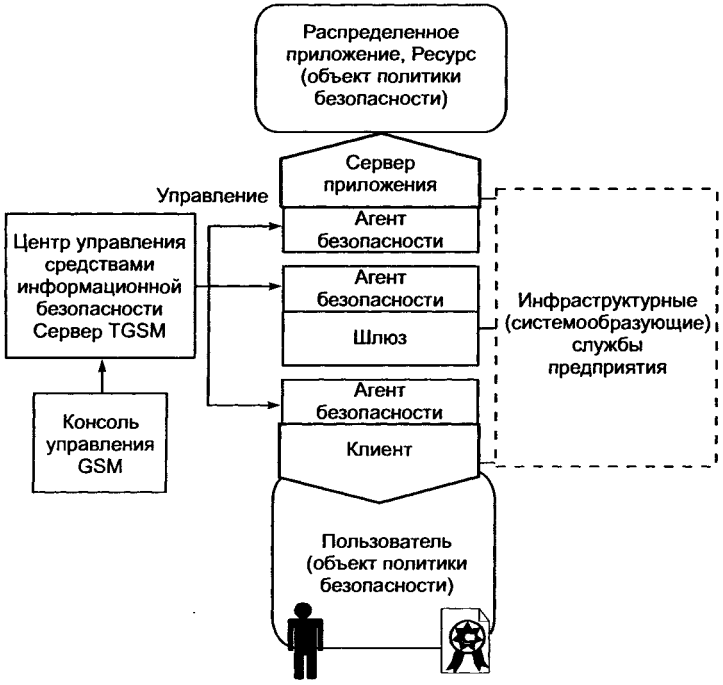


Рис. 16.2. Общая структурная схема системы управления средствами информационной безопасности

Агент безопасности, установленный на *шлюзовом компьютере*, обеспечивает развязку сегментов сети внутри предприятия или между предприятиями.

Центр управления (Trusted GSM Server) обеспечивает описание и хранение глобальной политики безопасности в масштабах сети, трансляцию глобальной политики в локальные политики безопасности устройств защиты, загрузку устройств защиты и контроль состояний всех агентов системы. Для организации распределенной схемы управления безопасности предприятия в системе GSM предусматривается установка нескольких (до 65 535) серверов GSM.

Консоль управления (Trusted GSM Console) предназначена для организации рабочего места администратора (администраторов) системы. Для каждого из серверов GSM может быть установлено несколько консолей, каждая из которых настраивается согласно ролевым правам каждого из администраторов системы GSM.

Локальный Агент безопасности (*Trusted Agent*) представляет собой программу, размещаемую на оконечном устройстве (клиенте, сервере, шлюзе) и выполняющую следующие функции защиты:

- аутентификацию объектов политики безопасности, включая интеграцию различных сервисов аутентификации;
- определение пользователя в системе и событий, связанных с данным пользователем;
- обеспечение централизованного управления средствами безопасности и контроля доступа;
- управление ресурсами в интересах приложений, поддержку управления доступом к ресурсам прикладного уровня;
- защиту и аутентификацию трафика;
- фильтрацию трафика;
- событийное протоколирование, мониторинг, тревожную сигнализацию.

Дополнительные функции Trusted Agent:

- поставка криптосервиса (multiple concurrent pluggable modules);
- управление периметрами Single Sign-On (как подзадача аутентификации пользователей);
- сервис в интересах защищенных приложений (криптосервис, сервис доступа к PKI, доступ к управлению безопасностью);
- сжатие трафика (IPcomp, pluggable module);
- управление резервированием сетевых ресурсов (QoS);
- функции локального агента сетевой антивирусной защиты.

Центральным элементом локального агента является *процессор локальной политики безопасности* (LSP processor), интерпретирующий локальную политику безопасности и распределяющий вызовы между остальными компонентами.

Защита ресурсов

Аутентификация и авторизация доступа. В рамках решения реализуются различные по функциональности схемы аутентификации, каждая из которых включает тип аутентификации и способ (механизм) идентификации объектов.

Для выбора типа аутентификации предусмотрены следующие возможности: аутентификация пользователя при доступе к среде GSM или локальной ОС, аутентификация пользователя при доступе в сеть (сегмент сети), взаимная сетевая аутентификация объектов (приложение—приложение). Для выбора способа иден-

тификации предусмотрены следующие варианты, предполагающие их любое совместное использование: токен (смарт-карта), пароль, «внешняя» аутентификация.

Контроль доступа при сетевых взаимодействиях. При инициализации защищенного сетевого соединения от локальной ОС или при получении запроса на установление внешнего соединения локальные агенты безопасности Trusted Agent на концах соединения (и/или на промежуточном шлюзе) обращаются к ЛПБ устройства и проверяют, разрешено ли установление этого соединения. В случае, если такое соединение разрешено — обеспечивается требуемый сервис защиты данного соединения, если запрещено — сетевое соединение не предоставляется.

Контроль доступа на уровне прикладных объектов. Для незащищенных распределенных приложений в GSM обеспечивается сервис разграничения прав доступа на уровне внутренних объектов данного приложения. Контроль доступа на уровне объектов прикладного уровня обеспечивается за счет применения механизма proxy. Proxy разрабатывается для каждого прикладного протокола. Предустановленным является протокол http.

Для построения распределенной схемы управления и снижения загрузки сети в GSM используется архитектура распределенных прокси-агентов (Proxy Module в составе Trusted Agent), каждый из которых:

- имеет абстрактный универсальный интерфейс, обеспечивающий модульное подключение различных proxy-фильтров;
- имеет интерфейс к системе управления, но использует временный кэш для управления параметрами фильтрации, а фильтрация управляется обобщенными правилами типа:
  - аутентифицировать субъект *X* в приложении-объекте *Y*;
  - разрешить доступ субъекту *X* к объекту *Y* с параметрами *P*;
  - запретить доступ субъекту *X* к объекту *Z*;
  - семантика правил управления proxy-фильтром и описания субъектов и объектов доступа зависят от конкретного прикладного протокола, однако центр управления имеет возможность регистрировать proxy-фильтры и обеспечивать управления ими в контексте общей глобальной политики безопасности.

Proxy Agent может быть установлен на шлюзе безопасности, непосредственно на сервере, исполняющем контролируемые приложения, и на клиентском месте системы.

Управление средствами защиты

Важнейшим элементом решения TrustWorks является централизованная, основанная на политике (policy based) система управления средствами сетевой и информационной безопасности масштаба предприятия. Эта система обеспечивает следующие качественные потребительские характеристики:

- высокий уровень защищенности системы управления (путем выделения защищенного периметра управления внутри сети предприятия);
- расширяемость системы управления информационной безопасностью;
- высокий уровень надежности системы управления и ключевых ее компонентов;
- интеграцию с корпоративными системами общего сетевого и информационного управления;
- простую, интуитивно воспринимаемую, эргономичную и инфраструктурную среду описания, формирования, мониторинга и диагностики политики безопасности масштаба предприятия (enterprise level policy based management).

Управление осуществляется специальным ПО администратора — *Консолью управления* (Trusted GSM Console). Количество и функции каждого из экземпляров установленного в системе ПО Trusted GSM Console задаются главным администратором системы в зависимости от организационной структуры предприятия. Для назначения функций каждого из рабочих мест Trusted GSM Console используется ролевой механизм разграничения прав по доступу к функциям управления (менеджмента) системы.

Функции управления GSM. В зависимости от вида управляемых объектов набор управляющих функций в GSM можно условно разбить на три категории.

1. Управление информационным каталогом. Функции управления информационным каталогом определяют информационную составляющую GSM:

- формирование разделов каталога;
- описание услуг каталога;
- назначение и контроль сетевых ресурсов, требуемых для выполнения услуги;
- регистрацию описания услуги;
- контроль состояния услуг или разделов каталога услуг;

- мониторинг исполнения услуг;
- подготовку и пересылку отчетов (протоколов) по состоянию каталога.

2. Управление пользователями и правами доступа. Для управления правами доступа пользователей системы к услугам (информационным или сетевым ресурсам) GSM обеспечивает следующие функции:

- формирование групп пользователей по ролям и/или привилегиям доступа к услугам системы;
- формирование иерархических агрегаций пользователей по административным, территориальным или иным критериям (домены и/или департаменты);
- формирование ролей доступа пользователей к услугам (информационным или сетевым ресурсам);
- назначение уровней секретности для услуг и пользователей системы (поддержка мандатного механизма разграничения прав);
- назначение фиксированных прав доступа группам, ролям, агрегациям пользователей или отдельным пользователям системы к информационным или сетевым ресурсам системы;
- подготовку и пересылку отчетов (протоколов) по доступу пользователей к услугам системы;
- подготовку и пересылку отчетов (протоколов) по работе администраторов системы

3. Управление правилами ГПБ. Правила ГПБ ставят в соответствие конкретные свойства защиты (как для сетевых соединений, так и для доступа пользователей к информационным услугам) предустановленным уровням безопасности системы. Контроль за соблюдением правил ГПБ выполняет специальный модуль в составе сервера системы — *Security Policy Processor*, обеспечивающий:

- определение каждого из уровней безопасности набором параметров защиты соединений, схемы аутентификации и разграничения прав;
- назначение уровней безопасности конкретным услугам или разделам каталога услуг;
- назначение уровней безопасности пользователям или любым агрегациям пользователей системы (группам, ролям, доменам, департаментам);
- контроль за целостностью ГПБ (полнотой правил);

- вычисление политик безопасности ЛПБ локальных устройств защиты — агентов безопасности — и контроль их исполнения;
- контроль за исполнением ГПБ по различным критериям;
- подготовку и пересылку отчетов (протоколов) по состоянию системы и всех попыток нарушения ГПБ.

Каждый из администраторов системы аутентифицируется и работает с системой через Trusted GSM Console согласно предустановленным для него правам (на каталог ресурсов или его часть, на определенный ролями набор функций управления, на группы или другие наборы пользователей). Все действия любого из администраторов протоколируются и могут попарно контролироваться.

16.4. Аудит и мониторинг безопасности

Для организаций, компьютерные сети которых насчитывают не один десяток компьютеров, функционирующих под управлением различных ОС, на первое место выступает задача управления множеством разнообразных защитных механизмов в таких гетерогенных корпоративных сетях. Сложность сетевой инфраструктуры, многообразие данных и приложений приводят к тому, что при реализации системы информационной безопасности за пределами внимания администратора безопасности могут остаться многие угрозы. Поэтому необходимо осуществление регулярного аудита и постоянного мониторинга безопасности ИС.

Аудит безопасности информационной системы

Понятие аудита безопасности. Аудит представляет собой независимую экспертизу отдельных областей функционирования предприятия. Одной из составляющих аудита предприятия является аудит безопасности его ИС.

В настоящее время актуальность аудита безопасности ИС резко возросла. Это связано с увеличением зависимости организаций от информации и ИС. Возросла уязвимость ИС за счет повышения сложности элементов ИС, появления новых технологий передачи и хранения данных, увеличения объема ПО. Расширился спектр угроз для ИС из-за активного использования предприятиями открытых глобальных сетей для передачи сообщений и транзакций.

Аудит безопасности ИС дает возможность руководителям и сотрудникам организаций получить ответы на вопросы:

- как оптимально использовать существующую ИС при развитии бизнеса;
- как решаются вопросы безопасности и контроля доступа;
- как установить единую систему управления и мониторинга ИС;
- когда и как необходимо провести модернизацию оборудования и ПО;
- как минимизировать риски при размещении конфиденциальной информации в ИС организации, а также наметить пути решения обнаруженных проблем.

На эти и другие подобные вопросы нельзя мгновенно дать однозначный ответ. Достоверную и обоснованную информацию можно получить, только рассматривая все взаимосвязи между проблемами. Проведение аудита позволяет оценить текущую безопасность ИС, оценить риски, прогнозировать и управлять их влиянием на бизнес-процессы организации, корректно и обоснованно подойти к вопросу обеспечения безопасности информационных ресурсов организации.

Цели проведения аудита безопасности ИС:

- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности.

В число дополнительных задач аудита ИС могут также входить выработка рекомендаций по совершенствованию политики безопасности организации и постановка задач для ИТ персонала, касающихся обеспечения защиты информации.

Проведение аудита безопасности информационных систем. Работы по аудиту безопасности ИС состоят из последовательных этапов, которые в целом соответствуют этапам проведения комплексного ИТ аудита автоматизированной системы:

- инициирования процедуры аудита;
- сбора информации аудита;
- анализа данных аудита;

- выработки рекомендаций;
- подготовки аудиторского отчета.

Аудиторский отчет является основным результатом проведения аудита. Отчет должен содержать описание целей проведения аудита, характеристику обследуемой ИС, результаты анализа данных аудита, выводы, содержащие оценку уровня защищенности АС или соответствия ее требованиям стандартов, и рекомендации по устранению существующих недостатков и совершенствованию системы защиты.

Мониторинг безопасности системы

Функции мониторинга безопасности ИС выполняют средства анализа защищенности и средства обнаружения атак (см. гл. 14). Средства анализа защищенности исследуют настройки элементов защиты ОС на рабочих станциях и серверах, БД. Они исследуют топологию сети, ищут незащищенные или неправильные сетевые соединения, анализируют настройки МЭ.

В функции системы управления безопасностью входит выработка рекомендаций администратору по устранению обнаруженных уязвимостей в сетях, приложениях или иных компонентах ИС организации.

Использование модели адаптивного управления безопасностью сети дает возможность контролировать практически все угрозы и своевременно реагировать на них, позволяя не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к их появлению.

Приложение
ТРЕБОВАНИЯ К СОВРЕМЕННЫМ СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к современным системам защиты информации основаны на материалах отечественных стандартов по информационной безопасности и руководящих документов (РД) по технической защите информации Государственной технической комиссии (ГТК) России.

Общие требования и рекомендации

Система (подсистема) защиты информации, обрабатываемой в автоматизированных системах различного уровня и назначения, должна предусматривать комплекс организационных, программных, технических и, при необходимости, криптографических средств и мер по защите информации при ее автоматизированной обработке, хранении и передаче по каналам связи.

Основными направлениями защиты информации являются:

- обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения и подделки в результате *несанкционированного доступа* (НСД) и специальных воздействий;
- обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

В качестве основных мер защиты информации рекомендуются:

- документальное оформление перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений;

- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам и документам;
- ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникации и хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей *автоматизированной системы* (АС) и обслуживающего персонала, контроль за НСД и действиями пользователей, обслуживающего персонала и посторонних лиц;
- учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;
- использование *специальных защитных знаков* (СЗЗ), создаваемых на основе физико-химических технологий для контроля доступа к объектам защиты и для защиты документов от подделки;
- необходимое резервирование технических средств и дублирование массивов и носителей информации;
- использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
- использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
- использование сертифицированных средств защиты информации;
- размещение объектов защиты на максимально возможном расстоянии относительно границы *контролируемой зоны* (КЗ);
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах КЗ;
- развязка цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

- электромагнитная развязка между линиями связи и другими цепями *вспомогательных технических средств и систем* (ВТСС), выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация;
- использование защищенных каналов связи и криптографических *средств защиты информации* (СЗИ);
- размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр информации;
- организация физической защиты помещений и собственно технических средств с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри контролируемой зоны технических средств разведки или промышленного шпионажа;
- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;
- предотвращение внедрения в АС программ-вирусов и программных закладок.

В целях дифференцированного подхода к защите информации, обрабатываемой в АС различного уровня и назначения, проводится классификация АС. Классификация АС осуществляется на основании требований РД ГТК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [21].

Конкретные требования по защите информации и мероприятия по их выполнению определяются в зависимости от установленного для АС класса защищенности. Рекомендуемые классы защищенности АС, СЗЗ, средств защиты информации по уровню контроля отсутствия недекларированных возможностей, а также показатели по классам защищенности СВТ и МЭ от НСД к информации приведены в таблице [21].

Лица, допущенные к автоматизированной обработке конфиденциальной информации, несут ответственность за соблюдение установленного в учреждении (на предприятии) порядка обеспечения защиты этой информации.

Классы защищенности от НСД к информации

	Руководящий документ	Классы защищенности																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Автоматизированные системы	1А	1Б	1В	1Г	1Д	2А	2Б	3А	3Б									
		1-я группа					2-я группа		3-я группа										
					*	*		*		*									
2	Средства вычислительной техники	4-я гр.	3-я группа			2-я группа		1-я гр.											
						*		-											
3	Межсетевые экраны				*														
4	Специальные защитные знаки													*					
5	Недекларированные возможности				*														

* рекомендуемые классы защищенности от НСД к конфиденциальной информации.

Конкретные требования к современным системам защиты информации приведены в следующих руководящих документах Гостехкомиссии России и государственных стандартах РФ:

1. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации. РД ГТК России. М., 1992.
2. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. РД ГТК России. М., 1992.
3. Средства вычислительной техники. МЭ. Защита от НСД к информации. Показатели защищенности от НСД к информации. РД ГТК России. М., 1997.
4. Защита информации. Специальные защитные знаки. Классификация и общие требования. РД ГТК России. М., 1992.
5. Защита от НСД к информации. Часть 1. ПО средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. РД ГТК России. М., 1999.
6. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). РД ГТК России. М., 2001.
7. ГОСТ Р 50739—95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
8. ГОСТ Р 51583—2000. Защита информации. Порядок создания систем в защищенном исполнении.

Литература

1. *Абрамов А. В., Панасенко С. П., Петренко С. А.* VPN-решения для российских компаний // Конфидент. 2001. № 1.

2. *Астахов А. М.* Аудит безопасности информационных систем. Конфидент. 2003. № 2.

3. *Ахметов К.* Безопасность в Windows XP // Безопасность. 2001. № 12.

4. *Гайкович В., Першин А.* Безопасность электронных банковских систем. М.: Единая Европа, 1994.

5. *Галатенко В. А.* Информационная безопасность — грани практического подхода. Конференция «Корпоративные Информационные Системы». М., 1999.

6. *Галатенко В. А., И. Трифоленков.* Введение в безопасность Интернет // LAN. 1996. № 6.

7. *Галатенко В. А.* Информационная безопасность // Открытые системы. 1996. № 1.

8. *Галатенко В. А.* Информационная безопасность в Intranet // LAN. 1996. № 7.

9. *Галицкий А. В., Рябко С. Д., Шаньгин В. Ф.* Защита информации в сети — анализ технологий и синтез решений М.: ДМК Пресс, 2004.

10. ГОСТ 28147—89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М., 1989.

11. ГОСТ Р 34.10—94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. М., 1994.

12. ГОСТ Р 34.11—94. Информационная технология. Криптографическая защита информации. Функция хэширования. М., 1994.

13. ГОСТ Р 50739—95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

14. ГОСТ Р 50922—96. Защита информации. Основные термины и определения.

15. ГОСТ Р 51275—99. Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения.

16. ГОСТ Р 51583—2000. Защита информации. Порядок создания систем в защищенном исполнении.

17. ГОСТ Р 34.10—2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

18. ГОСТ Р ИСО/МЭК 15408-1—2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М., 2002.

19. ГОСТ Р ИСО/МЭК 15408-2—2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. М., 2002.

20. ГОСТ Р ИСО/МЭК 15408-3—2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. М., 2002.

21. Гостехкомиссия России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: руководящий документ. М., 1992.

22. Гостехкомиссия России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации: руководящий документ. М., 1992.

23. Гостехкомиссия России. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: руководящий документ. М., 1997.

24. Гостехкомиссия России. Защита информации. Специальные защитные знаки. Классификация и общие требования: руководящий документ. М., 1992.

25. Гостехкомиссия России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей: руководящий документ. М., 1999.

26. Гостехкомиссия России. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К): руководящий документ. М., 2001.

27. *Грязное Е. С., Панасенко С. П.* Безопасность локальных сетей // Мир и безопасность. 2003. № 2.

28. *Диффи У.* Первые десять лет криптографии с открытым ключом // ТИИЭР. Т. 76. 1988. № 5.

29. *Дшхунян В. Л., Шаньгин В. Ф.* Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты. М.: АСТ: НТ Пресс, 2004.

30. *Зегжда Д. П., Ивашко А. М.* Основы безопасности информационных систем. М.: Горячая линия—Телеком, 2000.

31. *Зима В. М., Молдовян А. А., Молдовян Н. А.* Компьютерные сети и защита передаваемой информации. СПб.: Изд. СПбГУ, 1998.

32. *Зима В. М., Молдовян А. А., Молдовян Н. А.* Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2001.

33. *Иванов П.* IPSec: защита сетевого уровня // Сети. 2000. № 2.

34. ИСО/МЭК 14888-1—98. Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения.

35. ИСО/МЭК 14888-2—99. Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 2. Механизмы на основе подтверждения подлинности.

36. ИСО/МЭК 10118-1—94. Информационная технология. Методы защиты. Хэш-функции. Часть 1. Общие положения.

37. ИСО/МЭК 10118-2—94. Информационная технология. Методы защиты. Хэш-функции. Часть 2. Хэш-функции с использованием n-битного блочного алгоритма шифрации.

38. *Касперский Е.* Компьютерные вирусы: что это такое и как с ними бороться. М.: СК Пресс, 1998.

39. *Костров Д.* Системы обнаружения атак // BYTE Россия. 2002. № 8.

40. *Лукацкий А.* Обнаружение атак. СПб.: БХВ-Петербург, 2003.

41. *Лукацкий А.* Безопасность беспроводных сетей // Технологии и средства связи. 2005. № 1.

42. *Максим М., Полино Д.* Безопасность беспроводных сетей / Пер. с англ. А. В Семенова. М.: ДМК Пресс, 2004.

43. *Мамаев М., Петренко С.* Технологии защиты информации Интернета. Спец. справ. СПб.: Питер, 2002.

44. *Монин С.* Защита информации и беспроводные сети // КомпьютерПресс. 2005. № 4.

45. *Олифер В. Г., Олифер Н. А.* Новые технологии и оборудование IP-сетей. СПб.: БХВ-Петербург, 2000.

46. *Олифер В. Г.* Защита информации при работе в Интернет // Connect. 2002. № 11.

47. *Олифер Н. А.* Протоколы IPSec // LAN. 2001. № 3.

48. *Олифер Н. А.* Дифференцированная защита трафика средствами IPSec // LAN. 2001. № 4.

49. *Панасенко С. П.* Вновь об ЭЦП: стандарт X.509 // Системы безопасности, связи и телекоммуникаций. 2003. № 3.

50. *Панасенко С. П., Батура В. П.* Основы криптографии для экономистов: учеб. пособие / под ред. Л. Г. Гагариной. М.: Финансы и статистика, 2005.

51. *Панасенко С. П., Петренко С. А.* Криптографические методы защиты информации для российских корпоративных систем // Конфидент. 2001. № 5.

52. *Петренко С. А.* Реорганизация корпоративных систем безопасности // Конфидент. 2002. № 2.

53. *Петренко С. А.* Построение эффективной системы антивирусной защиты // Конфидент. 2002. № 3.

54. *Петров А. А.* Компьютерная безопасность: криптографические методы защиты. М.: ДМК Пресс, 2000.

55. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учеб. пособие для

вузов / П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др. М.: Радио и связь, 1999.

56. *Проскурин В. Г., Крутов С. В., Мацкевич И. В.* Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: учеб. пособие для вузов. М.: Радио и связь, 2000.

57. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей. М.: Московский офис Cisco Systems. Inc. 2001.

58. *Романец Ю. В., Тимофеев П. А., В. Ф. Шаньгин.* Защита информации в компьютерных системах и сетях. 2-е изд. М.: Радио и связь, 2001.

59. *Сарбуков А., Грушо А.* Аутентификация в компьютерных системах // Системы безопасности. 2003. № 5(53).

60. *Симонов С. В.* Методология анализа рисков в информационных системах // Конфидент. 2001. № 1.

61. *Скородумов Б.* Безопасность союза интеллектуальных карточек и персональных компьютеров // Мир карточек. 2002. № 5—6.

62. *Соколов А. В., Шаньгин В. Ф.* Защита информации в распределенных корпоративных сетях и системах. М.: ДМК Пресс, 2002.

63. Теоретические основы компьютерной безопасности: учеб. пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. М.: Радио и связь, 2000.

64. Типовые решения по применению технологии межсетевых экранов для защиты информационных ресурсов. СПб.: Конфидент, 2001.

65. Типовые решения по применению средств VPN для защиты информационных ресурсов. СПб.: Конфидент, 2001.

66. Типовые решения по применению технологии централизованного управления антивирусной защитой предприятия. СПб.: Конфидент, 2002.

67. *Трифаленков И., Зайцева Н.* Функциональная безопасность корпоративных систем // Открытые системы. 2002. № 7—8.

68. *Филиппов М.* Вопросы обеспечения безопасности корпоративных беспроводных сетей // Технологии и средства связи. 2003. № 2.

69. *Фролов А., Фролов Г.* Что нужно знать о компьютерных вирусах // BYTE Россия. 2002. № 8.

70. *Фролов А., Фролов Г.* Защита от компьютерных вирусов // BYTE Россия. 2002. № 9.

71. *Чепиков О.* Особенности применения двухфакторной аутентификации // Информационная безопасность. 2005. № 3.

72. *Чмора А. Л.* Современная прикладная криптография. М.: Гелиос АРВ, 2001.

73. *Шеннон К. Э.* Теория связи в секретных системах // Шеннон К. Э. Работы по теории информации и кибернетике. М.: Иностр. лит., 1963.

74. *Шрамко В. Н.* Комбинированные системы идентификации и аутентификации // PCWeek/RE. 2004. № 45.

75. *Шрамко В. Н.* Защита компьютеров: электронные системы идентификации и аутентификации // PCWeek/RE. 2004. № 12.

76. *Шрамко В. Н.* Аппаратно-программные средства контроля доступа // PCWeek/RE. 2003. № 9.

77. Interoperability Specification for ICCs and Personal Computer Systems. Part 8. Recommendations for ICC Security and Privacy Devices. Revision 1.0. PC/SC Workgroup, 1997.

78. ISO 17799 — Международный стандарт безопасности информационных систем. 2002.

79. ISO/IEC 14443-1 Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 1: Physical characteristics International Standard. 2000.

80. ISO/IEC 14443-2 Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 2: Radio frequency power and signal interface International Standard. 2001.

81. *Menezes A. J., van Oorschot P. C., Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, 1999.

82. *Schneier B.* Applied Cryptography. John Wiley & Sons, 1996.

Интернет-ресурсы

83. Базовый стандарт организации беспроводных локальных сетей IEEE 802.11. http://standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf

84. *Беляев А. В.* Методы и средства защиты информации. http://www.citforum.ru/internet/infsecure/its2000_01.shtml

85. *Касперский Е.* Компьютерные вирусы. http://www.kaspersky.ru/)

86. *Коротыгин С.* Развитие технологии беспроводных сетей: стандарт IEEE 802.11. http://www.ixbt.com/comm/wlan.shtml

87. *Кузнецов С.* Защита файлов в операционной системе UNIX. http://www.citforum.ru/database/articles/art_8.shtml,

88. *Олифер Н. А., Олифер В. Г.* Сетевые операционные системы, Центр Информационных Технологий. http://citforum.ru/operating_systems/sos/contents.shtml

89. Семейство стандартов IEEE 802.11. http://www.wireless.ru/wireless/wrl_base80211

90. *Скородумов Б. И.* Стандарты для безопасности электронной коммерции в сети Интернет. http://www.stcarb.comcor.ru

91. Advanced Encryption Standard (AES) Development Effort. February 2001 // csrc.nist.gov/CryptoToolkit/aes/index2.html

92. *Daemen J., Rijmen V.* AES Proposal: Rijndael. Document version 2. September 1999 // www.esat.kuleuven.ac.be/ ~rijmen/rijndael

93. *Dierks T., Allen C.* RFC 2246: The TLS Protocol Version 1.0. January 1999 // www.ietf.org/rfc/rfc2246.txt

94. FIPS Publication 197. Announcing the Advanced Encryption Standard (AES). November, 2001 // csrc.nist.gov/publications/fips/fipsl97/fips-197.pdf

95. *Hodges J.* RFC 3377: Lightweight Directory Access Protocol (v3): Technical Specification. September 2002 / J. Hodges, R. Morgan // www.ietf.org/rfc/rfc3377.txt

96. *Housley R., Ford W., Polk W. etc.* RFC 2459: Internet X.509 Public Key Infrastructure. January 1999 // www.ietf.org/rfc/ rfc2459.txt

97 *Kent S., Atkinson R.* RFC 2401: Security Architecture for IP. November 1998 // www.ietf.org/rfc/rfc2401.txt

98. *Orman H.* RFC 2412: The OAKLEY Key Determination Protocol. November 1998 // www.ietf.org/rfc/rfc2412.txt

99. PKCS #1 v2.1: RSA Cryptography Standard. RSA Laboratories. June 2002 // www.rsasecurity.com/rsalabs/pkcs/pkcs-l

100. *Dusse S., Hoffman P., Ramsdell B.* etc. RFC 2311: S/MIME Version 2 Message Specification. March 1998 // www.ietf.org/rfc/rfc2311.txt

101. *Leech M., Ganis M., Lee Y. etc.* RFC 1928: SOCKS Protocol Version 5. March 1996 // www.ietf.org/rfc/rfc1928.txt

102. *Maughan D., Schertler M. etc.* RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP). November 1998 // www.ietf.org/rfc/rfc2408.txt

103. *Rivest R.* The MD5 Message-Digest Algorithm. April 1992 // www.ietf.org/rfc/rfc1321 .txt

104. *Rivest R., Robshaw M.J.B., Sidney R. etc.* The RC6 Block Cipher. Version 1.1. August 1998 // www.rsasecurity.com/rsalabs/aes

105. *Zeilenga K.* RFC 3673: Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes. December 2003. www.ietf.org/rfc/rfc3673.txt

Оглавление

Шаньгин Владимир Федорович

Информационная безопасность компьютерных систем и сетей

Учебное пособие

Редактор *Е. Г. Соболевская*
Корректор *Н. Н. Морозова*
Компьютерная верстка *И. В. Кондратьевой*
Оформление серии *К. В. Пономарева*

Сдано в набор 15.02.2007. Подписано в печать 24.05.2007. Формат 60x90/16.
Печать офсетная. Гарнитура «Таймс». Усл. печ. л. 26,0. Уч.-изд. л. 26,5.
Бумага типографская. Тираж 3000 экз. Заказ № 5819.

ЛР № 071629 от 20.04.98
Издательский Дом «ФОРУМ»
101000, Москва — Центр, Колпачный пер., д. 9а
Тел./факс: (495) 625-39-27
E-mail: forum-books@mail.ru

ЛР № 070824 от 21.01.93
Издательский Дом «ИНФРА-М»
127282, Москва, Полярная ул., д. 31в
Тел.: (495) 380-05-40
Факс: (495) 363-92-12
E-mail: books@infra-m.ru
Http://www.infra-m.ru

По вопросам приобретения книг обращайтесь:

Отдел продаж «ИНФРА-М»
127282, Москва, ул. Полярная, д. 31в
Тел.: (495) 363-42-60
Факс: (495) 363-92-12
E-mail: books@infra-m.ru

Центр комплектования библиотек
119019, Москва, ул. Моховая, д. 16
(Российская государственная библиотека, кор. К)
Тел.: (495) 202-93-15

Магазин «Библиосфера» (розничная продажа)
109147, Москва, ул. Марксистская, д. 9
Тел.: (495) 670-52-18, (495) 670-52-19

Отпечатано с предоставленных диапозитивов
в ОАО «Тульская типография». 300600, г. Тула, пр. Ленина, 109.