

**Автономная некоммерческая организация высшего образования  
«Московский международный университет»**

**2022**

**Н.В. Келдыш**

# **Системная защита информации компьютерных сетей**



**Учебное пособие**

---

УДК 004  
ББК 30ф  
К 34

Рецензенты:

Матюнина О.Е. – исполнительный директор института информационных систем и инженерно-компьютерных технологий АНО ВО «Российский новый университет», кандидат технических наук.

Ванина М.Ф. – доцент Московского технического университета связи и информатики, кандидат технических наук.

**Келдыш, Наталья Всеволодовна**

К 34 Системная защита информации компьютерных сетей. Учебное пособие – М.: Мир науки, 2022. – 100 с. – Сетевое издание. – Загл. с экрана.

ISBN 978-5-907603-38-7

В учебном пособии подробно рассматриваются проблемы обеспечения информационной безопасности сетей, понятным языком излагаются базовые понятия криптографической защиты информации, детально обсуждаются понятия идентификации, аутентификации и авторизации пользователей при работе в информационных сетях, приводятся принципы комплексной защиты информации в сетях.

Для дисциплины «Информационная безопасность».

Для студентов высших учебных заведений, а также пособие может быть использовано в качестве дополнительного материала для слушателей курсов профессиональной переподготовки и повышения квалификации.

ISBN 978-5-907603-38-7

---

© Келдыш Наталья Всеволодовна  
© ООО Издательство «Мир науки», 2022

## Оглавление

Введение.....	4
Глава 1. Проблемы информационной безопасности компьютерных сетей .....	5
1.1. Модель ISO/OSI и стек протоколов TCP/IP как основной стандарт построения компьютерных сетей.....	5
1.2. Угрозы сетевой безопасности и проблемы безопасности IP-сетей.....	14
1.3. Угрозы безопасности беспроводным сетям и уязвимости беспроводных сетей .....	22
1.4. Обеспечение информационной безопасности компьютерных сетей.....	26
Глава 2. Криптографическая защита информации в компьютерных сетях .....	30
2.1. Основные понятия криптографической защиты информации .....	30
2.2. Симметричные крипtosистемы шифрования.....	35
2.3. Асимметричные крипtosистемы шифрования.....	39
2.4. Функция хэширования .....	42
2.5. Электронная цифровая подпись.....	44
Глава 3. Идентификация, аутентификация и управление доступом .....	49
3.1. Аутентификация, авторизация и администрирование действий пользователей в компьютерных сетях .....	49
3.2. Аутентификация на основе многоразовых паролей .....	53
3.3. Аутентификация на основе одноразовых паролей .....	55
3.4. Биометрическая аутентификация пользователей.....	56
Глава 4. Безопасность операционных систем.....	61
4.1. Угрозы безопасности операционной системы .....	61
4.2. Понятие защищенной операционной системы.....	64
Глава 5. Современные подходы к обеспечению анонимности работы в сети Интернет .....	69
5.1. Прокси-серверы .....	69
5.2. Виртуальные частные сети (VPN/SSH).....	72
5.3. Сеть анонимизации TOR .....	74
5.4. Сеть анонимизации I2P .....	80
Глава 6. Вредоносные программы и спам .....	84
6.1. Классификация вредоносных программ .....	84
6.2. Рекомендации по безопасной работе в сети Интернет .....	90
Список литературы.....	94
Словарь англоязычных аббревиатур .....	95

## Введение

Современное состояние общества характеризуется активным развитием средств вычислительной техники и связи, а также методов автоматизированной обработки информации.

Применение этих средств и методов приняло всеобщий характер, а создаваемые при этом информационно-вычислительные системы и сети стали глобальными как в смысле территориальной распределённости, так и в смысле широты охвата в рамках единых технологий процессов сбора, передачи, накопления, хранения, поиска, обработки информации и выдачи ее для использования. Обработка информации при этом базируется на использовании персональных компьютеров, локальных сетей, региональных и глобальных сетей.

Без знания основ построения информационной безопасности сетей и квалифицированного применения современных информационных технологий, стандартов, протоколов и средств защиты информации невозможно достичь требуемого уровня понимания процессов и безопасного применения компьютерных систем и сетей.

В связи с этим в настоящем учебном пособии подробно рассматриваются проблемы обеспечения информационной безопасности сетей, понятным языком излагаются базовые понятия криптографической защиты информации, детально обсуждаются понятия идентификации, аутентификации и авторизации пользователей при работе в информационных сетях, приводятся принципы комплексной защиты информации в сетях. Автором приводится классификация вредоносных программ, описываются современные подходы к обеспечению анонимности работы в Интернете, даются рекомендации по повышению безопасности работы в Интернете.

# Глава 1. Проблемы информационной безопасности компьютерных 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).

## 1.1. Модель ISO/OSI и стек протоколов TCP/IP как основной стандарт построения компьютерных сетей

Основная задача, решаемая, при создании компьютерных сетей – обеспечение совместимости оборудования по электрическим и механическим характеристикам, а также по 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 Международного института стандартов ISO (International Standards Organization) в начале 1980-х годов 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 формализованные 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. Стек TCP/IP объединяет в себе целый 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, а также передачу блоков данных по этим маршрутам, и протокол TCP, обеспечивающий надежную доставку, безошибочность и правильный порядок приема передаваемых данных.

Сегодня этот стек используется для связи компьютеров всемирной информационной сети Интернет, а также в огромном числе корпоративных и ведомственных сетей. Стек TCP/IP является самым распространенным средством организации составных компьютерных сетей.

**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. 1.1. Стек протоколов TCP/IP имеет четыре уровня: прикладной (Application), транспортный (Transport), уровень межсетевого взаимодействия (Internet) и уровень сетевых интерфейсов (Network). 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 SMTP, используемый в электронной почте сети Интернет, гипертекстовые сервисы доступа к удаленной информации, например, WWW и многие другие. Рассмотрим несколько подробнее некоторые из этих протоколов.

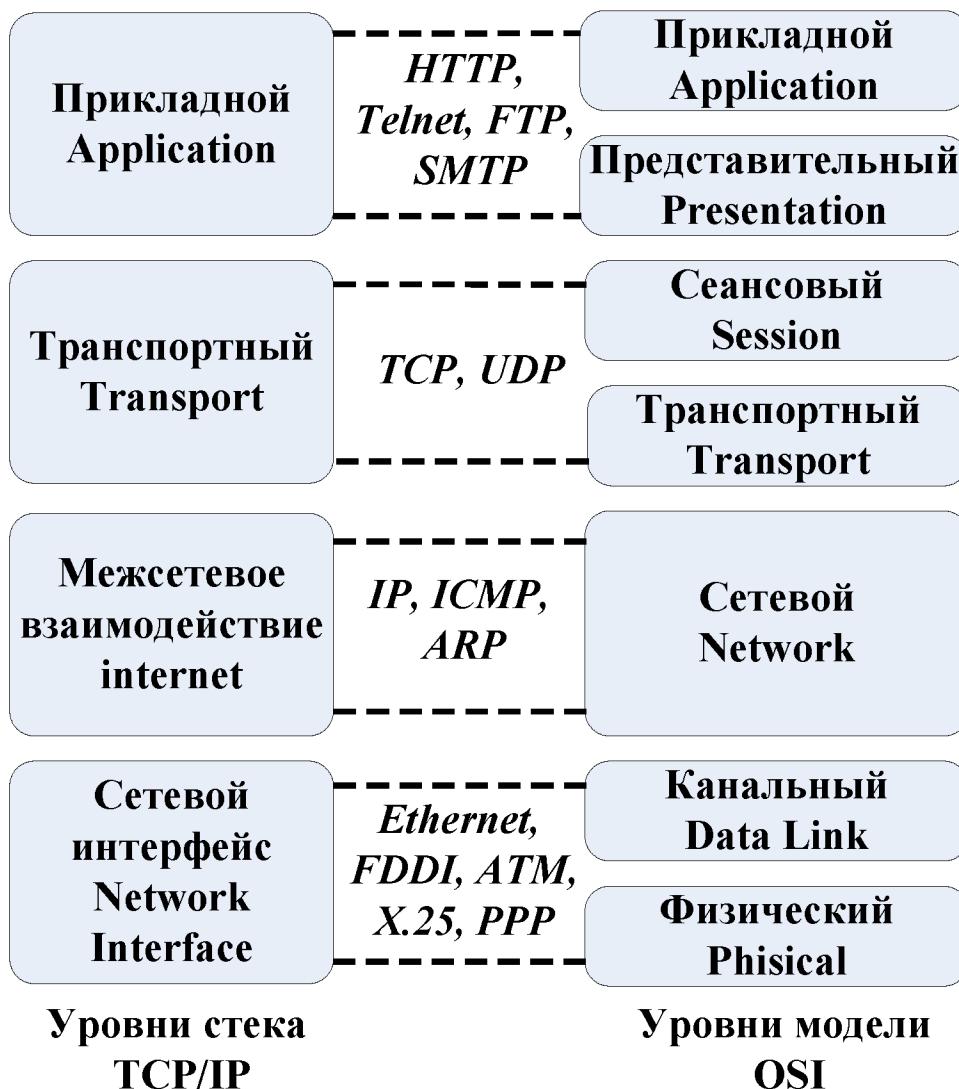


Рис. 1.1. Уровни стека протоколов TCP/IP

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. В стеке TCP/IP протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования. Если приложению не требуются все возможности протокола FTP, тогда можно использовать простой протокол пересылки файлов TFTP (*Trivial File Transfer Protocol*). Этот

---

протокол реализует только передачу файлов, причем в качестве транспорта используется протокол без установления соединения – UDP.

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 Интернета. 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 протоколы TCP и UDP.

Протокол управления передачей TCP (*Transmission 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.

Протоколдейтаграмм 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 он «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, которые состоят из большого количества локальных сетей, объединенных как локальными, так и глобальными связями.

Суть протокола IP заключается в том, что у каждого пользователя всемирной сети Интернет должен быть свой уникальный адрес (IP-адрес). Без этого нельзя говорить о точной доставке TCP-пакетов в нужное 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, сможет по этим четырем числам определить, кому из ближайших «соседей» надо переслать пакет, чтобы он оказался «ближе» к получателю. В результате конечного числа перебросок 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 «далее», 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 – 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. На рис. 1.2 показано, как осуществляется физическое и логическое соединение уровней. Вертикальные стрелки показывают физическое соединение в рамках одного хоста, а горизонтальные – логическое соединение между одноименными уровнями в различных хостах.

Приложение передает транспортному уровню сообщение (message), которое имеет соответствующие 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, затем к уровню межсетевого взаимодействия и далее через уровень сетевого интерфейса в сеть, каждый протокол выполняет соответствующую обработку

и инкапсулирует результат этой обработки, присоединяя спереди свой заголовок. На рис. 1.3 показана схема процесса инкапсуляции передаваемых данных и формирования заголовков пакетов в стеке TCP/IP.

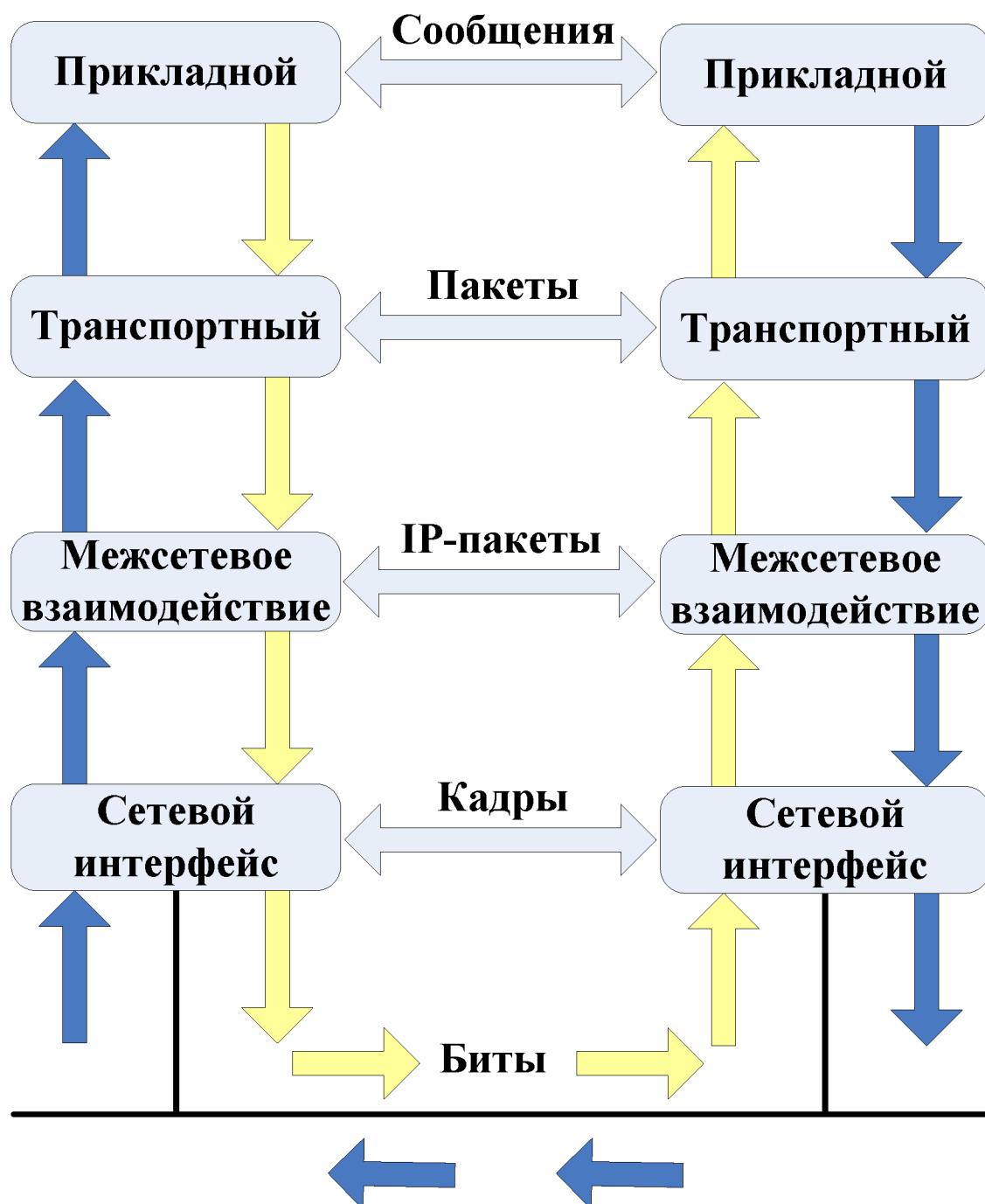


Рис. 1.2. Логические и физические соединения между уровнями стека TCP/IP

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 на нижних уровнях. Например, если шифруются данные на уровне IP, то уровень TCP и прикладной остаются неизменными.

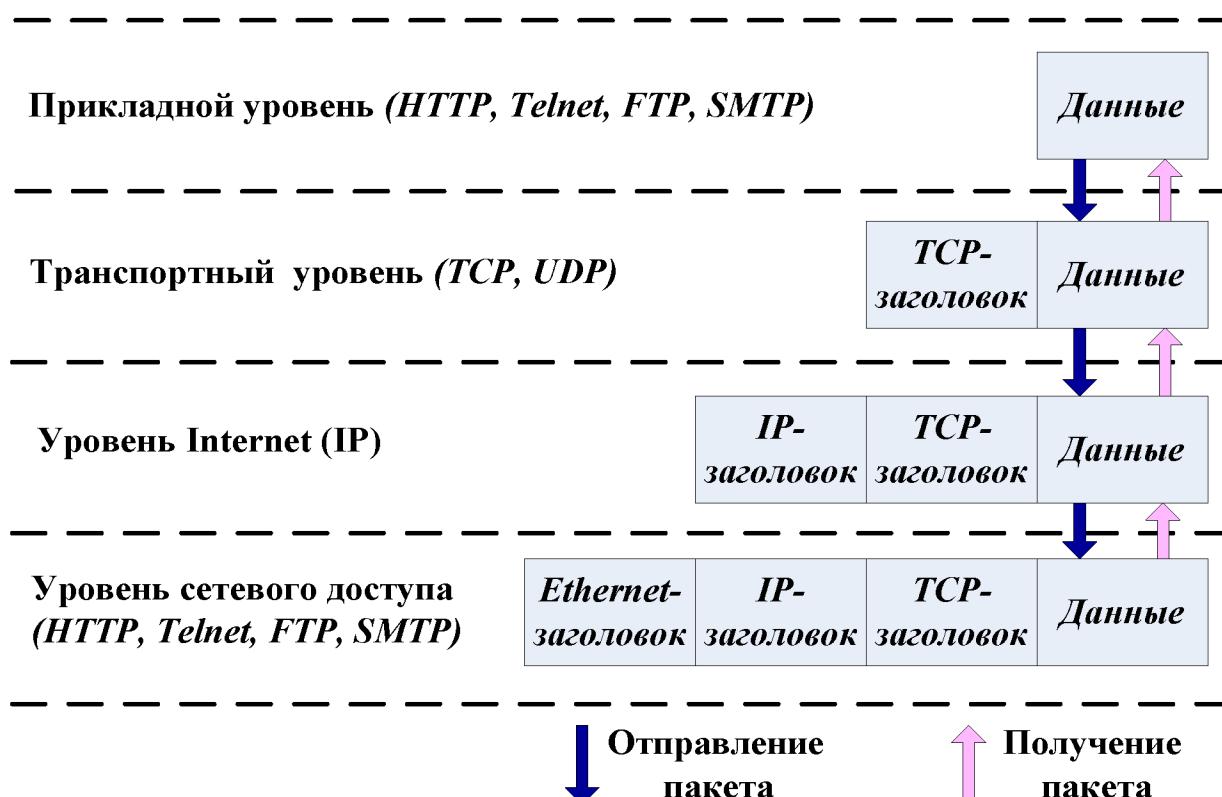


Рис. 1.3. Схема инкапсуляции данных в стеке протоколов TCP/IP

Что касается безопасности протоколов TCP/IP, т.е. безопасности передачи данных в Интернете в целом, пользователям необходимо иметь в виду, что, если не принято специальных мер, все данные передаются протоколами TCP/IP в открытом виде.

## 1.2. Угрозы сетевой безопасности и проблемы безопасности IP-сетей

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 для межсетевого взаимодействия. Однако повсеместное распространение стека протоколов TCP/IP обнажило и его слабые стороны.

Стремительный рост популярности интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т.д.

**Особенности сетевых атак.** Специалисты спецслужб в области ИТ и хакеры 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. Сегодня к этой сети подключены миллионы компьютеров. Многие миллионы компьютеров будут подключены к Интернету в ближайшем будущем, поэтому вероятность доступа к уязвимым компьютерам и компьютерным сетям постоянно возрастает. Кроме того, широкое распространение Интернета позволяет хакерам обмениваться информацией в глобальном масштабе.

Во-вторых, это всеобщее распространение простых в использовании операционных систем 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 мышью.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью. Другие

---

может осуществить обычный оператор, даже не предполагающий, какие последствия может иметь его деятельность. Нарушитель, осуществляя атаку, обычно ставит перед собой следующие цели:

- нарушение конфиденциальности передаваемой информации;
- нарушение целостности и достоверности передаваемой информации;
- нарушение работоспособности системы в целом или отдельных ее частей.

С точки зрения безопасности распределенные системы характеризуются прежде всего наличием *удаленных атак*, 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, поскольку необнаруживаемость препятствует своевременному реагированию на осуществленную угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

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

На практике IP-сети уязвимы для ряда 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. Рассмотрим наиболее распространенные виды

---

сетевых атак.

**Подслушивание (Sniffing).** По большей части данные по компьютерным сетям передаются в незащищенном формате (открытым текстом), что позволяет заинтересованному лицу, получившему доступ к линиям передачи данных в вашей сети, подслушивать или считывать трафик. Для подслушивания в компьютерных сетях используют снiffeр. *Сниффер пакетов* представляет собой прикладную программу, которая перехватывает все сетевые пакеты, передаваемые через определенный домен.

В настоящее время снiffeры 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 снiffeра можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

*Перехват пароля (Password Sniffing)*, передаваемого по сети в незашифрованной форме, путем «подслушивания» канала является разновидностью атаки подслушивания. 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 снiffeинга пакетов можно с помощью следующих мер и средств: применение для аутентификации однократных паролей; установка аппаратных или программных средств, распознающих снiffeры; применение 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, наверняка вы не захотите, чтобы они были изменены по пути.

**Анализ сетевого трафика.** Целью атак подобного типа являются прослушивание каналов связи и анализ передаваемых данных и служебной информации с целью изучения топологии и архитектуры построения системы, добывания критической пользовательской информации. Атакам данного типа подвержены такие протоколы, как FTP и 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 операционных систем 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, или IP-спуфингом (IP-spoofing)*.

IP-спуфинг имеет место, когда злоумышленник (или агент), находящийся внутри организации 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 являются отправной точкой для других атак. Классическим примером является атака типа «отказ в обслуживании» (DoS), которая начинается с чужого адреса, скрывающего истинную личность атакующего.

Угрозу спуфинга можно ослабить (но не устраниТЬ) с помощью следующих мер: правильная настройка управления доступом из внешней сети; пресечение попыток спуфинга чужих сетей пользователями своей сети; введение дополнительных методов аутентификации пользователей (на основе одноразовых паролей или других методов криптографии).

**Посредничество.** Атака типа «посредничество» 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 – «человек-в-середине»).** Для проведения атаки «человек-в-середине» специалистам спецслужб 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 снiffeры пакетов, транспортные протоколы и протоколы маршрутизации.

В более общем случае атаки «человек-в-середине» 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 «человек-в-середине» 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 специалистом компьютерной разведки на новый хост, а исходному серверу выдается команда разорвать соединение. В результате «собеседник» законного пользователя оказывается незаметно подмененным.

После получения доступа к сети у атакующего появляются следующие возможности:

- он может посыпать некорректные данные приложениям и сетевым службам, что приводит к их аварийному завершению или неправильному функционированию;
- он может также наводнить компьютер или всю сеть трафиком, пока не произойдет остановка системы в связи с перегрузкой;
- наконец, атакующий может блокировать трафик, что приведет к потере доступа авторизованных пользователей к сетевым ресурсам.

**Отказ в обслуживании – DoS (Denial of Service).** Эта атака отличается

от атак других типов. Она не нацелена на получение доступа к вашей 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 операционной системы или приложения. По существу, эта атака лишает обычных пользователей доступа к ресурсам или компьютерам сети организации.

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

Если атака этого типа проводится одновременно через множество устройств, мы говорим о *распределенной атаке отказа в обслуживании DDoS (Distributed DoS)*.

Простота реализации атак DoS и огромный вред, причиняемый ими организациям и пользователям, привлекают к этим атакам пристальное внимание администраторов сетевой безопасности.

**Парольные атаки.** Целью этих атак является завладение паролем и логином законного пользователя. Сотрудники подразделений компьютерной разведки могут проводить парольные атаки, используя такие методы, как:

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

IP-спуфинг и снiffeинг 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 подход 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).

Средства перехвата, подбора и взлома паролей в настоящее время считаются практически легальными и официально выпускаются достаточно большим числом компаний. Они позиционируются как программы для аудита безопасности и восстановления забытых паролей и их можно на законных

---

основаниях приобрести у разработчиков.

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

**Угадывание ключа.** Криптографический ключ представляет собой код или число, необходимое для расшифровки защищенной информации. Хотя узнать ключ доступа трудно 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.** Эти атаки могут проводиться несколькими способами. Самый распространенный из них состоит в использовании известных слабостей серверного программного обеспечения (FTP, HTTP, веб-сервера).

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через межсетевой экран.

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.

**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. Эхотестирование 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.

**Злоупотребление доверием.** Данный тип действий не является атакой в полном смысле этого слова. Он представляет собой злонамеренное использование отношений доверия, существующих в сети. Типичным примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте обычно располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к 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.

Перечисленные атаки на IP-сети возможны в силу ряда причин:

- использование 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;
- отсутствие в базовой версии стека протоколов TCP/IP механизмов, обеспечивающих конфиденциальность и целостность передаваемых сообщений;
- аутентификация отправителя осуществляется по его IP-адресу. Процедура аутентификации выполняется только на стадии установления соединения, а в дальнейшем подлинность принимаемых пакетов не проверяется;
- отсутствие возможности контроля за маршрутом прохождения сообщений в сети Интернет, что делает удаленные сетевые атаки практически безнаказанными.

**Криминализация атак на компьютерные сети и системы.** В последние годы растет криминализация атак на информационные системы. Киберпреступность изменяется не только количественно, но и качественно. Школьников и студентов, которые раньше писали большинство вирусов и занимались хакингом из любопытства и тщеславия, сейчас заменяют «серезные люди», строящие на реализации угроз информационной безопасности свой бизнес. Вместо хаотичного распространения вредоносных программ они организуют направленные комплексные атаки на системы организаций-жертв с четкой целью завладения конфиденциальной информацией или хищения денежных средств в электронных расчетных системах.

Компьютерные преступления перемещаются в область организованной преступности и получают все более четкую ориентацию на получение доходов в результате их совершения. Растет число инцидентов, связанных с нелегальным получением доступа к конфиденциальной информации, вымогательством под угрозой организации атаки на компьютерную систему, подкупом сотрудников атакуемой организации, заказными атаками «отказ в обслуживании» коммерческих интернет-порталов. Онлайн-криминал незаметно превратился в организованный и очень живучий бизнес с инновациями, инвестициями и транснациональной структурой.

Переход компьютерных преступлений «на деловые рельсы» и повышение организованности атак на информационные системы вызывает серьезный рост опасности их последствий для атакуемых организаций.

### **1.3. Угрозы безопасности беспроводным сетям и уязвимости беспроводных сетей**

При построении беспроводных сетей одной из наиболее острых проблем является обеспечение 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 количества возможных уязвимостей для атак и проникновений.

---

Оборудование беспроводных локальных сетей WLAN (Wireless Local Area Network) включает в себя точки беспроводного доступа и компьютеры абонентов.

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 Интернетом. Каждая точка доступа может обслуживать несколько абонентов. Несколько близко расположенных 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 связано с наличием неконтролируемой области между конечными точками беспроводной сети. Это позволяет атакующим, находящимся в непосредственной близости от беспроводных структур, производить целый ряд действий, которые невозможны в проводном мире.

При использовании беспроводного доступа к локальной сети угрозы безопасности существенно возрастают (рис. 1.4).

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 зарегистрироваться беспроводные узлы 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 посыпается при подключении, поэтому все равно существует небольшое окно уязвимости.

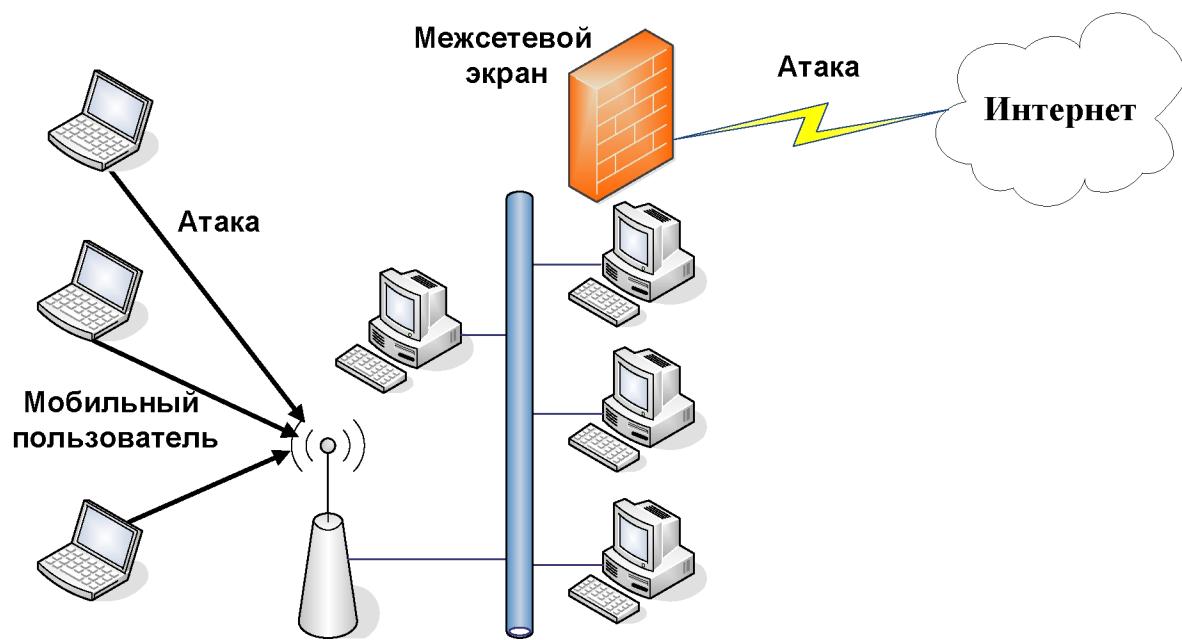


Рис. 1.4. Угрозы при беспроводном доступе к локальной сети

*Обнаружение WLAN.* Для обнаружения беспроводных сетей WLAN используется, например, утилита NetStumbler совместно со спутниковым навигатором глобальной системы позиционирования 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 добывшие данные для того, чтобы получить доступ к сетевым

---

ресурсам. Оборудование, используемое для подслушивания в сети, может быть не сложнее того, которое применяется 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. Это позволяет подключиться к беспроводной, сети, располагающейся в здании, человеку, сидящему в машине на стоянке рядом с ним. 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, чтобы заглушить истинную точку доступа в сеть.

*Отказ в обслуживании.* Полную парализацию сети может вызвать атака типа «отказ в обслуживании» (DoS). Цель любой атаки отказа в обслуживании 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. Можно 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 типа «человек-в-середине» выполняются на беспроводных сетях гораздо проще, чем на проводных, так как к проводной сети требуется реализовать определенный вид доступа. Обычно атаки «человек-в-середине» используются для нарушения конфиденциальности и целостности сеанса связи. Атаки «человек-в-середине» более сложны, чем большинство других атак: для их проведения требуется подробная информация о сети. Спецслужбы обычно подменяют идентификацию одного из сетевых ресурсов, после чего используют возможность прослушивания и нелегального захвата потока данных с целью изменения его содержимого, необходимого для выполнения своих задач.

*Анонимный доступ в Интернет.* Незащищенные беспроводные ЛВС

(локальные вычислительные сети) 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.

Атаки, используемые хакерами для взлома беспроводных сетей, не ограничиваются описанными выше.

#### **1.4. Обеспечение информационной безопасности компьютерных сетей**

Существует два подхода к проблеме обеспечения безопасности компьютерных систем и сетей: фрагментарный и комплексный.

*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. Существенным недостатком данного подхода является отсутствие 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 либо 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.

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 организации, и конкретные меры безопасности, касающиеся людей);
- программно-технического (конкретные технические меры).

*Меры законодательного уровня* очень важны для обеспечения информационной безопасности. К этому уровню можно отнести весь комплекс мер, направленных на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности. Большинство людей не совершают противоправных действий потому, что это осуждается и/или наказывается обществом, и потому, что так поступать не принято.

*Меры административно-организационного уровня.* Администрация организации должна сознавать необходимость поддержания режима безопасности и выделения на эти цели соответствующих ресурсов. Основой мер защиты административно-организационного уровня является политика

---

безопасности и комплекс организационно-технических мер. Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов организации.

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

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

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

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, администраторов и т.п.

*Меры и средства программно-технического уровня.* В рамках современных информационных систем должны быть доступны, по крайней мере, следующие механизмы безопасности:

- идентификация и проверка подлинности пользователей;
- управление доступом;
- протоколирование и аудит;
- криптография;
- экранирование;
- обеспечение высокой доступности.

*Необходимость применения стандартов.* Информационные системы министерств и ведомств почти всегда построены на основе программных и аппаратных продуктов различных производителей. Дело в том, что на данный момент 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

---

---

будут отвечать за безопасность каждого компонента ИС: правильно их настраивать, постоянно отслеживать происходящие изменения, контролировать работу пользователей. Очевидно, что чем разнороднее информационная система, тем сложнее обеспечить ее безопасность. Изобилие в корпоративных сетях и системах устройств защиты, межсетевых экранов, 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.

Стандарты образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности и определяют критерии управления безопасностью. Стандарты являются необходимой базой, обеспечивающей совместимость продуктов разных производителей, что чрезвычайно важно при создании систем сетевой безопасности в гетерогенных средах.

Комплексный подход к решению проблемы обеспечения безопасности, рациональное сочетание законодательных, административно-организационных и программно-технических мер и обязательное следование промышленным, национальным и международным стандартам являются тем фундаментом, на котором строится вся система защиты корпоративных сетей.

## Глава 2. Криптографическая защита информации в компьютерных сетях

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 данных.

### 2.1. Основные понятия криптографической защиты информации

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 также 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 легитимность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

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 *зашифрованием информации* понимается процесс преобразования открытой информации (исходного текста) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптоматрице с использованием ключа шифрования называют *расшифровыванием* (десифрованием).

Обобщенная схема крипосистемы шифрования показана на рис. 2.1. Исходный текст передаваемого сообщения (или хранимой информации)  $M$  зашифровывается с помощью криптографического преобразования  $Ek_1$  с получением в результате *шифртекста*  $C$ :

$$C = Ek_1(M),$$

где  $k_1$  – параметр функции  $E$  называемый ключом шифрования.

Шифртекст  $C$ , называемый еще *криптоматрицей*, 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 преобразования. 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.

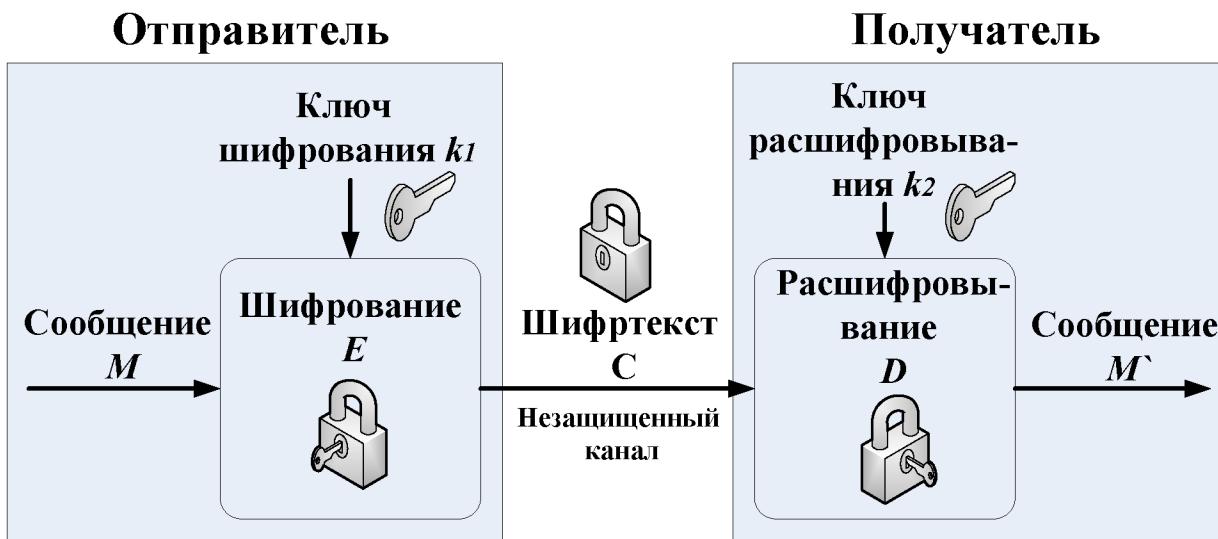


Рис. 2.1. Обобщенная схема криптосистемы шифрования

Обратное преобразование информации выглядит следующим образом:

$$M' = Dk_2(C).$$

Функция  $D$  является обратной к функции  $E$  и производит расшифрование 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 расшифрования 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 расшифрования. Соответственно различают два основных класса криптосистем:

- симметричные криптосистемы;
- асимметричные криптосистемы.

Известно несколько классификаций криптографических алгоритмов (КА). 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, например, показанная на рис. 2.2.

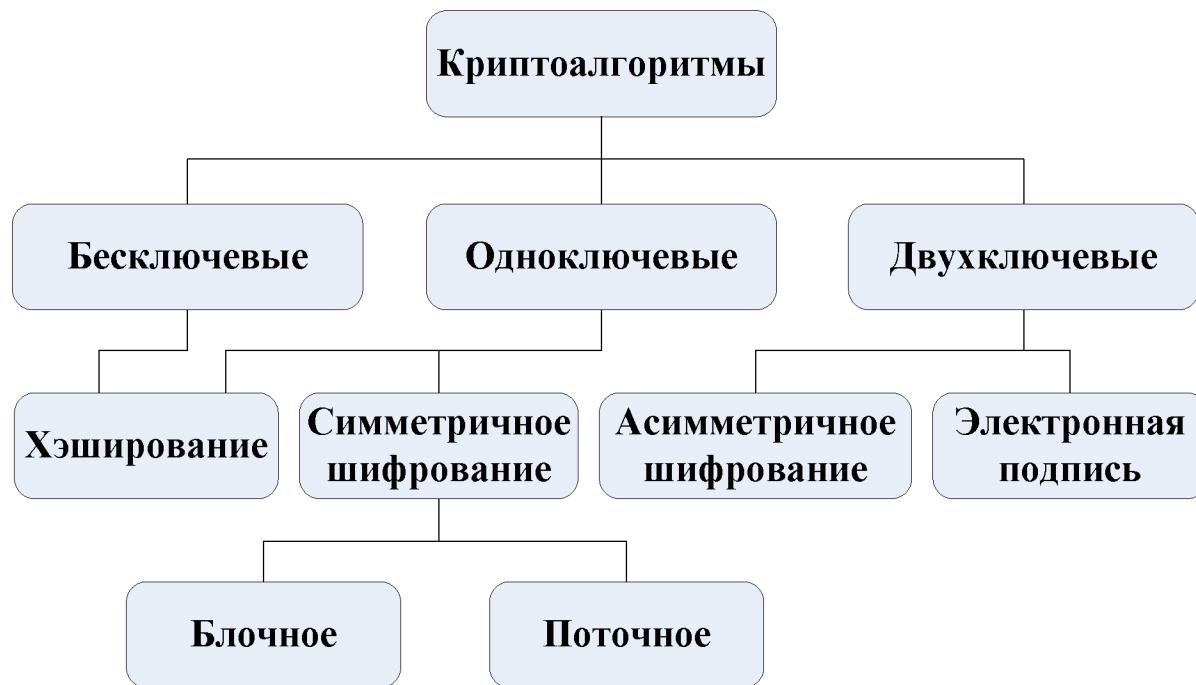


Рис. 2.2. Классификация криптоалгоритмов защиты информации

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. Хэширование может выполняться как с использованием некоторого секретного ключа, так и без него. Такое криптографическое контрольное суммирование широко используется в различных методах защиты информации, в частности для подтверждения целостности данных, если использование электронной подписи невозможно (например, из-за большой ресурсоемкости) или избыточно. Кроме того, данный метод применяется в схемах электронной подписи («подписывается» обычно хэш-значение данных, а не все данные целиком), а также в схемах аутентификации пользователей (при проверке, действительно ли пользователь является тем, за кого себя выдает).

---

*Симметричное шифрование* использует один и тот же ключ как для зашифрования, так и для расшифрования информации. Фактически оба ключа (зашифрования и расшифрования) могут и различаться, но если в каком-либо КА их легко вычислить один из другого в обе стороны, такой алгоритм однозначно относится к симметричному шифрованию.

Симметричное шифрование подразделяется на два вида: блочное и поточное, хотя стоит сразу 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» – 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, достаточных для формирования блока. Алгоритмы поточного шифрования шифруют данные побитно или посимвольно.

*Асимметричное шифрование* характеризуется применением двух типов ключей: открытого - для зашифрования информации - и секретного - для ее расшифрования. Секретный и открытый ключи связаны между собой достаточно сложным соотношением. Главное в этом соотношении - легкость вычисления открытого ключа из секретного и невозможность (за ограниченное время при реальных ресурсах) вычисления секретного ключа из открытого при достаточно большой размерности операндов.

*Электронная цифровая подпись (ЭЦП)* используется для подтверждения целостности и авторства данных. Как и в случае асимметричного шифрования, в данном методе применяются двухключевые алгоритмы с таким же простым вычислением открытого ключа из секретного и практической невозможностью обратного вычисления. Однако назначение

ключей ЭЦП совершенно иное. Секретный ключ применяется для вычисления ЭЦП, открытый ключ необходим для ее проверки. При соблюдении правил безопасного хранения секретного ключа никто, кроме его владельца, не в состоянии вычислить верную ЭЦП какого-либо электронного документа.

## 2.2. Симметричные криптосистемы шифрования

Исторически первыми появились симметричные криптографические системы. В симметричной криптосистеме шифрования используется один и тот же ключ для зашифрования и расшифрования 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. 2.3.

Данные криптосистемы характеризуются наиболее высокой скоростью шифрования, и с их помощью обеспечивается как конфиденциальность и подлинность, так и целостность передаваемой информации.

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 диске 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.

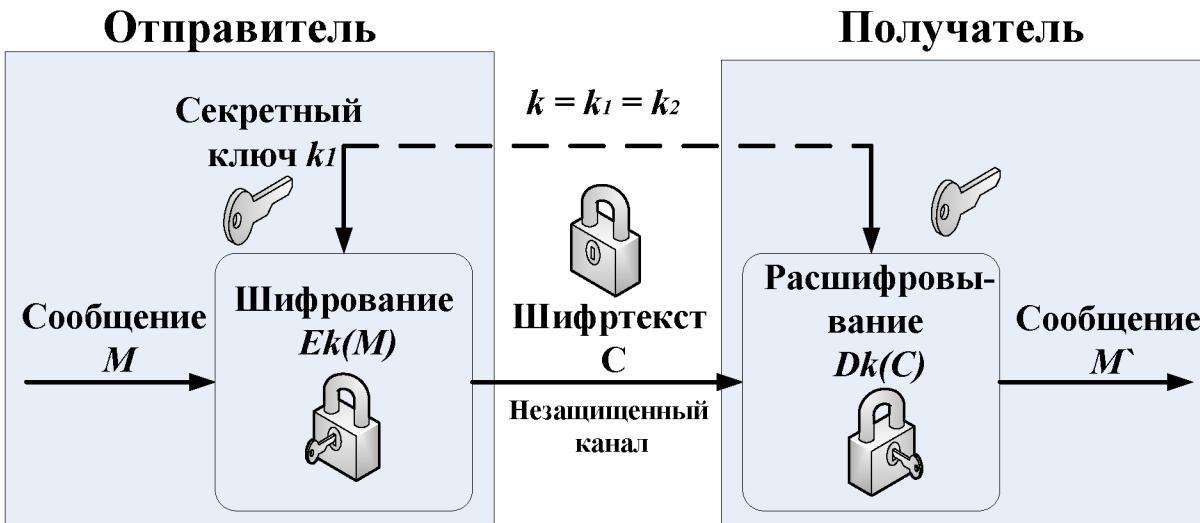


Рис. 2.3. Схема симметричной криптосистемы шифрования

Целостность данных обеспечивается присоединением к передаваемым данным специального кода (имитоприставки), вырабатываемого по секретному ключу. Имитоприставка является разновидностью контрольной суммы, т.е. некоторой эталонной характеристикой сообщения, по которой осуществляется проверка целостности последнего. Алгоритм формирования имитоприставки должен обеспечивать ее зависимость по некоторому сложному криптографическому закону от каждого бита сообщения. Проверка целостности сообщения выполняется получателем сообщения путем выработки по секретному ключу имитоприставки, соответствующей полученному сообщению, и ее сравнения с полученным значением имитоприставки. 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 предотвратить несанкционированный доступ 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.

Существуют реализации алгоритмов симметричного шифрования для абонентского шифрования данных - т.е. для отправки шифрованной информации абоненту, например, через Интернет. Использование одного ключа для всех абонентов подобной криптографической сети недопустимо по соображениям безопасности. Действительно, в случае компрометации (утери, хищения) ключа под угрозой будет находиться документооборот всех абонентов.

Характерной особенностью симметричных криптоалгоритмов является то, что в ходе своей работы они производят преобразование блока входной информации фиксированной длины и получают результирующий блок того же объема, но недоступный 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. Симметричные криптосистемы позволяют кодировать и декодировать файлы произвольной длины. 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.

Все действия, производимые блочным криптоалгоритмом над данными, основаны на том факте, что преобразуемый блок может быть представлен в виде целого неотрицательного числа из диапазона, соответствующего его разрядности. Например, 32-битный блок данных можно интерпретировать как число из диапазона 0...4294967295. Кроме того, блок, разрядность которого представляет собой «степень двойки», можно трактовать как сцепление нескольких независимых неотрицательных чисел из меньшего диапазона (указанный выше 32-битный блок можно также представить в виде сцепления двух независимых 16-битных чисел из диапазона 0...65535 или в виде сцепления четырех независимых 8-битных чисел из диапазона 0...255).

**Особенности применения алгоритмов симметричного шифрования.** Алгоритмы симметричного шифрования используют ключи относительно небольшой длины и могут быстро шифровать большие объемы данных. При симметричной методологии шифрования отправитель и получатель применяют для осуществления процессов шифрования и расшифрования сообщения один и тот же секретный ключ. Алгоритмы симметричного шифрования строятся исходя из предположения, что зашифрованные данные не сможет прочитать никто из тех, кто не обладает ключом для их расшифрования. Если ключ не был скомпрометирован, то при расшифровании автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, позволяющий расшифровать информацию.

Алгоритмы симметричного шифрования применяются для абонентского шифрования данных – т.е. для шифрования информации,

предназначенной для отправки кому-либо, например, через Интернет. Использование только одного секретного ключа для всех абонентов сети, конечно, недопустимо по соображениям безопасности: в случае компрометации (утери, хищения) ключа под угрозой будет находиться документооборот всех абонентов сети.

### 2.3. Асимметричные криптосистемы шифрования

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

- *открытый ключ*  $K$ : используется для шифрования информации, вычисляется из секретного ключа  $k$ ;
- *секретный ключ*  $k$ : используется для расшифрования 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 еще двухключевыми криптографическими системами или криптосистемами с открытым ключом.

Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом показана на рис. 2.4.

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, он должен быть надежно защищен от несанкционированного доступа (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:

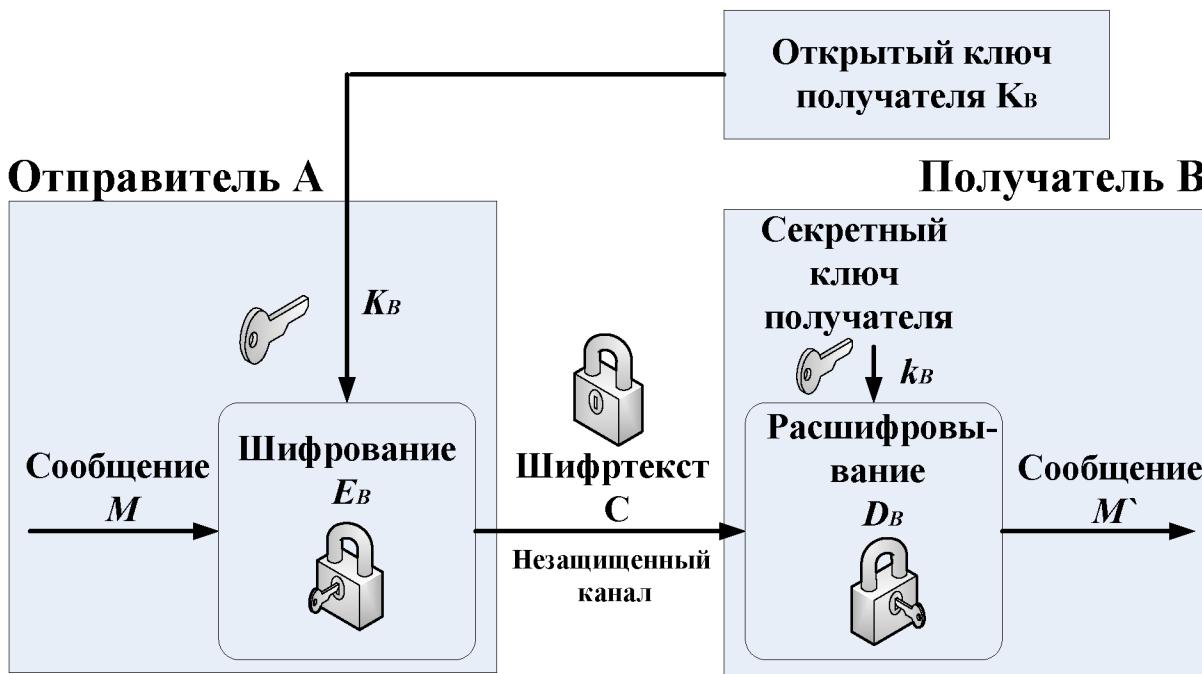


Рис. 2.4. Обобщенная схема асимметричной криптосистемы шифрования

1. Подготовительный этап:

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

2. 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.

Отметим характерные особенности асимметричных криптосистем:

1. Открытый ключ  $K_B$  и криптограмма  $C$  могут быть отправлены по незащищенным каналам, т. е. противнику известны  $K_B$  и  $C$ .

## 2. Алгоритмы шифрования и расшифрования

$$E_B : M \rightarrow C$$

$$D_B : C \rightarrow M$$

являются открытыми.

Сформулированы требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы:

1. Вычисление пары ключей ( $K_B, k_B$ ) получателем  $B$  на основе начального условия должно быть простым.
2. Отправитель  $A$ , зная открытый ключ  $K_B$  и сообщение  $M$ , может легко вычислить криптомограмму

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

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

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

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.

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.

Асимметричные криптографические системы обладают следующими важными преимуществами перед симметричными криптосистемами:

– в асимметричных крипtosистемах 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 квадратическая зависимость числа ключей от числа пользователей; в асимметричной крипtosистеме количество используемых ключей связано с количеством абонентов линейной зависимостью (в системе из  $N$  пользователей используются  $2 \times N$  ключей), а не квадратичной, как в симметричных системах;

– асимметричные крипtosистемы позволяют реализовать протоколы взаимодействия сторон, которые не доверяют друг другу, поскольку при использовании асимметричных крипtosистем закрытый ключ должен быть известен только его владельцу.

Однако у асимметричных крипtosистем существуют и недостатки:

– на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах функций;

– по сравнению с симметричным шифрованием асимметричное существенно медленнее, поскольку при шифровании и расшифровании используются весьма ресурсоемкие операции. По этой же причине реализовать аппаратный шифратор с асимметричным алгоритмом существенно сложнее, чем реализовать аппаратно симметричный алгоритм;

– необходимо защищать открытые ключи от подмены.

## 2.4. Функция 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  $h()$  принимает в качестве аргумента сообщение (документ)  $M$  произвольной длины и возвращает хэш-значение (хэш)  $H = h(M)$  фиксированной длины (рис. 2.5).

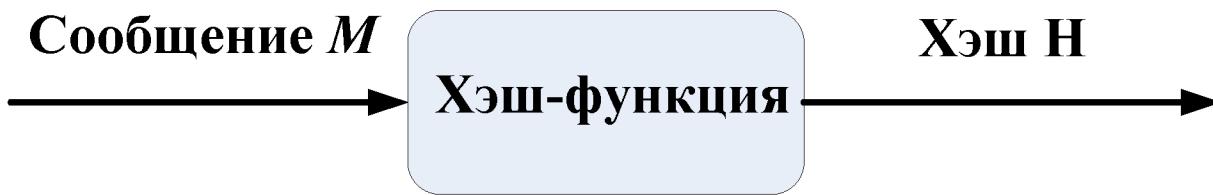


Рис. 2.5. Схема формирований хэша  $H = h(M)$

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 позволяет сжать подписываемый документ  $M$  до 128 и более битов (в частности, 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 ко всевозможным изменениям в тексте  $M$ , таким как вставки, перестановки и т.п.

5. Хэш-функция должна быть односторонней, 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

предусмотреть способ 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.

Функция хэширования может использоваться для обнаружения изменений сообщения, т.е. она 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 электронной цифровой подписи.

Хэш-функции широко используются также в целях 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 – расшифрованием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования на основе хэш-функции.

## 2.5. Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП) используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. При таком обмене электронными документами существенно снижаются затраты на обработку и хранение документов, ускоряется 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* посыпает документ абоненту *B* от имени абонента *A*;

- *ренегатство* – абонент  $A$  заявляет, что не посыпал 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  $A$  посыпал абоненту  $B$ .

Эти виды действий могут нанести существенный ущерб объектам критических инфраструктур иностранных государств и частным лицам, применяющим в своей деятельности компьютерные информационные технологии.

**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.

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 – 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  $K_A$  рассыпается 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. 2.6).

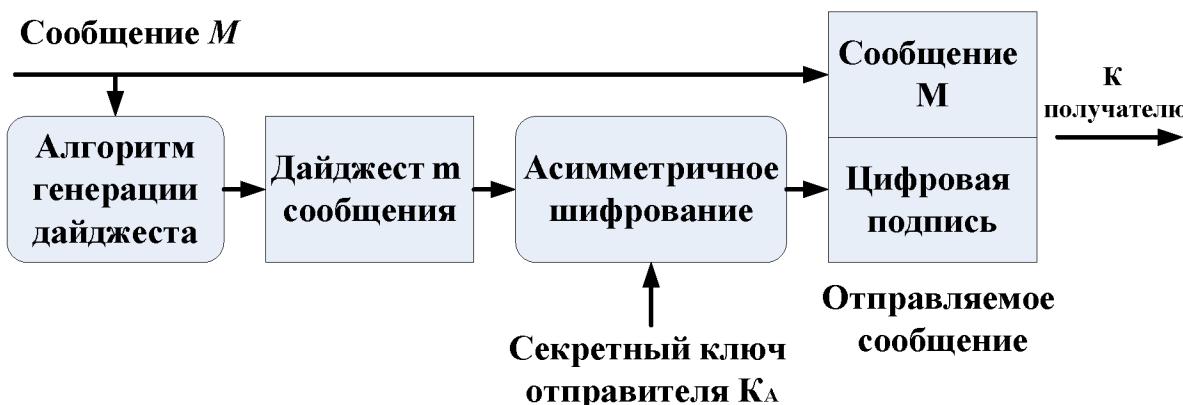


Рис. 2.6. Схема формирования электронной цифровой подписи

Хэш-функция служит для сжатия исходного подписываемого текста  $M$  в дайджест – относительно короткое число, состоящее из фиксированного небольшого числа битов и характеризующее весь текст  $M$  в целом. Далее отправитель  $A$  шифрует дайджест  $M$  своим секретным ключом  $k_A$ . Поручаемая 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 отправителя  $K_A$  этого сообщения (рис. 2.7).

При проверке ЭЦП абонент  $B$  – получатель сообщения  $M$  –

расшифровывает принятый дайджест  $m$  открытым ключом отправителя  $A$ . Кроме того, получатель сам вычисляет с помощью хэш-функции  $h(M)$  дайджест  $m'$  принятого сообщения  $M$  и сравнивает его с расшифрованным. Если эти два дайджеста  $m$  и  $m'$  совпадают, то 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 несанкционированного доступа. Секретный ключ ЭЦП аналогично ключу симметричного шифрования, рекомендуется хранить на персональном ключевом носителе в защищенном виде.

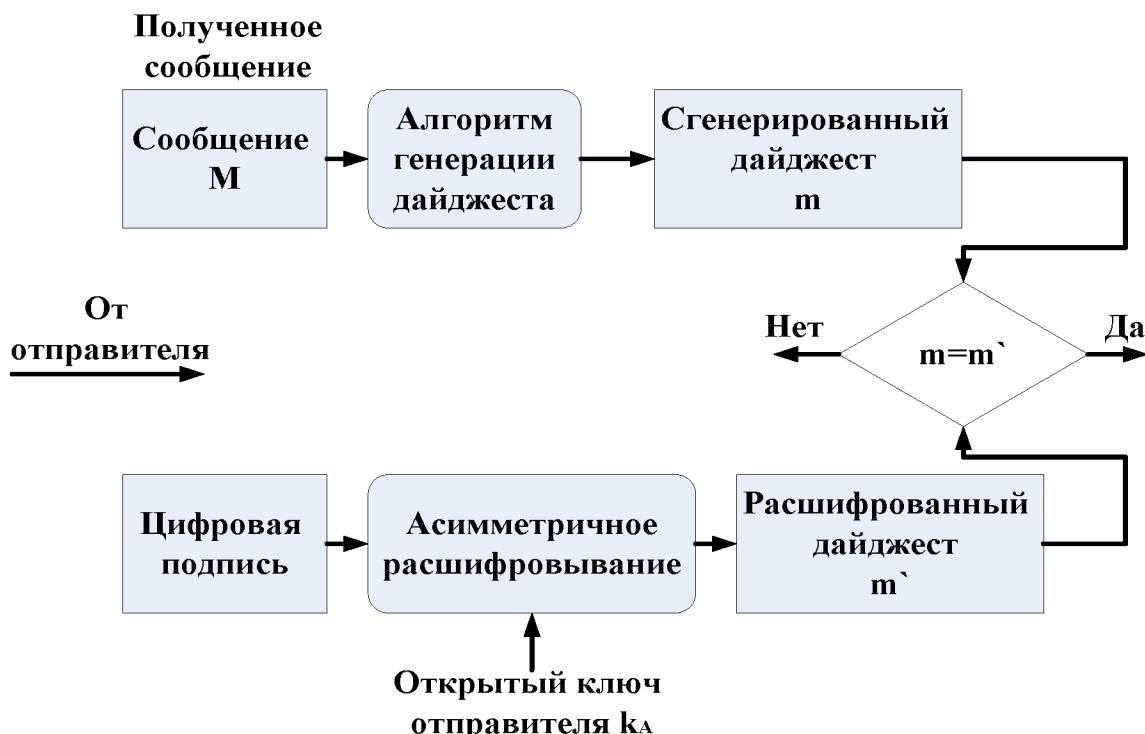


Рис. 2.7. Схема проверки электронной цифровой подписи

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.

## Глава 3. Идентификация, аутентификация и управление доступом

Применение открытых каналов передачи данных создает потенциальные возможности для реализации угроз в области ИТ. 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.

### 3.1. Аутентификация, авторизация и администрирование действий пользователей в компьютерных сетях

С каждым зарегистрированным в компьютерной сети субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов, обозначающие данный субъект. Эту информацию называют идентификатором субъекта. Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (законным) пользователем. Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию и аутентификацию.

*Идентификация* – это процедура распознавания пользователя по его идентификатору, присвоенному данному пользователю ранее и занесенному в базу данных в момент его регистрации в качестве легального пользователя системы. Эта функция выполняется в первую очередь, 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* – процедура проверки подлинности входящего в систему объекта (пользователя, процесса или устройства), предъявившего свой идентификатор. 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, неизвестную 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* – процедура предоставления пользователю (процессу или устройству) определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации, иными словами, авторизация устанавливает сферу действия пользователя и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в этой системе могут быть нарушены.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя. Задачи аутентификации, авторизации и администрирования тесно связаны между собой. Для краткости их взаимосвязанное решение называют решением задач AAA.

*Администрирование* – это процесс управления доступом пользователей к ресурсам системы.

В настоящее время для решения задач идентификации, аутентификации, авторизации и администрирования используют подсистему управления идентификацией и доступом IAM (Identity and Access Management).

Необходимый уровень аутентификации определяется требованиями безопасности, которые установлены в организации. Общедоступные веб-серверы могут разрешить анонимный или гостевой доступ к информации. Финансовые транзакции могут потребовать строгой 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 – в процессе установления соединения абонентов. Термин «соединение» указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры является 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 следующие категории:

–на основе знания чего-либо. Примерами могут служить пароль, персональный идентификационный PIN-код, а также секретные и открытые ключи, знание которых демонстрируется в протоколах типа запрос-ответ;

–на основе обладания чем-либо. Обычно это магнитные карты, смарт-карты, сертификаты, USB-ключи или USB-токены (token (англ.) – опознавательный признак, маркер);

–на основе каких-либо неотъемлемых характеристик. Эта категория включает методы, базирующиеся на проверке биометрических характеристик пользователя (голос, радужная оболочка и сетчатка глаза, отпечатки пальцев, геометрия ладони и др.). В данной категории не используются криптографические методы и средства. Аутентификация на основе биометрических характеристик применяется для контроля доступа в помещения либо к какой-либо технике.

Пароль – это то, что знает пользователь и что также знает 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 посыпает 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 появился ряд коммерческих инфраструктур управления открытыми ключами РКИ для распространения сертификатов открытых ключей. Пользователи могут получить сертификаты различных уровней.

Процессы аутентификации можно также классифицировать по уровню обеспечиваемой безопасности. В соответствии с данным подходом процессы аутентификации разделяются на следующие типы:

- простая аутентификация, использующая пароли;
- строгая аутентификация на основе использования многофакторных проверок и криптографических методов;
- 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.

Основными атаками на протоколы аутентификации являются:

–*маскарад (Impersonation)*. Пользователь пытается выдать 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 следующие приемы:

–использование механизмов типа запрос-ответ, меток времени, случайных чисел, идентификаторов, цифровых подписей;

–привязка результата аутентификации к последующим действиям пользователей в рамках системы. Примером подобного подхода может служить осуществление в процессе аутентификаций обмена секретными сеансовыми ключами, которые применяются при дальнейшем взаимодействии пользователей;

–периодическое выполнение процедур аутентификации в рамках уже установленного сеанса связи и т.п.

### **3.2. Аутентификация на основе многоразовых паролей**

В современных операционных системах предусматривается централизованная служба аутентификации, которая выполняется одним из серверов сети и использует для своей работы базу данных. В этой базе данных хранятся учетные данные о пользователях сети. В эти учетные данные наряду с другой информацией включены идентификатор (login) и пароль (password) пользователя.

Процедуру простой аутентификации пользователя в сети можно представить следующим образом. При попытке логического входа пользователя в сеть он набирает на клавиатуре компьютера свои идентификатор и пароль. Эти данные поступают для обработки на сервер аутентификации. В базе данных учетных записей пользователей, хранящейся

на сервере аутентификации, по идентификатору пользователя находится соответствующая запись, из нее извлекается эталонное значение пароля и сравнивается с тем паролем, который ввел пользователь. Если введенная пользователем пара login/password совпала с эталонной, то аутентификация прошла успешно, пользователь получает права на ресурсы сети, которые определены его статусом.

Схема простой аутентификации с использованием пароля показана на рис. 3.1.

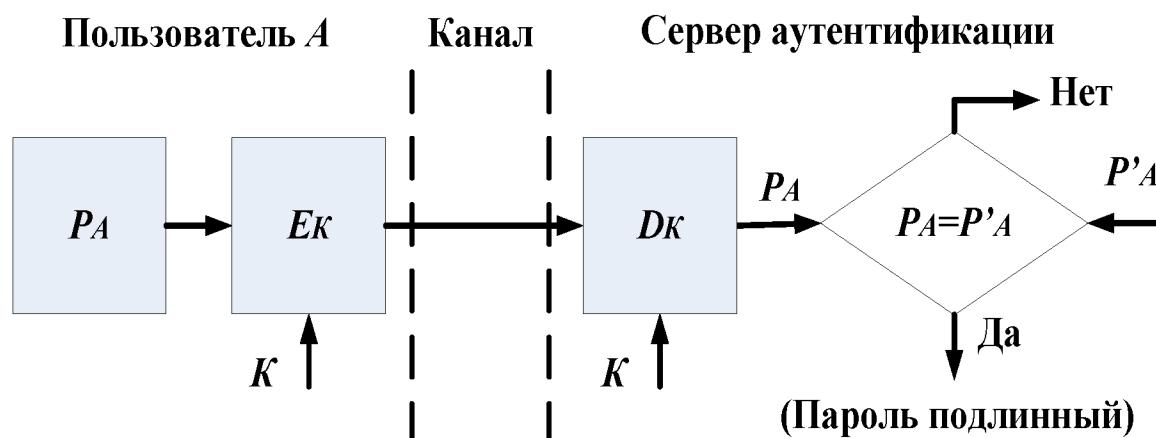


Рис. 3.1. Простая аутентификация с использованием пароля

Чтобы защитить пароль, его нужно зашифровать перед пересылкой по незащищенному каналу. Для этого в схему включены средства шифрования  $E_K$  и расшифрования  $D_K$ , управляемые разделяемым секретным ключом  $K$ . Проверка подлинности пользователя основана на сравнении присланного пользователем пароля  $P_A$  и исходного значения  $P'_A$ , хранящегося в сервере аутентификации. Если значения  $P_A$  и  $P'_A$  совпадают, то пароль  $P_A$  считается подлинным, а пользователь  $A$  – законным.

Системы простой аутентификации на основе многоразовых паролей имеют пониженную стойкость, поскольку в них выбор аутентифицирующей информации происходит из относительно небольшого множества слов. Срок действия многоразового пароля должен быть определен в политике безопасности организации, и такие пароли должны регулярно изменяться. Выбирать пароли нужно так, чтобы они были трудны для угадывания и не присутствовали в словаре.

Схемы аутентификации, основанные на многоразовых паролях, не

---

обладают достаточной безопасностью. Такие пароли можно перехватить, разгадать, подсмотреть или просто украсть.

### 3.3. Аутентификация на основе одноразовых паролей

Как уже отмечалось, схемы аутентификации, основанные на традиционных многоразовых паролях, не обладают достаточной безопасностью. Более надежными являются процедуры аутентификации на основе одноразовых паролей OTP (One Time Password).

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 кто-то перехватил его, пароль окажется бесполезным. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от угроз извне.

Одноразовые пароли генерируются с помощью OTP-токена. Для этого используется секретный ключ пользователя, размещенный как внутри OTP-токена, так и на сервере аутентификации.

Для того чтобы получить доступ к необходимым ресурсам, пользователь должен ввести пароль, созданный с помощью OTP-токена. Этот пароль сравнивается со значением, сгенерированным на сервере аутентификации, после чего выносится решение о предоставлении доступа. Преимуществом такого подхода является то, что пользователю не требуется соединять токен с компьютером (в отличие от вышеперечисленных типов идентификаторов).

Однако количество приложений ИТ-безопасности, которые поддерживают возможность работы с OTP-токенами, намного меньше, чем для смарт-карт и USB-токенов. Недостатком OTP-токенов является ограниченное время жизни этих устройств (три-четыре года), так как автономность работы предполагает использование батарейки.

Обычно системы аутентификации с одноразовыми паролями используются для проверки удаленных пользователей.

### 3.4. Биометрическая аутентификация пользователей

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, персональный идентификатор, секретный ключ и т.п.). Привычные системы аутентификации не всегда удовлетворяют современным требованиям в области информационной безопасности, особенно если речь идет об ответственных приложениях (онлайновые финансовые приложения, доступ к удаленным базам данных и т.п.).

В последнее время все большее распространение получает биометрическая аутентификация пользователя, позволяющая уверенно аутентифицировать потенциального пользователя путем изменения физиологических параметров и характеристик человека, особенностей его поведения. Использование решений, основанных на биометрической технологии, позволяет в ряде случаев улучшить положение дел в области аутентификации.

Отметим основные достоинства биометрических методов аутентификации пользователя по сравнению с традиционными:

- высокая степень достоверности аутентификации по биометрическим признакам из-за их уникальности;
- неотделимость биометрических признаков от дееспособной личности;
- трудность фальсификации биометрических признаков.

В качестве биометрических признаков, которые активно используются при аутентификации потенциального пользователя, можно выделить следующие:

- 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 образец законного пользователя. Биометрический образец обрабатывается системой для получения информации в виде ЭИП (эталонного идентификатора пользователя или эталона для проверки) ЭИП представляет собой числовую последовательность, при этом сам образец невозможно восстановить из эталона.

Эталонный идентификатор пользователя хранится системой в электронной форме и используется для проверки идентичности каждого, кто выдает себя за соответствующего законного пользователя. Снятая в процессе идентификации характеристика пользователя сравнивается с ЭИП. Поскольку эти два значения (полученное при попытке доступа и ЭИП) полностью никогда не совпадают, то для принятия положительного решения о доступе степень совпадения должна превышать определенную настраиваемую пороговую величину. В зависимости от степени совпадения или несовпадения совокупности предъявленных признаков с ЭИП лицо, их предъявившее, признается законным пользователем (при совпадении) или нет (при несовпадении).

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».

Наибольшее число биометрических систем в качестве параметра идентификации использует отпечатки пальцев (дактилоскопические системы). Отпечаток пальца считается одним из наиболее устойчивых идентификационных признаков (не изменяется со временем, при повреждении кожного покрова идентичный папиллярный узор полностью восстанавливается, при сканировании не вызывает дискомфорта у пользователя).

**Дактилоскопические системы аутентификации.** Одной из основных причин широкого распространения таких систем является наличие больших банков данных по отпечаткам пальцев. Основными пользователями подобных систем во всем мире 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, который пользователь предоставляет системе.

Основными элементами дактилоскопической системы аутентификации являются:

- сканер;
- ПО идентификации, формирующее идентификатор пользователя;

–ПО аутентификации, производящее сравнение отсканированного отпечатка пальца с имеющимися в базе данных «паспортами» пользователей.

Ряд производителей 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 сканеру, ключ удостоверяет его личность. Комбинация биометрических устройств и смарт-карт является удачным решением, повышающим надежность процессов аутентификации и авторизации.

**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 девятиразрядный образец для дальнейших сравнений. Этот образец может быть сохранен локально, на индивидуальном сканере ладони либо в централизованной базе данных.

По уровню доходов устройства сканирования формы ладони занимают второе место среди биометрических устройств, однако 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.

**Системы аутентификации по лицу и голосу** являются наиболее

---

доступными 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 используют собственные математические алгоритмы для идентификации пользователей.

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 около 15% между запрашиваемым изображением и образцом, который находится в базе данных, 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 уникальные для каждого человека особенности голоса, как высота, модуляция и частота звука. Эти показатели определяются физическими характеристиками голосового тракта и уникальны для каждого человека. Распознавание голоса уже применяется вместо набора номера в некоторых системах. Такой вид распознавания голоса отличается от распознавания речи. В то время как технология распознавания речи интерпретирует то, что говорит абонент, технология распознавания голоса абонента подтверждает личность говорящего.

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 надежными среди всех биометрических систем. Такие средства идентификации 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.

## Глава 4. Безопасность операционных систем

Проблема защиты от несанкционированных действий при взаимодействии с внешними сетями может быть успешно решена только на основе комплексной защиты корпоративных информационных систем. Защищенные операционные системы относятся к базовым средствам многоуровневой комплексной защиты компьютерных информационных сетей.

### 4.1. Угрозы безопасности операционной системы

Большинство программных средств защиты информации являются прикладными программами. Для их выполнения требуется поддержка операционной системы (ОС). Окружение, в котором функционирует ОС, называется *доверенной вычислительной базой* (ДВБ). ДВБ включает в себя полный набор элементов, обеспечивающих информационную безопасность: операционную систему, программы, сетевое оборудование, средства физической защиты и даже организационные процедуры. Краеугольным камнем этой пирамиды является защищенная операционная система. Без нее доверенная вычислительная база оказывается построенной на песке.

Организация эффективной и надежной защиты операционной системы невозможна без предварительного анализа возможных угроз ее безопасности. Угрозы безопасности операционной системы существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается в системе, и т.д. Например, если операционная система используется для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом (НСД) к файлам. Если же операционная система используется как платформа провайдера интернет-услуг, очень опасны атаки на сетевое программное обеспечение операционной системы.

Угрозы безопасности операционной системы можно классифицировать по различным аспектам их реализации.

Классификация угроз *по цели атаки*:

- несанкционированное чтение информации;

- несанкционированное изменение информации;
- несанкционированное уничтожение информации;
- полное или частичное разрушение операционной системы.

Классификация угроз *по принципу воздействия на операционную систему*:

- использование известных (легальных) каналов получения информации, например угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно – разрешен доступ пользователю, которому согласно политике безопасности доступ должен быть запрещен;
- использование скрытых каналов получения информации, например, угроза использования специальными службами недокументированных возможностей операционной системы;
- создание новых каналов получения информации с помощью программных закладок.

Классификация угроз *по типу используемой злоумышленником уязвимости защиты*:

- неадекватная политика безопасности, в том числе ошибки администратора системы;
- ошибки и недокументированные возможности программного обеспечения операционной системы, в том числе и так называемые ляжи – случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты;
- ранее внедренная программа закладка.

Классификация угроз 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.

Операционная система может подвергнуться следующим типичным

атакам:

– сканирование файловой системы. Подготовленный агент просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате заинтересованное лицо получает доступ к информации, который должен быть ему запрещен;

– подбор пароля. Существует 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.);

– кражи ключевой информации. Агент 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;

– сборка мусора. Во многих операционных системах информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый мусор). Агент восстанавливает эту информацию, просматривает ее и копирует интересующие его фрагменты;

– превышение 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;

– программные закладки. Программные закладки, внедряемые в операционные системы, не имеют существенных отличий от других классов программных закладок;

– жадные программы – 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 операционной системы.

## 4.2. Понятие защищенной операционной системы

Операционную систему называют *зашитенной*, если она предусматривает средства защиты от основных классов угроз. Защищенная операционная система обязательно должна содержать средства разграничения доступа пользователей к своим ресурсам, а также средства проверки подлинности пользователя, начинаящего работу с операционной системой. Кроме того, защищенная операционная система должна содержать средства противодействия случайному или преднамеренному выводу операционной системы из строя.

Если операционная система предусматривает защиту не от всех основных классов угроз, а только от некоторых такую ОС называют *частично защищенной*.

**Подходы к построению защищенных операционных систем.** Существует два основных подхода к созданию защищенных операционных систем – 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 операционная система, на нее устанавливают антивирусный пакет, систему шифрования, систему регистрации действий пользователей и т.д.

При применении фрагментарного подхода подсистема защиты операционной системы 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 операционную систему на этапе проектирования архитектуры операционной системы 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 операционной системы, что не позволяет специалистам компьютерной разведки отключать защитные функции системы. При фрагментарном подходе такая организация подсистемы защиты невозможна.

Как правило, подсистему защиты операционной системы, 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 операционной системы 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 операционной системы*, особенно ее подсистемы защиты. Такой контроль удобно организовать, если операционная система 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 операционной системы, а также на изменения в конфигурации операционной системы, установку и удаление прикладных программ.

3. *Осведомление 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 операционной системы, было труднее замаскировать свои несанкционированные действия.

В конкретных ОС могут потребоваться и другие административные меры защиты информации.

**Адекватная политика безопасности.** Выбор и поддержание адекватной политики безопасности являются одной из наиболее важных задач администратора операционной системы. Если принятая в ОС политика безопасности неадекватна, это может привести к несанкционированному доступу заинтересованных лиц 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 несанкционированного доступа, 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 операционной системе защищенных функций, тем больше времени и средств нужно тратить на поддержание защиты;

- подсистема защиты операционной системы, как и любой другой программный пакет, потребляет аппаратные ресурсы компьютера. Чем сложнее устроены защитные функции операционной системы, 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 операционной системы.

---

Чрезмерно жесткая политика безопасности может привести к трудно выявляемым ошибкам и сбоям в процессе функционирования операционной системы и даже к краху ОС.

*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 операционной системы 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 несанкционированного доступа 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 операционных систем не существует. Для оценки защищенности операционных систем используются стандарты, разработанные для компьютерных систем вообще. Как правило, сертификация операционной системы по некоторому классу защиты сопровождается составлением требований к адекватной политике безопасности, при безусловном выполнении которой защищенность конкретного экземпляра операционной системы будет соответствовать требованиям соответствующего класса защиты.

## Глава 5. Современные подходы к обеспечению анонимности работы в сети Интернет

В настоящее время с учетом все возрастающей роли глобальной коммуникационной сети Интернет и расширяющимися возможностями по обеспечению доступа к ней, актуальным вопросом является обеспечение анонимности при удаленном подключении к сетевым ресурсам.

В настоящее время активно применяется ряд схем анонимной работы в Интернет.

Отметим, что существует два аспекта анонимности:

- «социальная (персональная) анонимность» - это то, что человек сам осознанно или неосознанно рассказывает о себе в Интернет.
- «техническая (технологическая) анонимность», когда утечка деанонимизирующих данных связана с используемыми при работе в Интернет техническими средствами и программными приложениями.

В данной главе рассматриваются способы, обеспечивающие именно техническую анонимность.

Наиболее распространенные из них базируются на применении следующих аппаратно-технических средств:

- прокси-серверы;
- виртуальные частные сети VPN;
- сеть анонимизации TOR;
- сеть анонимизации I2P.

### 5.1. Прокси-серверы

Прокси-сервер (от англ. Proxy - представитель, уполномоченный) представляет собой посредника между клиентом (пользователем) и сервером. С технической точки зрения прокси-сервер – это комплекс программ, позволяющий клиентам выполнять косвенные запросы к различным ресурсам Интернета. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс, расположенный на другом сервере. Затем прокси-сервер подключается к указанному серверу и получает ресурс у него. В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-

---

сервером для достижения определенных целей. Также прокси-сервер позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять его анонимность.

С точки зрения обеспечения анонимности существуют следующие типы прокси-серверов:

- HTTP(веб)-прокси-серверы. Такие серверы «пропускают» через себя только HTTP-трафик, по умолчанию добавляя в передаваемый трафик данные о применении прокси;

- CGI-прокси или «анонимайзеры», которые представляют собой web-сервер с формой, где клиент вводит адрес нужного сайта. После чего открывается страница запрошенного ресурса, но в адресной строке браузера виден адрес CGI-прокси. CGI-прокси, как и любой web-сервер может использовать закрытый протокол HTTPS (HyperText Transfer Protocol Secure – расширение протокола HTTP, поддерживающее шифрование) для защиты канала связи между собой и клиентом.

- SOCKS-прокси-серверы. В отличие от HTTP-прокси-серверов, SOCKS передает всю информацию, ничего не добавляя от себя. Протокол SOCKS находится на сеансовом уровне эталонной модели взаимодействия открытых систем – OSI. Этим достигается независимость от высокоуровневых протоколов, таких как HTTP, FTP, POP3 и др., что и позволяет SOCKS пропускать через себя весь трафик, а не только HTTP;

Существуют разные версии SOCKS:

- SOCKS4. В протоколе указывается IP-адрес для подключения через прокси. Для обращения по доменным именам ресурсов необходимо в обход прокси осуществить DNS-преобразование имени в IP-адрес. Это может привести к деанонимизации, так как интернет-провайдер видит DNS-запросы в открытом виде. Данная уязвимость называется DNS-leaks.

- SOCKS4a. Является расширением SOCKS4. Главное отличие состоит в том, что SOCKS4a-сервер принимает от клиента только DNS-имя адресата, а не его IP-адрес.

- SOCKS5. Também является расширением SOCKS4. Сервер SOCKS5 поддерживает UDP, IPv6, авторизацию и пр. Однако, некоторые приложения, поддерживающие SOCKS5, могут сами получать IP-адрес адресата до того, как

обратятся к SOCKS5-прокси, что также может привести к утечке DNS-запросов.

Альтернативным методом проксирования является построение SSH-туннелей (Secure SHell – «безопасная оболочка»). Данный протокол позволяет построить закрытый канал передачи данных и в совокупности с протоколом SOCKS обеспечивает возможность доступа к ресурсам через посредника с использованием шифрования.

В случае осуществления контроля входа и выхода у прокси-сервера возможно однозначное последовательное сопоставление клиента и ресурса, который он посещает. Классические прокси-серверы не имеют криптографических средств обеспечения анонимности, а, следовательно, и бескомпроматности.

Схема работы прокси-сервера (цепочки серверов) представлена на рис. 5.1.



Рис. 5.1. Схема работы прокси-сервера

К положительным характеристикам прокси-серверов можно отнести их дешевизну (существует множество бесплатных прокси-серверов).

Отрицательными особенностями использования прокси-серверов являются:

- нет никаких гарантий, что на прокси-сервере не ведутся журналы обращений, и он не является приманкой со стороны специальных служб;
- для HTTP-прокси надо фильтровать HTTP-заголовки от различных деанонимизирующих признаков (тип и версия операционной системы и браузера, установленный язык в ОС, региональные признаки и пр.);
- протоколы прокси (HTTP, SOCKS) не поддерживают шифрование между HTTP/SOCKS-прокси и клиентом. А прокси с поддержкой SSL (Secure

Sockets Layer – уровень защищенных соединений) означает лишь то, что клиент может работать с https-ресурсами (шифрованными web ресурсами);

- многие протоколы, например, протокол передачи файлов FTP, не поддерживают прокси;
- необходимость настройки прокси-сервера для каждого приложения, либо использование отдельных программ-соксификаторов (например, Proxifier).

## 5.2. Виртуальные частные сети (VPN/SSH)

VPN (англ. Virtual Private Network - виртуальная частная сеть) - обобщённое название технологии, позволяющей обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что организация связи осуществляются по сетям с неизвестным уровнем доверия (Интернет), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

Говоря о технологии VPN, в данной статье подразумевается также и технология SSH-туннелирования. Эта технология предполагает «проброс» соединения через сервер с настроенным сервисом SSH (англ. Secure SHell – защищенный протокол управления сервером). Несмотря на некоторые различия, основной принцип анонимизации работы в Интернет, содержащийся в этих технологиях, одинаков.

Схема работы VPN показана на рисунке 5.2.

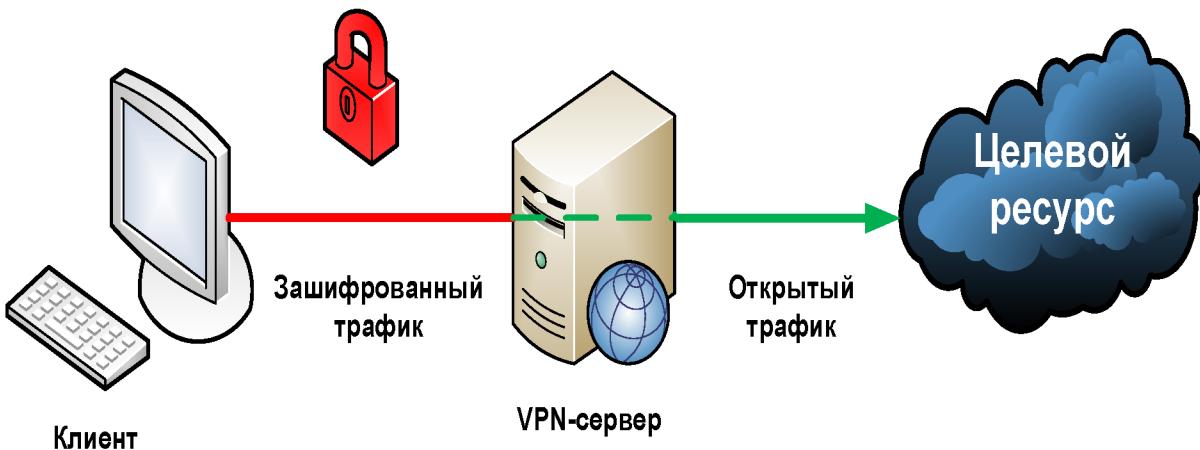


Рис. 5.2. Схема работы VPN

В настоящее время коммерческими провайдерами предлагаются следующие сервисы VPN:

- PPTP - используется наиболее широко, быстрый, легко настраивается, однако считается «наименее защищённым» по сравнению с остальными;
- L2TP + IPSec. L2TP обеспечивает транспорт, а IPSec отвечает за шифрование. Данная связка имеет более сильное шифрование, чем PPTP, устойчива к уязвимостям PPTP, обеспечивает также целостность сообщений и аутентификацию сторон;
- OpenVPN - безопасный, открытый, а, следовательно, распространённый, позволяет обходить многие блокировки, но требует отдельного программного клиента;
- SSTP - такой же безопасный, как и OpenVPN, не требует отдельного клиента, однако сильно ограничен в платформах. Реализован только в ОС Windows Vista SP1, Windows 7, Windows 8.

Отдельно стоит отметить сервисы, предоставляющие «DoubleVPN», когда перед тем, как выйти в Интернет, трафик проходит два разных VPN-сервера в разных странах, или даже «QuadVPN», когда используется четыре сервера, которые пользователь может выбрать сам и расположить в произвольном порядке.

Положительная особенность VPN/SSH состоит в быстром и удобном применении по сравнению с прокси-серверами (не надо отдельно настраивать приложения).

Отрицательный момент VPN/SSH в том, что нужно доверять VPN/SSH-серверу/провайдеру или приобретать и настраивать собственный сервер.

Стоит отметить, что большинство тематических дополнений для браузеров и «программ для анонимности» используют в своей основе именно прокси-серверы и VPN-серверы для скрытия ip-адреса клиента.

### 5.3. Сеть анонимизации TOR

TOR (The Onion Router - луковая маршрутизация) представляет собой систему маршрутизаторов, в которой пользователь (клиент) соединяется с Интернетом через цепочку узлов. Как правило, цепочка состоит из трех узлов, каждому из них неизвестны адреса клиента и ресурса одновременно. Кроме того, TOR шифрует сообщения отдельно для каждого узла, а открытый трафик виден только выходному роутеру.

Система TOR была создана в «Центре высокопроизводительных вычислительных систем» Исследовательской лаборатории Военно-морских сил США совместно с управлением перспективных исследований министерства обороны США (DARPA). В 2002 году эту разработку рассекретили, а исходные тексты программ были переданы независимым разработчикам, которые, после внесения в тексты программ ряда изменений, опубликовали исходный код под свободной лицензией, чтобы все желающие могли проверить его на отсутствие ошибок и недекларируемых (скрытых) возможностей.

О поддержке проекта объявили ряд организаций по защите гражданских свобод, которые начали активно пропагандировать новую систему и прилагать усилия для расширения сети за счет увеличения количества промежуточных узлов сети – нодов (от англ. Node – узел).

На рис. 5.2 показана схема работы сети TOR.

Сеть TOR относится к гибридной анонимной сети с «луковичной маршрутизацией». В настоящее время существуют версии и решения TOR практически для всех современных операционных систем. Сеть TOR способна обеспечивать анонимность для сетевых сервисов. Данные сервисы в сети получили название скрытых сервисов (hidden services). Доступ к скрытым службам возможен лишь при использовании клиента TOR на стороне пользователя.

Скрытые службы доступны через специальные псевдо-домены верхнего

уровня .onion. Сеть TOR распознает эти домены и направляет информацию анонимно к скрытым службам, которые затем обрабатывают ее посредством стандартного программного обеспечения, настроенного на прослушивание только непубличных (закрытых для внешнего доступа) интерфейсов.

Доменные имена в зоне .onion генерируются на основе открытого ключа сервера и состоят из 16 цифр или букв латинского алфавита.

У скрытых сервисов TOR есть собственные каталоги сайтов, поисковые системы, электронные торговые площадки, шлюзы интернет-трейдинга, почтовые серверы, электронные библиотеки, торрент-трекеры, блог-платформы, социальные сети, файловые хостинги, облачные хранилища, службы коротких сообщений, чат-комнаты, IRC-сети, серверы SILK, XMPP и SFTP, а также многие другие ресурсы.

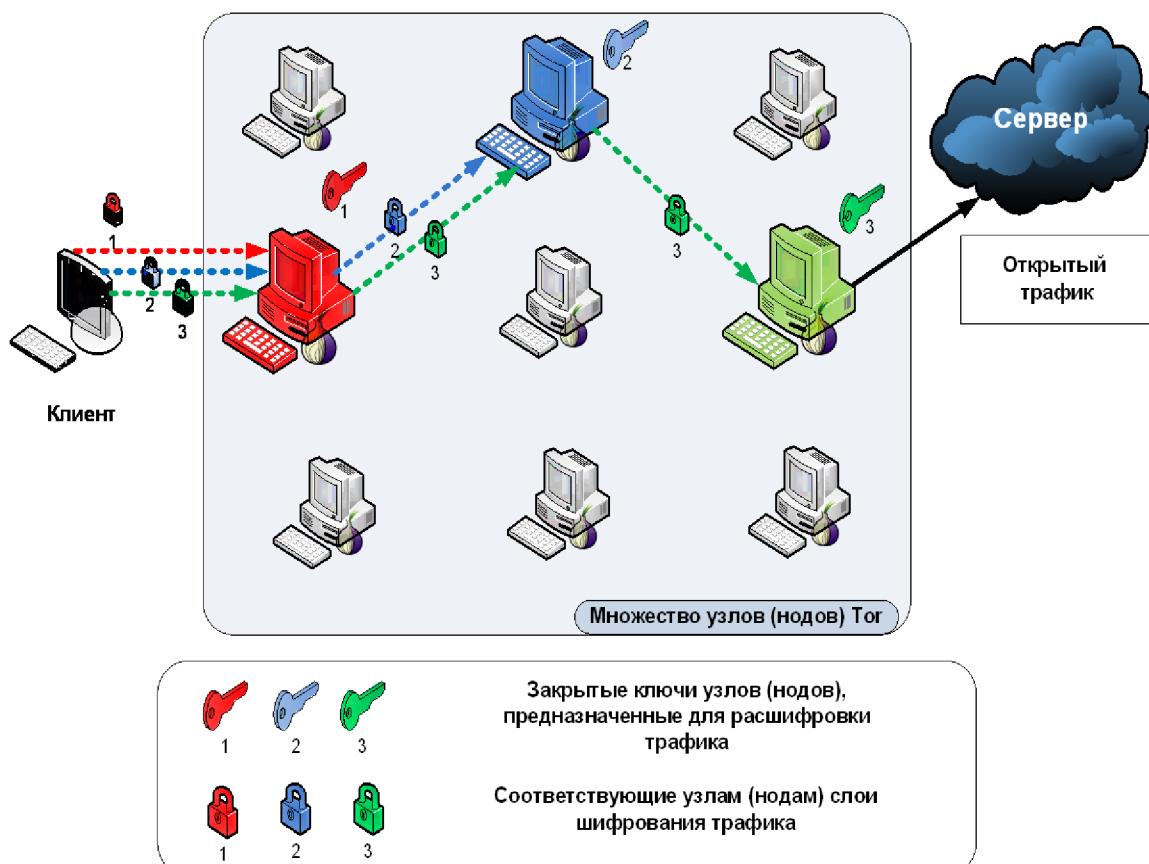


Рис. 5.2. Схема работы сети TOR

Ряд известных сайтов имеет свои зеркала среди скрытых сервисов,

---

например, The Pirate Bay, DuckDuckGo, WikiLeaks и Cryptocat. Кроме того, существуют шлюзы для доступа к скрытым сервисам непосредственно из Интернета, а также для посещения других анонимных сетей через TOR.

Скрытые сервисы TOR могут быть размещены за межсетевыми экранами, прокси-серверами и не требуют обязательного наличия публичного IP-адреса.

Как уже говорилось, принцип работы сети TOR основан на протоколе «луковичной маршрутизации» (рис. 5.3). Клиенты выбирают случайный маршрут в сети и строят цепочку, в которой каждый узел в этом маршруте знает только своего предшественника и преемника, но никаких других узлов цепочки. Трафик следует по цепочке в виде пакетов стандартного размера, с которых каждый узел снимает свое симметричное шифрование (как снятие слоя у луковицы) и передает дальше (рис. 5.4).

В качестве потокового шифра используется AES 128-бит в режиме CBC, все байты вектора инициализации IV устанавливаются в 0. В качестве шифра с открытым ключом используется RSA 1024 бит и фиксированная экспонента 65537. В качестве системы определения общего ключа используется схема Диффи-Хеллмана с 1024-битным простым числом и генератором 2. В качестве хеш-функции используется SHA-1. Все узлы TOR используют TLS/SSLv3 для сетевой аутентификации и шифрования. Все пакеты при передаче между узлами сети мультиплексируются в одно TLS-соединение.

Различают следующие виды узлов TOR:

- входные узлы (entry node);
- посреднические узлы (middleman node);
- выходные узлы (exit node);
- сторожевые узлы (guard node);
- мостовые узлы (bridge relay);
- выходные анклавы (exit enclave).

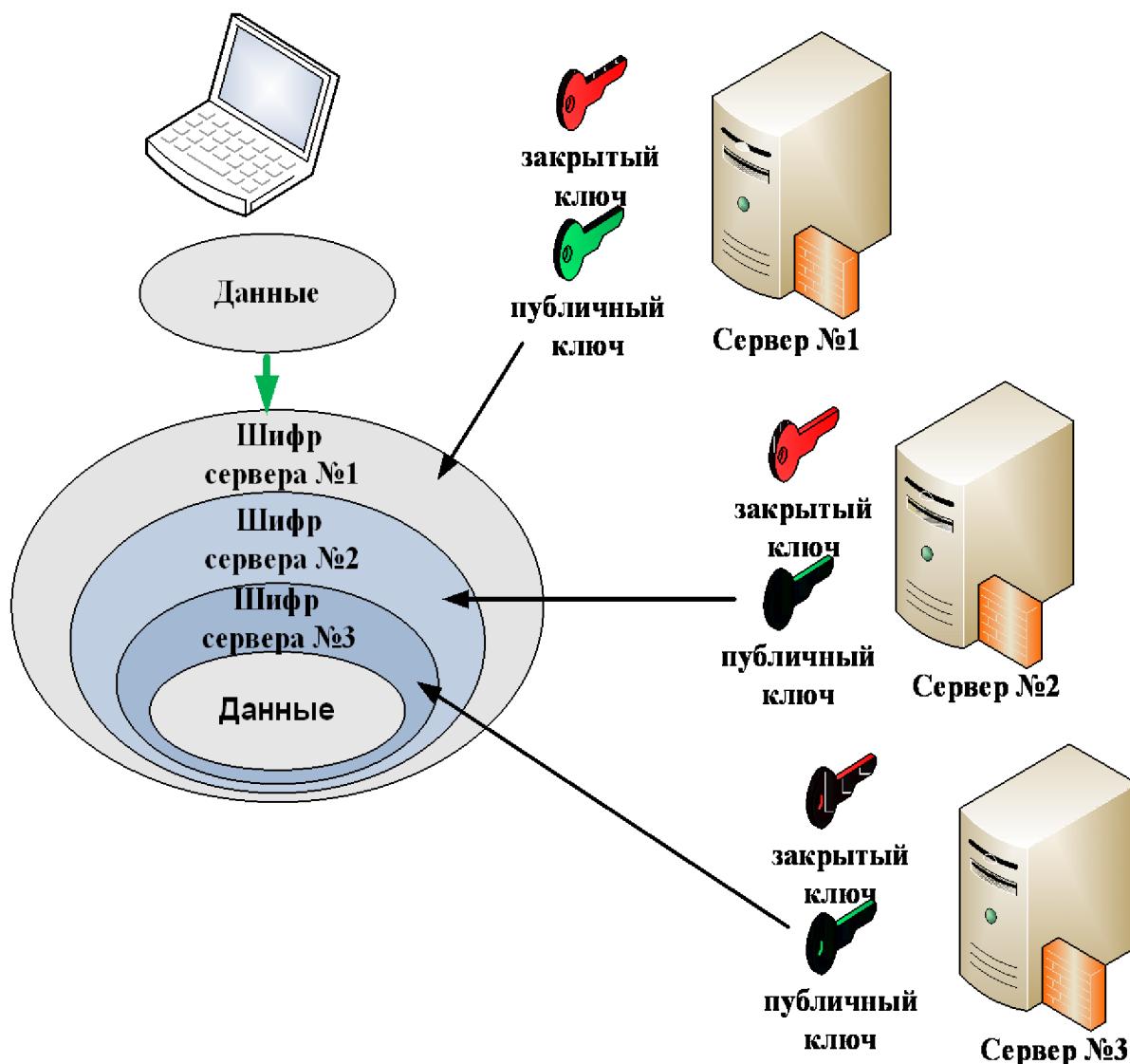


Рис. 5.3. Принцип луковичного шифрования

Входные узлы принимают соединения клиентов сети TOR. Посреднический узел передает пакеты только между другими узлами сети. Узлы, находящиеся в цепочке последними, называют выходными узлами. Сторожевыми называются узлы, выбранные клиентом сети TOR для входа в сеть в качестве постоянных точек входа. Ретрансляторы, называемые мостами (Tor Bridges), являются узлами сети TOR, адреса которых не публикуются в сервере каталогов и используются в качестве точек входа как для загрузки директорий, так и для построения цепочек. Поскольку открытого списка мостов не существует, даже блокировка всех публичных адресов TOR не повлияет на доступность этих скрытых ретрансляторов. Корневые серверы мостовых узлов собирают IP-адреса мостов и передают их пользователям по электронной почте, через веб-серверы или путём запросов, что значительно

повышает их защищенность от блокирования. Выходной анклав – это ретранслятор TOR, который позволяет выйти на обычный сервис, находящийся по тому же IP-адресу, что и сам «анклав». Каждый узел сети TOR может относиться к нескольким видам узлов одновременно.

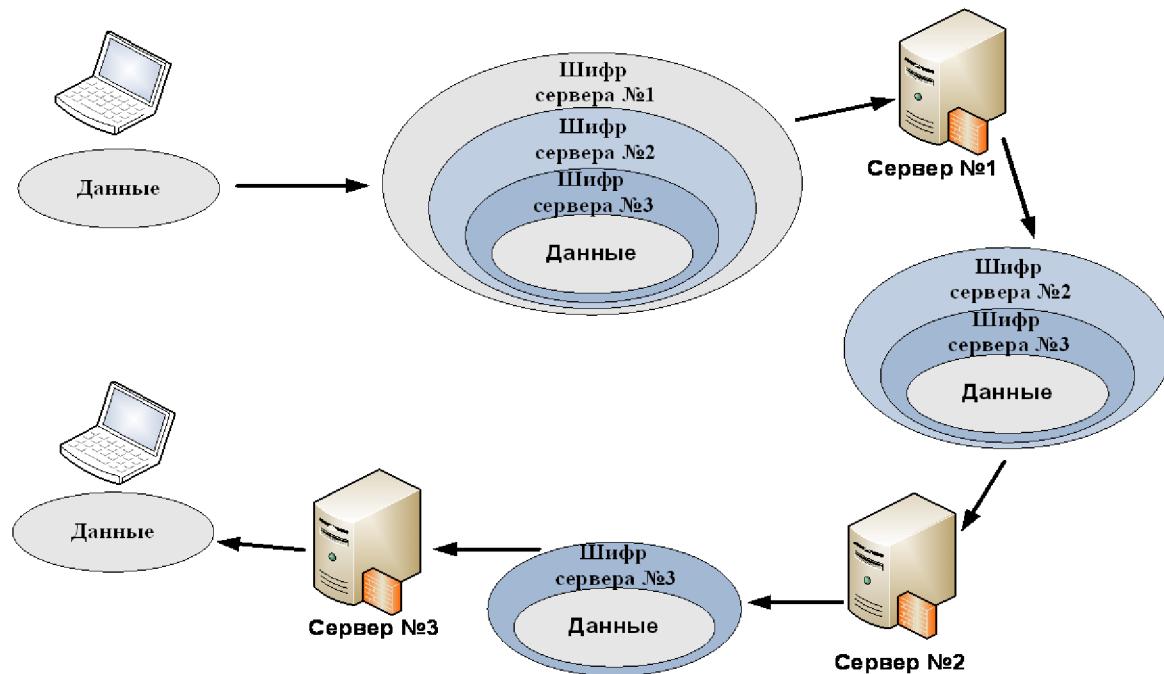


Рис. 5.4. Принцип луковичной маршрутизации

Организация доступа к скрытым сервисам включает 6 этапов (рис. 5.5). На первом этапе при запуске скрытого сервиса его узел случайным образом выбирает несколько промежуточных узлов, строит до них стандартные луковичные цепочки и назначает точками входа. На втором этапе список точек входа, подписанный публичным ключом скрытого сервиса, узел отправляет в распределенную базу данных сервисов (хеш-таблицу). На третьем этапе клиент, пожелавший соединиться со скрытым сервисом, в первую очередь должен узнать доменное имя onion. После этого он загружает из распределенной хеш-таблицы адреса точек входа и устанавливает луковичную цепочку до случайно выбранного узла сети, называет его точкой randevu и генерирует одноразовый ключ, которым подписывает данные точки randevu. На четвертом этапе клиент скрытого сервиса устанавливает соединение с одной из точек входа и передает в нее данные о точке randevu и одноразовый ключ, подписанные публичным ключом скрытого сервиса. На пятом этапе скрытый сервис расшифровывает сообщение о встрече в точке

рандеву и одноразовый ключ. Сервис строит луковичную цепочку до точки рандеву и отправляет в нее одноразовый ключ. На шестом шаге точка рандеву информирует клиента об успешном установлении соединения со скрытым сервисом. После этого клиент может использовать скрытый сервис. В цепочке между клиентом и скрытым сервисом длина цепочки составляет 6 узлов.

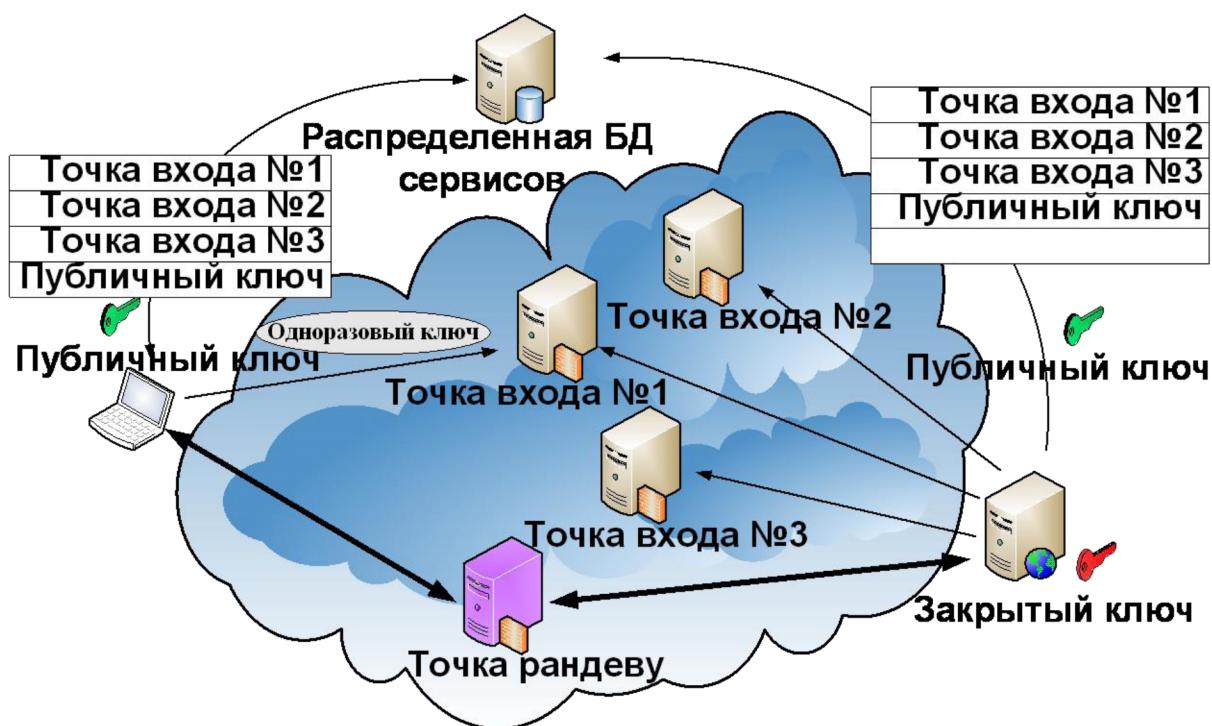


Рис. 5.5. Установление связи со скрытым сервисом

Необходимо уточнить, что обратно трафик идет в открытом виде, на выходном узле он зашифровывается временным симметричным ключом и передается по цепочке.

Сеть TOR критикуют потому, что требуют от нее слишком много: безопасно передавать в сеть трафик любых приложений, защищать от глобального наблюдателя, обеспечивать конфиденциальность передаваемых данных и пр. Но она решает главную задачу при своей модели угроз: достаточно высокий уровень анонимности клиента при передаче только http-трафика при соблюдении всех обязательных правил, которые подробно описаны на официальном сайте разработчиков TOR: [www.torproject.org](http://www.torproject.org).

Положительными особенностями использования TOR являются:

- высокая степень анонимности клиента при соблюдении всех правил;

–простота использования (скачал TOR Browser Bundle, запустил и пользуйся).

Отрицательными особенностями использования TOR является то, что:

- выходной трафик прослушивается (однако, никто не мешает создавать последним сервером в цепочке свой собственный сервер);
- обмен данными происходит с низкой скоростью;
- необходимо наличие управляющих серверов.

#### 5.4. Сеть анонимизации I2P

I2P (сокр. от англ. Invisible Internet Project - «Проект невидимый Интернет») - открытое программное обеспечение, созданное для организации сверхустойчивой анонимной, оверлейной, зашифрованной сети и применимое для веб-сёрфинга (поиск различных ресурсов в Интернет), анонимного хостинга (создания анонимных сайтов, форумов и чатов, файлообменных серверов и т. д.), систем обмена мгновенными сообщениями, ведения блогов, а также для файлообмена и электронной почты. Адреса сайтов в сети I2P находятся в псевдо-доменном пространстве «.i2p».

В I2P есть два главных понятия:

- «туннель» - это временный односторонний путь через некоторый список узлов. ТунNELи бывают входящие и исходящие;
- «сетевая база NetDb», которая распределена по всем клиентам I2P. Её назначение - хранение информации о том, как клиенту соединиться с определенным адресатом.

База NetDb хранит в себе следующую информацию:

- RouterInfos - контактные данные роутеров (клиентов), которые используются для построения туннелей;
- LeaseSets - контактные данные адресатов, которые используются для связи исходящих и входящих туннелей.

Сеть I2P похожа на традиционный Интернет, но отличается невозможностью цензуры, благодаря использованию механизмов шифрования, P2P-архитектуре и переменным посредникам (хопам). Использование таких механизмов позволяет увеличить сложность деанонимизации, атак типа «человек посередине» и сделать полностью

---

невозможной прозрачную для пользователя подмену пакетов.

В настоящий момент единственным централизованным элементом сети является особая реализация обычных серверов доменных имен. От привычных DNS-серверов они отличаются в следующем:

- для определения дестхеша (адреса узла сети) используется локальная база адресов;
- база адресов периодически обновляется с серверов имен, тогда как в традиционных DNS адрес определяется по запросу к нему;
- поддомены не привязаны к домену-родителю, но поставщик адресных подписок имеет возможность ограничить регистрацию субдоменов по разрешению домена-родителя;
- возможно использование нескольких серверов имен. В официальной реализации роутера конфликты решаются по схеме «первый пришёл - первый обслужил», но стоит заметить, что дестхеши, явно указанные пользователем в адресных базах «privatehosts» и «userhosts», обрабатываются первыми - то есть имеют большее влияние, чем подписки.

Поскольку сеть является одноранговой и децентрализованной, скорость и надежность сети напрямую зависит от участия людей в передаче чужого трафика. Официальный роутер по умолчанию сконфигурирован на его раздачу.

Для доступа в I2P необходимо установить на своем компьютере программу-маршрутизатор, которая шифрует/дешифрует, сжимает/разжимает трафик и направляет его узлам сети I2P. Для работы с внутрисетевыми сайтами необходимо настроить браузер для направления HTTP-пакетов роутеру, «слушающему» определенный порт. Для обращения к внешнему Интернету через I2P необходимо использовать прокси-серверы изнутри I2P (outproxy), которых на настоящее время мало. Также внутренние сайты в сети I2P доступны из внешнего Интернета через прокси, ведущие внутрь (inproxy).

Рассмотрим алгоритм взаимодействия узлов.

Шаг первый (рис. 5.6). Узел «Москва» строит исходящие тунNELи. Он обращается к базе NetDb за данными о роутерах и строит туннель с их участием.

Шаг второй (рис. 5.7). Узел «Лондон» строит входной туннель

аналогично тому, как и строится исходящий туннель. Затем он публикует свои координаты или так называемый «LeaseSet» в NetDb.

Шаг третий (рис. 5.8). Когда «Москва» хочет оправить сообщение «Лондону», она запрашивает в NetDb LeaseSet «Лондона». И по исходящим туннелям пересыпает сообщение к шлюзу адресата.

Достоинствами I2P являются:

- высокая степень анонимности клиента;
- полная децентрализация, что ведёт к устойчивости сети;
- конфиденциальность данных: сквозное шифрование между клиентом и адресатом.

Недостатки I2P состоят в следующем:

- низкая скорость передачи данных;
- необходимость создания и применения «своего Интернета».

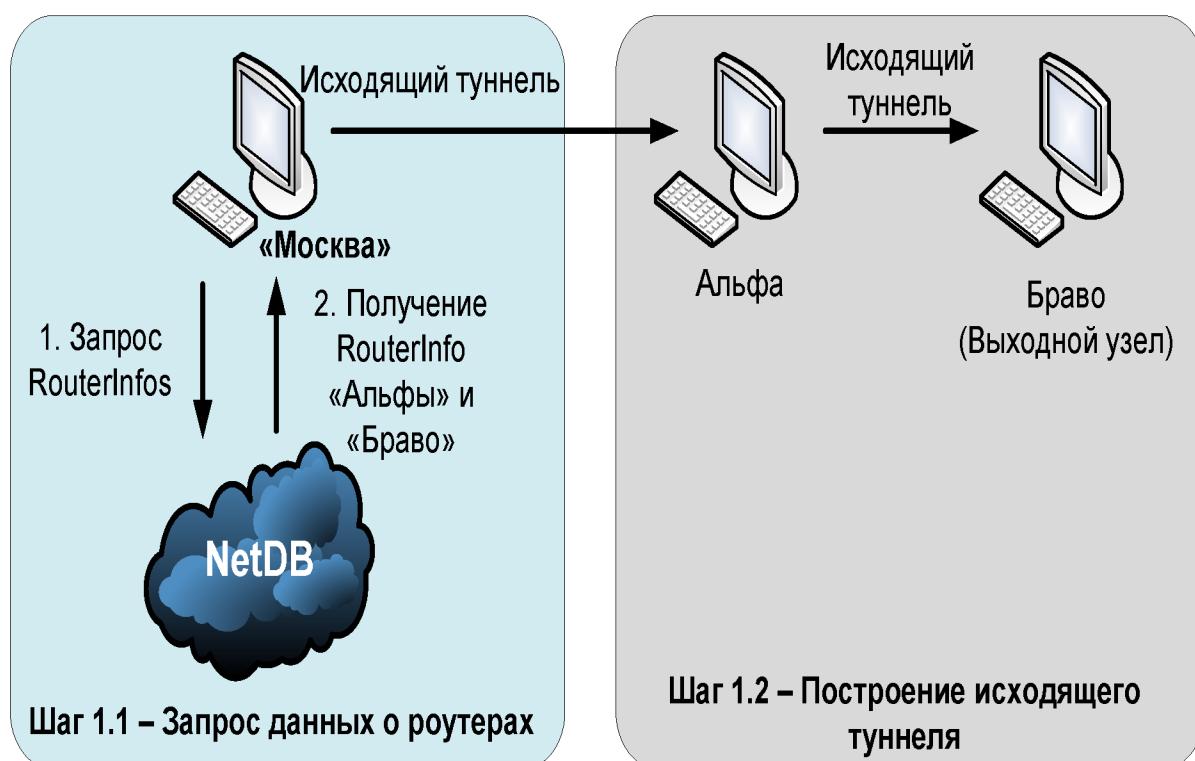


Рис. 5.6. Первый шаг алгоритма

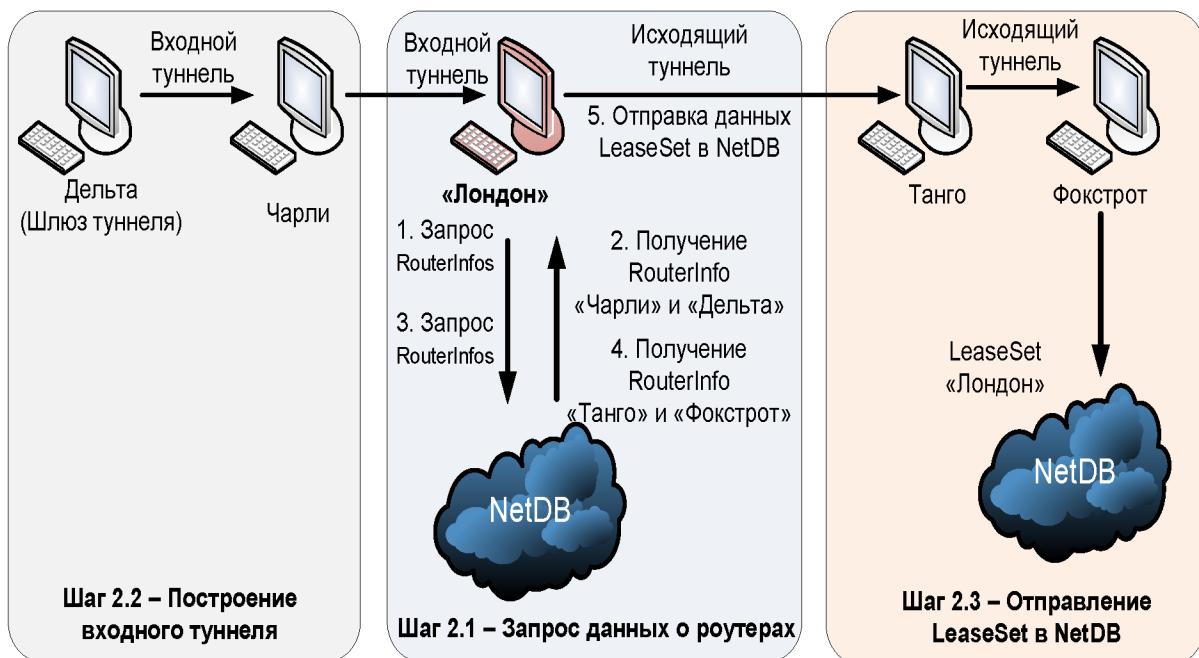


Рис. 5.7. Второй шаг алгоритма

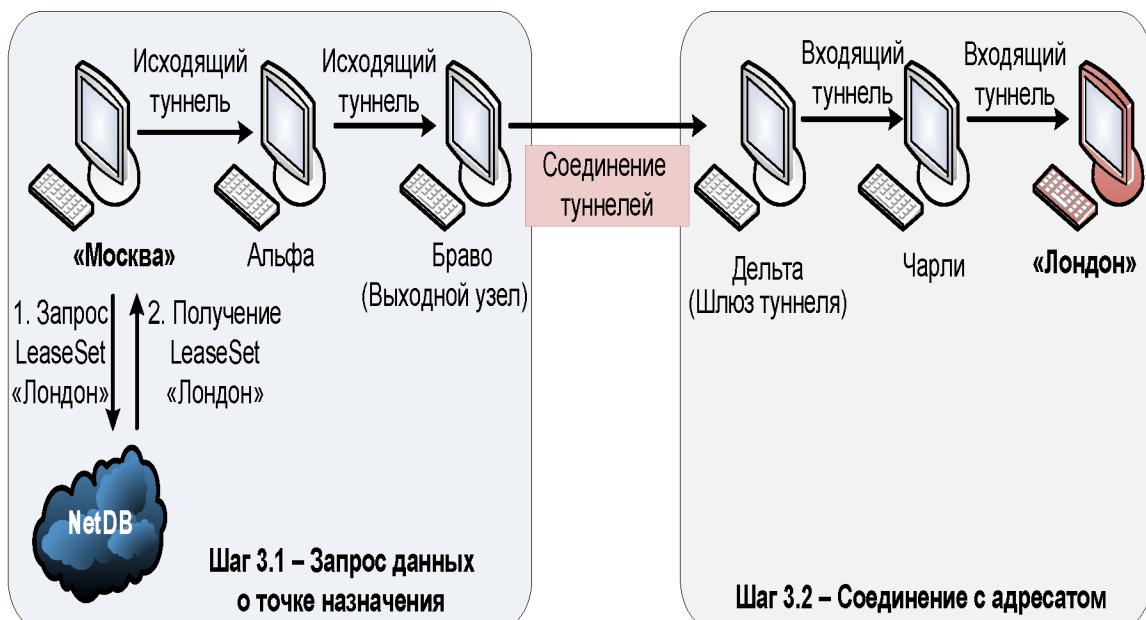


Рис. 5.8. Третий шаг алгоритма

Существуют другие проекты, посвященные анонимности в Интернете, не считая «дополнений в браузерах» и «программ для анонимности». Просто другие, менее популярные решения, либо уже скомпрометированы, либо еще не так известны, а следовательно, не изучены экспертами, чтобы говорить об их достаточной надежности.

## Глава 6. Вредоносные программы и спам

Существуют программы, намеренно написанные с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов. Такие программы несут вредоносную нагрузку и соответственно называются вредоносными.

### 6.1. Классификация вредоносных программ

Вредоносные программы классифицируют по способу проникновения, размножения и типу вредоносной нагрузки.

В соответствии со способами распространения и вредоносной нагрузки все вредоносные программы можно разделить на четыре основных типа: компьютерные вирусы, черви, трояны и другие программы.

Следует отметить, что компьютерным вирусом часто называют любую вредоносную программу. Это обусловлено тем, что первые известные вредоносные программы были именно компьютерными вирусами, и в течение последующих десятилетий число вирусов значительно превышало количество всех остальных вредоносных программ. Однако в последнее время наметились тенденции к появлению новых невирусных технологий, которые используют вредоносные программы. При этом доля истинных вирусов в общем числе инцидентов с вредоносными программами за последние годы значительно сократилась.

В настоящее время вредоносные программы – это уже большей частью именно не вирусы, хотя такие термины, как «вирус» и «заражение вирусом», применяются по отношению ко всем вредоносным программам. Поэтому далее под термином «вирус» будет пониматься и вредоносная программа.

**Компьютерные вирусы.** *Компьютерный вирус* – это программа, способная создавать свои дубликаты и внедрять их в компьютерные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Основная цель любого компьютерного вируса – это распространение на другие ресурсы компьютера и выполнение специальных действий при

---

определенных событиях или действиях пользователя (например, 26-го числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

Жизненный цикл любого компьютерного вируса можно разделить на четыре этапа:

- проникновение на чужой компьютер;
- активация;
- поиск объектов для заражения;
- подготовка и внедрение копий.

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения – фактически все каналы, по которым можно скопировать файл. Однако, в отличие от червей, вирусы не используют сетевые ресурсы – заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал, например, скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

После проникновения следует активация вируса. Это может происходить разными путями, и в зависимости от выбранного метода вирусы делятся на такие виды:

- загрузочные вирусы заражают загрузочные сектора жестких дисков и мобильных носителей;
- файловые вирусы заражают файлы.

Дополнительным признаком отличия вирусов от других вредоносных программ служит их привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Так, вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например UNIX.

При подготовке своих копий вирусы могут применять для маскировки разные технологии:

- шифрование – в этом случае вирус состоит из двух частей: сам вирус и шифратор;
- метаморфизм – при применении этого метода вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки

---

местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд.

Соответственно, в зависимости от используемых методов маскировки вирусы можно делить на шифрованные, метаморфные и полиморфные, использующие комбинацию двух типов маскировки.

**Сетевые черви.** В отличие от вирусов *сетевые черви* – это вполне самостоятельные вредоносные программы. Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов.

В зависимости от способа проникновения систему черви делятся на следующие типы:

- *сетевые черви* используют для распространения локальные сети и Интернет;
- *почтовые черви* распространяются с помощью почтовых программ;
- *IM-черви* используют программы обмена сообщениями IM (Instant Messenger) в режиме реального времени;
- *IRC-черви* распространяются через чаты IRC (Internet Relay Chat);
- *P2P-черви* распространяются при помощи пиринговых файлообменных сетей P2P (Peer-to-Peer – равный с равным).

После проникновения на компьютер червь должен активироваться – иными словами, запуститься. По методу активации все черви можно разделить на две большие группы: на тех, которые требуют активного участия пользователя и тех, кто его не требует.

Отличительная особенность червей из первой группы – это использование обманных методов. Например, получатель инфицированного файла вводится в заблуждение текстом полученного письма и добровольно открывает вложение с почтовым червем, тем самым его активируя. Черви из второй группы используют ошибки в настройке или бреши в системе безопасности операционной системы. В последнее время наметилась тенденция к совмещению этих двух технологий – такие черви наиболее опасны и часто вызывают глобальные эпидемии.

Сетевые черви могут кооперироваться с вирусами – такая пара способна самостоятельно распространяться по сети (благодаря черви) и в то же время заражать ресурсы компьютера (функции вируса).

**Троянские программы.** *Троянская программа* (программа класса «троянский конь», или просто троян) имеет только одно назначение – нанести ущерб целевому компьютеру путем выполнения не санкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

В отличие от вирусов и червей, трояны сами не размножаются. Жизненный цикл троянов состоит всего из трех этапов:

- проникновение в систему;
- активация;
- выполнение вредоносных действий.

Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы с целью проникновения в нее. В этом случае обычно применяется маскировка, когда троян выдает себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск (например, загружает из Интернета) и запускает. При этом программа действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные трояну.

Однако в большинстве случаев трояны проникают на компьютеры вместе с вирусом либо червем – т.е. такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу.

После проникновения на компьютер трояну необходима активация, и здесь он похож на червя – либо требует активных действий от пользователя либо через уязвимости в программном обеспечении самостоятельно заражает систему.

Поскольку главная цель троянов – это выполнение несанкционированных действий, они классифицируются по типу вредоносной нагрузки:

- *похитители паролей* предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат;
- *утилиты скрытого удаленного управления* – это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Обычно это возможность скрыто загружать,

---

отсылать, запускать или уничтожать файлы. Такие трояны могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов уничтожения данных;

– логические бомбы характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, в ответ на определенное действие пользователя или команды извне) выполнять какое-либо действие, например удаление файлов;

– клавиатурные шпионы, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры, с целью последующей их передачи своему автору;

– анонимные SMTP- и прокси-серверы – такие трояны на зараженном компьютере организуют несанкционированную отправку электронной почты, что часто используется для рассылки спама;

– утилиты дозвона в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернета;

– модификаторы настроек браузера меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, лимитируют нажатия на рекламные баннеры и т.п.

Отдельно отметим, что существуют программы из класса троянов, которые наносят вред другим удаленным компьютерам и сетям, при этом не нарушая работоспособности инфицированного компьютера. Яркие представители этой группы – организаторы DDoS-атак.

**Другие вредоносные программы и нежелательная корреспонденция.** Кроме вирусов, червей и троянов существует еще много других вредоносных программ и нежелательной корреспонденции. Среди них можно выделить следующие группы:

– шпионское ПО (*Spyware*) – опасные для пользователя программы, предназначенные для слежения за системой и отсылки собранной информации третьей стороне – создателю или заказчику такой программы. Среди заказчиков шпионского ПО – спамеры, рекламщики, маркетинговые агентства, спам-агентства, преступные группировки, деятели промышленного шпионажа. Шпионские программы интересуются системными данными, типом браузера, посещаемыми веб-узлами, иногда и содержимым файлов на жестком диске компьютера-жертвы. Такие программы тайно закачиваются на компьютер

---

вместе с каким-нибудь бесплатным софтом или при просмотре определенным образом сконструированных HTML-страниц и всплывающих рекламных окон и самоустанавливаются без информирования об этом пользователя. Побочные эффекты от присутствия шпионского ПО на компьютере – нестабильная работа браузера и замедление производительности системы;

– *условно опасные программы*, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:

– *апплеты (applets)* – прикладные программы, небольшие Java-приложения, встраиваемые в HTML-страницы. По своей сути эти программы не вредоносные, но могут использоваться в злонамеренных целях. Особенно апплеты опасны для любителей онлайновых игр, так как в них апплеты Java требуются обязательно. Апплеты, как и шпионское ПО, могут использоваться для отправки собранной на компьютере информации третьей стороне;

– *рекламные утилиты (adware)* – условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается и программы начинают работать в обычном режиме. Проблема рекламных утилит кроется в механизмах, которые используются для загрузки рекламы на компьютер. Кроме того, что для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже после регистрации такие модули могут автоматически не удаляться и продолжать свою работу в скрытом режиме;

– *riskware* – вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим хакерам использовать их с вредоносными целями. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернета, утилиты восстановления забытых паролей и др.;

– *хакерские утилиты* – к этому виду программ относятся программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов),

---

наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit), и другие подобные утилиты. Такие специфические программы обычно используют только хакеры;

– *мистификации* – программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений, например о форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений зависит от фантазии автора программы;

– *спам* – нежелательная почтовая корреспонденция рекламного характера, загружающая трафик и отнимающая время у пользователей.

Самыми эффективными средствами защиты от вирусов являются специальные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах. Такие программы называются *антивирусы*, и для того чтобы построить действительно надежную антивирусную защиту, использовать их нужно обязательно.

В антивирусных продуктах используется два основных подхода к обнаружению вредоносных программ: сигнатурный и проактивный/эвристический.

*Сигнатурные методы* – точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.

*Проактивные/эвристические методы* – приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Возможности антивирусных программ расширяют дополнительные средства защиты от вредоносных программ и нежелательной корреспонденции.

Такими средствами защиты являются:

- обновления, устраниющие уязвимости в операционной системе, через которые могут проникать вирусы;
- брандмауэры – программы, защищающие от атак по сети;
- средства борьбы со спамом.

## 6.2. Рекомендации по безопасной работе в сети Интернет

**Основные правила** безопасной работы в Интернет, позволяющие

---

избежать потери и утечки информации сводятся к следующему:

– избегать установок на компьютер программ, полученных из сомнительных источников. В сети можно скачать много различных бесплатных и условно бесплатных программ. Лучше всего загружать программы с сайтов разработчиков. Часто в каталогах программ размещается ссылка на сайт автора. При скачивании программ со сторонних сайтов, обратите внимание на посещаемость сайта (при наличии независимых счетчиков). Иногда надежность ресурса можно оценить, прочитав отзывы, которые можно отыскать через поисковые системы;

– не запускать исполняемые файлы, полученные по электронной почте или любым другим способом. Вредоносные программы могут проникать на компьютер через электронную почту. Если от неизвестного источника пришло письмо с текстом непонятного содержания и/или прикрепленным файлом, имеющим расширения, указанные в таблице 6.1, удалайте подобные письма, так как при запуске подобных файлов высока вероятность заражения компьютера;

– следить за постоянной работой антивирусной программы на компьютере. Если нет возможности установить платное антивирусное обеспечение, то можно воспользоваться одним из бесплатных. Их можно скачать с серверов разработчиков. Не забывайте периодически обновлять антивирусные базы данных, так как постоянно появляются новые вирусы;

– не хранить логины и пароли в открытом виде на своем компьютере. Файлы, содержащие важную информацию, следует архивировать с паролем;

– не использовать простые пароли для доступа к ресурсам сети. Длина пароля должна быть не менее 10-12 символов с использованием символов +, \*, / и т.д.;

– не устанавливать одинаковые пароли на разные сайты. Желательно наиболее важные пароли периодически менять;

– использовать современный браузер, так как он является основной программой для работы в сети. Его нужно периодически обновлять, поскольку постоянно обнаружаются новые уязвимости;

– задействовать межсетевой экран (брандмауэр, файрвол). Это специализированная программа, позволяет фильтровать сетевые пакеты и ограничивать доступ к ресурсам компьютера из сети. Если вы не знакомы с

работой и настройкой подобных программ, то можно использовать встроенный в операционную систему межсетевой экран.

**Дополнительные меры** по недопущению распространения в Интернете информации о пользователе:

- не использовать социальные сети для общения;
- не хранить в облачных сервисах личные данные;
- не хранить личных данных на компьютере, подключенном к Интернету;

Таблица 6.1

### Расширения исполняемых файлов

Расширение	Описание	Популярность использования
.apk	пакет приложения Android	очень часто
.bat	пакетный файл MS-DOS	очень часто
.bin	исполняемый файл Unix	средне
.bin	двоичный исполняемый файл	средне
.cgi	общий интерфейс шлюза	очень часто
.com	исполняемый файл MS-DOS	очень часто
.cpp	файл Apple Xcode Core C	редко
.js	исполняемый файл JScript	средне
.exe	исполняемый файл	очень часто
.exe	приложение PortableApps.com	часто
.gadget	гаджет Windows	очень часто
.gtp	исполняемый файл Atari ST	очень редко
.jar	файл архива Java	очень часто
.msi	установочный файл Windows	очень часто
.msu	пакет обновлений Windows	средне
.paf.exe	файл PortableApps.com	часто
.pif	информация о приложении с	очень часто
.pwz	файл мастера создания Microsoft PowerPoint	редко
.scr	файл скрипта	часто
.thm	макро файл Thermwood	редко
.vb	скрипт VBScript	очень часто
.wsf	файл сценария Windows	очень часто

– очищать системные журналы событий (удалять log-файлы) после каждого доступа к ресурсам Интернет, запретить создание cookies-файлов, запретить отсылку любых отчетов;

– поддерживать связь только с «адекватными» партнерами, которые не станут заносить в свои сетевые хранилища (адресные книги) подробные сведения о вас;

- не устанавливать на компьютер лишние программы, не подписываться на сервисные рассылки, по возможности избегать регистрации на сайтах и форумах;
- запретить автоматическое выполнение любых сетевых операций (в том числе установку обновлений), отключить все службы, позволяющие управлять компьютером удаленно;
- избегать использования сервисов и приложений, встроенных в Windows по умолчанию – windows mail, netmeeting, браузер, файрвол, антивирус, медиаплеер и др. по возможности использовать программы сторонних производителей;
- создавать сетевое соединение только на время работы в Интернете, не держать постоянно активными программы Интернет-телефонии и других видов связи через сеть, никогда не запускать сервисы автоматического сбора почты с разных ящиков: постоянное подключение к сети дает возможность вторжения извне в ваш компьютер.

## Список литературы

1. Зима В.М. Безопасность глобальных сестевых технологий / В.М.Зима, А.А.Молдовян, Н.А.Молдовян. – СПб.; БХВ-Петербург, 2019. – 320 с.
2. Келдыш Н.В. Информационная безопасность. Защита информации на объектах информатизации: учеб. пособие / Н.В. Келдыш. - М.: Мир науки, 2022. – сетевое издание. <https://www.twirpx.org/file/3773488/>.
3. Олифер В.Г., Новые технологии и оборудование IP-сетей / В.Г.Олифер, Н.А.Олифер. – СПб.; БХВ-Петербург, 2021. – 1005 с.
4. Пушнин А.В. Информационные сети и телекоммуникации / А.В.Пушнин, В.В.Янушко. – Таганрог: Изд-во ТРТУ, 2015. – 128 с.
5. Сизова О.В. Информационная безопасность: учеб. пособие / О.В.Сизова; Иван.гос.хим-технол. ун-т. – Иваново, 2015. – 120 с.
6. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф.Шаньгин. – М. : ИД «ФОРУМ» : ИНФРА-М, 2022 – 592 с.

## Словарь англоязычных аббревиатур

**DDoS-атака** (Distributed Denial of Service) – распределённая атака типа «отказ в обслуживании». Атака выполняется одновременно с большого числа компьютеров. Такая атака проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищенной крупной компании или правительственный организации.

**DNS** (Domain Name System) – компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов.

**DoS** (Denial of Service) – отказ в обслуживании. Атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. В настоящее время DoS и DDoS-атаки наиболее популярны, так как позволяют довести практически любую систему, не оставляя юридически значимых улик.

**ESMTP** (Extended SMTP) – масштабируемое расширение протокола SMTP. В настоящее время под "протоколом SMTP", как правило, подразумевают SMTP и его расширения.

**FTP** (File Transfer Protocol) – стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). FTP часто используется для загрузки сетевых страниц и других документов с частного устройства разработки на открытые сервера хостинга.

**HTTP** (HyperText Transfer Protocol) – протокол передачи гипертекста. Протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов в формате HTML, в настоящий момент используется для передачи произвольных данных). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом. HTTP в настоящее время повсеместно используется

---

в Интернете для получения информации с веб-сайтов. HTTP — протокол прикладного уровня, аналогичными ему являются FTP и SMTP.

**HTTPS** (HyperText Transfer Protocol Secure) – расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS. HTTPS широко используется и поддерживается всеми популярными браузерами.

**ICMP** (Internet Control Message Protocol) – протокол межсетевых управляющих сообщений. Сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции.

**IP-адрес** (Internet Protocol Address) – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. В сети Интернет требуется глобальная уникальность адреса. В случае работы в локальной сети требуется уникальность адреса в пределах сети.

**ISO** (International Standards Organization) – Международная организация по стандартизации. ISO разработала модель, которая четко определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какую работу должен делать каждый уровень. Эта модель называется моделью взаимодействия открытых систем (Open System Interconnection, OSI) или моделью ISO/OSI.

**OSPF** (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути. Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

**OSI** (Open Systems Interconnection) – сетевая модель стека сетевых протоколов OSI/ISO. В модели OSI взаимодействие делится на семь уровней. Каждый уровень поддерживает интерфейсы с выше- и нижележащими уровнями. В связи с затянувшейся разработкой протоколов OSI, в настоящее время основным используемым стеком протоколов является TCP/IP, разработанный ещё до принятия модели OSI и вне связи с ней.

---

**POP3** (Post Office Protocol Version 3) – протокол почтового отделения, версия 3. Стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP/IP-соединению. POP и IMAP (Internet Message Access Protocol) – наиболее распространенные интернет-протоколы для извлечения почты. Практически все современные клиенты и серверы электронной почты поддерживают оба стандарта. Протокол POP был разработан в нескольких версиях, нынешним стандартом является третья версия (POP3). Большинство поставщиков услуг электронной почты (такие как Hotmail, Gmail и Yahoo! Mail) также поддерживают IMAP и POP3.

**PKI** (Public Key Infrastructure) – инфраструктура открытых ключей. Набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей. Фактически, PKI представляет собой систему, основным компонентом которой является удостоверяющий центр и пользователи, взаимодействующие между собой посредством удостоверяющего центра.

**SMTP** (Simple Mail Transfer Protocol) – это сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP. SMTP используется для отправки почты от пользователей к серверам и между серверами для дальнейшей пересылки к получателю. Для приёма почты почтовый клиент должен использовать протоколы POP3 или IMAP.

**SNMP** (Simple Network Management Protocol) – простой протокол сетевого управления. Стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора.

**SSID** (Service Set Identifier) – уникальное сетевое имя для идентификации сети. Это имя также называется идентификатором обслуживания сети или идентификатором SSID.

**TELNET** (TErminaL NETwork) – сетевой протокол для реализации

---

текстового интерфейса по сети. Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола. Выполняет функции протокола прикладного уровня модели OSI.

**TCP** (Transmission Control Protocol) – один из основных протоколов передачи данных Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP. Выполняет функции протокола транспортного уровня в стеке протоколов IP.

**TFTP** (Trivial File Transfer Protocol) – простой протокол передачи файлов, используется главным образом для первоначальной загрузки бездисковых рабочих станций. TFTP, в отличие от FTP, не содержит возможностей аутентификации (хотя возможна фильтрация по IP-адресу) и основан на транспортном протоколе UDP.

**TOR** (The Onion Router) – свободное и открытое программное обеспечение для реализации второго поколения так называемой луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. С помощью Тор пользователи могут сохранять анонимность в интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика обеспечивается за счёт использования распределённой сети серверов.

**UDP** (User Datagram Protocol) – протокол пользовательских датаграмм. Один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посыпать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных.

**VPN** (Virtual Private Network) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к

---

построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

**WEP** (Wired Equivalent Privacy) – алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения конфиденциальности и защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания. Для безопасности в сетях Wi-Fi рекомендуется использовать WPA. WEP часто неправильно называют Wireless Encryption Protocol.

**WLAN** (Wireless Local Area Network) – локальная сеть, построенная на основе беспроводных технологий. При таком способе построения сетей передача данных осуществляется через радиоэфир; объединение устройств в сеть происходит без использования кабельных соединений. Наиболее распространенным на сегодняшний день способом построения является Wi-Fi.

Келдыш Наталья Всеволодовна

**Системная защита информации компьютерных сетей**

Учебное пособие издано в авторской редакции

Сетевое издание

Ответственный за выпуск – Алимова Н.К.

Учебное издание

**Системные требования:**

операционная система Windows XP или новее, macOS 10.12 или новее, Linux.

Программное обеспечение для чтения файлов PDF.

Объем данных 2 Мб

Принято к публикации «14» августа 2022 года

Яз. рус., англ.

ООО «Издательство «Мир науки»

«Publishing company «World of science», LLC

Адрес:

Юридический адрес — 127055, г. Москва, пер. Порядковый, д. 21, офис 401.

Почтовый адрес — 127055, г. Москва, пер. Порядковый, д. 21, офис 401.

**ДАННОЕ ИЗДАНИЕ ПРЕДНАЗНАЧЕНО ИСКЛЮЧИТЕЛЬНО ДЛЯ ПУБЛИКАЦИИ НА  
ЭЛЕКТРОННЫХ НОСИТЕЛЯХ**