18. ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

18.1 Аутефекация и управление сертификатами

18.1.1 Цифровые подписи

Цифровые подписи *- это форма шифрования, обеспечивающая аутентификацию (подтверждение подлинности) цифровой информации.*

С помощью цифровой подписи можно повысить уровень этой защиты и обезопасить информацию от изменения после получения и дешифрования.

Рис. 18.1 - Схема формирования цифровой подписи по алгоритму RSA

До настоящего времени наиболее часто для построения схемы цифровой подписи использовался алгоритм RSA. В основе этого алгоритма лежит концепция Диффи-Хеллмана. Она заключается в том, что каждый пользователь сети имеет свой закрытый ключ, необходимый для формирования подписи; соответствующий этому секретному ключу открытый ключ, предназначенный для проверки подписи, известен всем другим пользователям сети.

На рис. 18.1 показана схема формирования цифровой подписи по алгоритму RSA. Подписанное сообщение состоит из двух частей: незашифрованной части, в которой содержится исходный текст *T*, и зашифрованной части, представляющей собой цифровую подпись.

Если результат расшифровки цифровой подписи совпадает с открытой частью сообщения, то считается, что документ подлинный, не претерпел никаких изменений в процессе передачи, а автором его является именно тот человек, который передал свой открытый ключ получателю. Если сообщение снабжено цифровой подписью, то получатель может быть уверен, что оно не было изменено или подделано по пути.

Цифровые подписи применяются к тексту до того, как он шифруется. Если помимо снабжения текста электронного документа цифровой подписью надо обеспечить его конфиденциальность, то вначале к тексту применяют

цифровую подпись, а затем шифруют все вместе: и текст, и цифровую подпись (рис. 18.2).

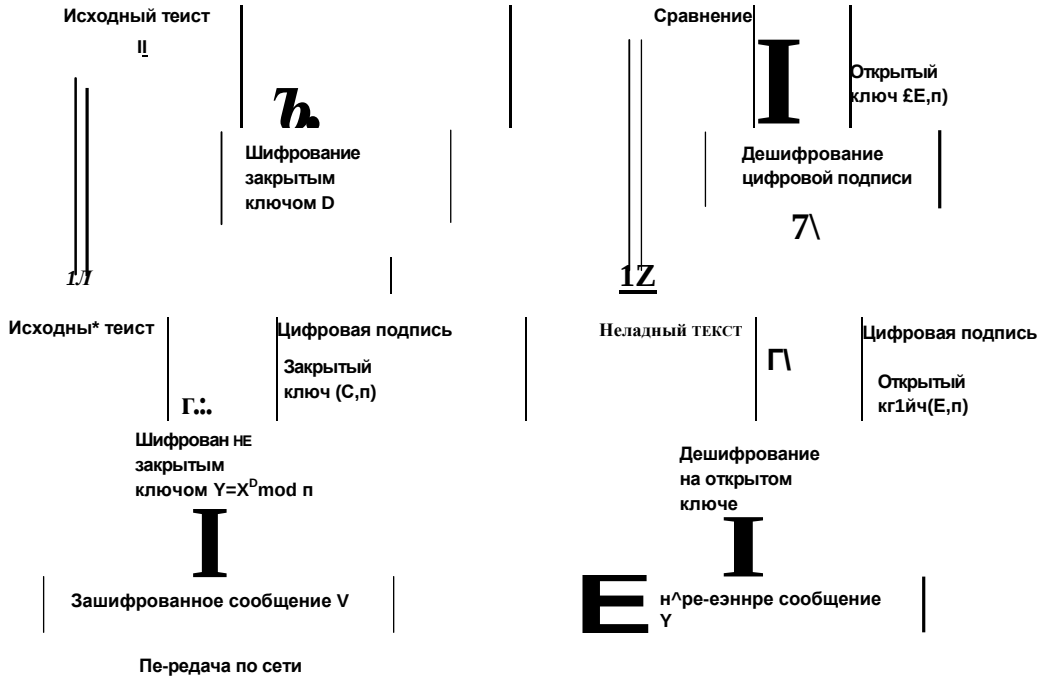


Рис. 18.2 - Обеспечение конфиденциальности документа с цифровой подписью

18.1.2 Управление ключами и сертификация ключей

Управление ключами является самой неприятной задачей при использовании любой системы шифрования. Ключи представляют собой самые важные объекты во всей системе, так как если злоумышленник получает ключ, у него появляется возможность расшифровывать все данные, зашифрованные с помощью этого ключа. Управление ключами заключается не только в защите их при использовании. Данная задача предусматривает создание надежных ключей, безопасное распространение ключей среди удаленных пользователей, обеспечение корректности ключей, отмену в случае их раскрытия или истечения срока действия.

Если ключи некоторым образом передаются в удаленное место расположения, они должны проверяться при получении на предмет того, не подверглись ли они вмешательству в процессе передачи. Это можно делать вручную либо использовать некоторую форму цифровой подписи.

Открытые ключи предназначены для публикации или передачи другим пользователям и должны сертифицироваться как принадлежащие владельцу ключевой пары. ***Сертификация*** *осуществляется с* ***помощью центрального бюро сертификатов (Certificate Authority - CA)****. В данном случае CA предоставляет цифровую подпись на открытом ключе, и благодаря этому CA с доверием воспринимает тот факт, что открытый ключ принадлежит владельцу ключевой пары* (см. рис. 18.3).

Цифровой сертификат *представляет собой цифровой документ (небольшой файл), заверяющий подлинность и статус владельца для пользователя или компьютерной системы.*

Бюро сертификатов (Certificate Authority - CA) *- объединение, включающее сервер сертификатов и создающее сертификаты.*

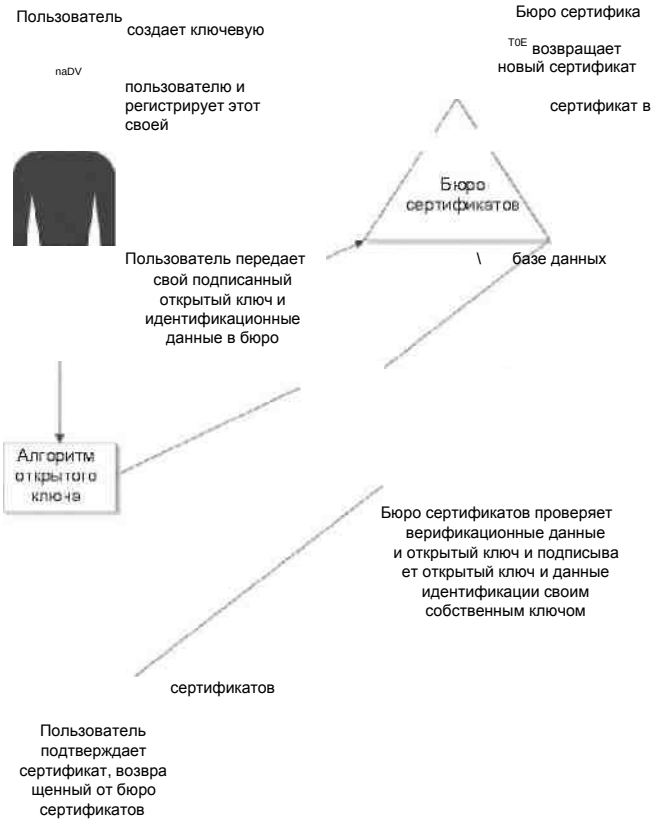


Рис. 18.3 - Сертификация открытого ключа в бюро сертификатов

18.1.3 Концепция доверия в информационной системе

Концепция доверия является основополагающим принципом информационной безопасности и шифрования в частности. Для работы шифрования необходима уверенность в том, что ключ шифра не будет раскрыт, и что используемый алгоритм шифрования является достаточно мощным. В случае с аутентификацией и цифровыми подписями необходима также уверенность в том, что открытый ключ на самом деле принадлежит тому, кто его использует.

18.1.3.1 Иерархическая модель доверия

Иерархическая модель доверия наиболее проста для восприятия. Говоря простым языком, в данном случае вы доверяете человеку, который находится выше в иерархической цепи, так как от него было получено соответствующее указание о необходимости доверия. На рисунке 18.4 изображена схема этой модели.

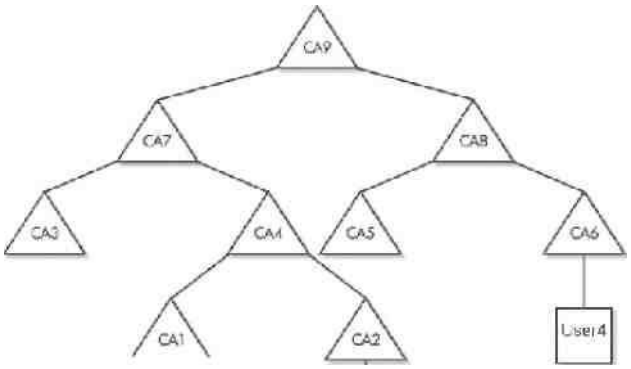


Рис. 18.4 - Иерархическая модель доверия

Как видно из рисунка, пользователи *User1* и *User2* располагаются под *CA1*. Следовательно, если *CA1* говорит, что сертификат открытого ключа принадлежит пользователю *User1*, пользователь *User2* будет верить этому. На практике *User2* передает пользователю *User1* свой сертификат открытого ключа, подписанный *CA1*. Пользователь *User1* проверяет подпись *CA1* с использованием открытого ключа *CA1*. Так как *CA1* находится в иерархии выше, чем *User1*, то *User1* доверяет *CA1* и, следовательно, доверяет сертификату пользователя *User2*.

Если пользователю *User1* нужно проверить информацию от пользователя *User3*, все несколько усложняется. *CA1* не знает о пользователе *User3*, в отличие от *CA2*. Тем не менее, пользователь *User1* не доверяет *CA2*, так как это бюро сертификатов напрямую не принадлежит цепочке пользователя *User1*. Следующий уровень вверх по цепочке - *CA4*. Пользователь *User1* может верифицировать информацию от пользователя *User3* посредством проверки с помощью *CA4* следующим образом.

- Пользователь *User1* смотрит на сертификат пользователя *User3*. Он подписан в *CA2*.
- Пользователь *User1* получает сертификат пользователя *CA2*. Он подписан в *CA4*.
- Так как пользователь *User1* доверяет *CA4*, открытый ключ *CA4* может использоваться для верификации сертификата *CA2*.
- Как только сертификат *CA2* верифицирован, пользователь *User1* может верифицировать сертификат пользователя *User3*.
- Как только будет верифицирован сертификат пользователя *User3*, пользователь *User1* может использовать открытый ключ пользователя *User3* для верификации данных.

18.1.3.2 Сетевая модель доверия

Сеть с доверием представляет собой альтернативную модель доверия. Эта концепция была впервые использована в технологии Pretty Good Privacy (PGP).

Сетевая модель доверия *заключается в том, что каждый пользователь сертифицирует свой сертификат и передает его известным ассоциированным объектам. Эти объекты могут подписать сертификат другого пользователя, так как он известен (см. рис. 18.5).*

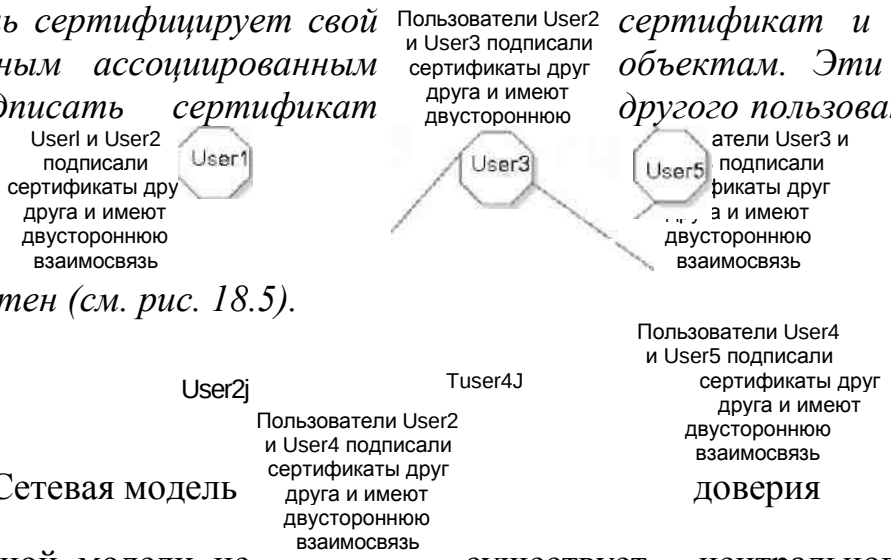


Рис. 18.5 - Сетевая модель доверия

В данной модели не существует центрального бюро сертификатов. Если пользователю *User1* требуется верифицировать информацию, поступающую от пользователя *User2*, он запрашивает сертификат пользователя *User2*. Так как пользователь *User1* знает пользователя *User2*, то доверяет сертификату и даже может его подписать.

Теперь рассмотрим ситуацию, в которой User1 получает информацию от *User3*. Пользователь *User3* не известен пользователю *User1*, но у пользователя User3 есть сертификат, подписанный пользователем *User2*. Таким образом, рассматриваемая модель распространяется на всю компьютерную сеть. Единственным решением, которое должно приниматься в процессе работы, является число переходов, которому доверяет пользователь. Как правило, это число равно 3 или 4. Кроме того, может возникнуть ситуация, в которой для установления доверия другому пользователю есть два пути. Например, *User2* может использовать два пути установления доверия с пользователем *User5*: один через пользователя *User3* и другой через пользователя User4. Так как оба пользователя *User3* и *User4* сертифицируют пользователя *User5*, пользователь *User2* может быть уверен в сертификате пользователя *User5*.

Главной проблемой, связанной с данной моделью доверия*, является недостаток масштабируемости. Так как модель сети состоит из*

двусторонних взаимоотношений, каждый пользователь должен иметь некоторое число таких взаимосвязей, чтобы пользоваться в сети каким-либо доверием. На практике такие взаимосвязи могут отсутствовать, так как большинство пользователей работают с небольшим числом связей и редко выходят на уровень трех или четырех переходов.

18.1.4 Аутентификация с использованием протоколов открытого ключа

Протоколы открытых ключей позволяют устанавливать авторизованные шифруемые связи между узлами внутренних сетей и в интернете.

Существуют три модели аутентификации, проводимой в этих протоколах; они используются как по отдельности, так и в комбинации.

- ***Аутентификация клиента***. Позволяет серверу Windows 2000 VPN или веб-серверу IIS идентифицировать пользователя с использованием стандартных методов шифрования на открытом ключе. Осуществляет проверку подлинности сертификата клиента и общего ID, а также проверку того, что эти данные сгенерированы бюро сертификатов, корневой сертификат которого установлен в перечне доверенных CA. Эта проверка очень важна, если сервером является банк, который передает конфиденциальную финансовую информацию клиенту и должен подтвердить личность получателя. На рисунке 18.6 отображен процесс аутентификации.

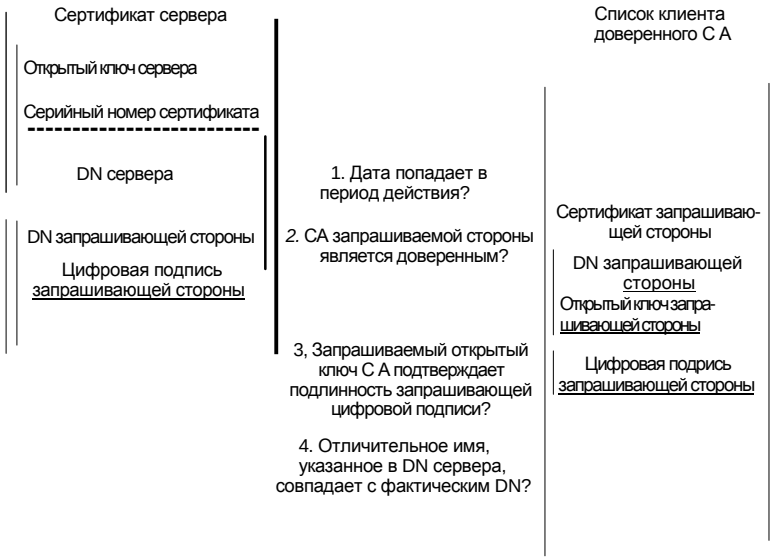


Рис. 18.6 -Аутентификация сервером сертификата клиента

- ***Аутентификация сервера***. Позволяет клиенту VPN или браузеру клиента SSL/TLS подтверждать идентичность сервера, проверяя правильность сертификата сервера и идентификатора ID, а также то, что сертификаты выпущены бюро сертификатов (CA), корневой сертификат которого присутствует в перечне доверенных CA

клиента. Это подтверждение имеет важное значение для пользователя веб-сайта, который отправляет номер кредитной карты через сеть и хочет удостовериться в том, что это именно тот сервер, который ему нужен.

- ***Взаимная аутентификация***. Позволяет клиенту и серверу авторизовать друг друга единовременно. Взаимная аутентификация требует, чтобы клиент и сервер имели цифровые сертификаты и соответствующие корневые сертификаты CA в перечнях доверенных CA.

18.2 Протокол конфиденциального обмена данными SSL

Протокол SSL спроектирован для *обеспечения конфиденциальности обмена между двумя прикладными процессами клиента и сервера* (см. http://www.netscape.com). Он предоставляет возможность аутентификации сервера и, опционно, клиента. SSL требует применения надежного транспортного протокола (например, TCP).

Преимуществом SSL является то, что он независим от прикладного протокола. Протоколы приложения, такие как HTTP, FTP, TELNET и т.д. могут работать поверх протокола SSL совершенно прозрачно. Протокол SSL может согласовывать алгоритм шифрования и ключ сессии, а также аутентифицировать сервер до того как приложение примет или передаст первый байт данных.

Все протокольные прикладные данные в SSL передаются зашифрованными с гарантией конфиденциальности.

Протокол SSL предоставляет «безопасный канал», который имеет три основные свойства.

- *Канал является частным.* Шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа.
- *Канал аутентифицирован.* Серверная сторона диалога всегда аутентифицируется, в то время как клиентская — аутентифицируется опционно.
- Канал надежен. Транспортировка сообщений включает в себя проверку целостности (с привлечением MAC – Message Authentication Code).

Сеанс SSL между клиентом и сервером устанавливается следующим образом.

1. *Клиент открывает сокет и запрашивает подключение к серверу.*
2. *Сервер аутентифицирует клиента (либо по паролю, либо посредством сертификата, отправляемого клиентом).*

3. *После установки соединения сервер передает браузеру свой открытый ключ посредством отправки сертификата сервера, выпущенного доверенным бюро сертификатов.*
4. *Клиент аутентифицирует сертификат.*
5. *Клиент и сервер осуществляют обмен настроечной информацией для определения типа и силы шифрования, используемых в сеансе соединения.*
6. *Клиент создает сеансовый ключ, используемый для шифрования данных.*
7. *Клиент шифрует сеансовый ключ с помощью открытого ключа сервера (полученного из сертификата сервера) и отправляет его серверу. Секретный ключ, с помощью которого можно расшифровать сеансовый ключ, находится только на сервере.*
8. *Сервер расшифровывает сеансовый ключ и использует его для создания безопасной сессии, через которую будет осуществляться обмен данными с клиентом.*

В несколько упрощенном варианте диалог SSL представлен на рис. 18.7.

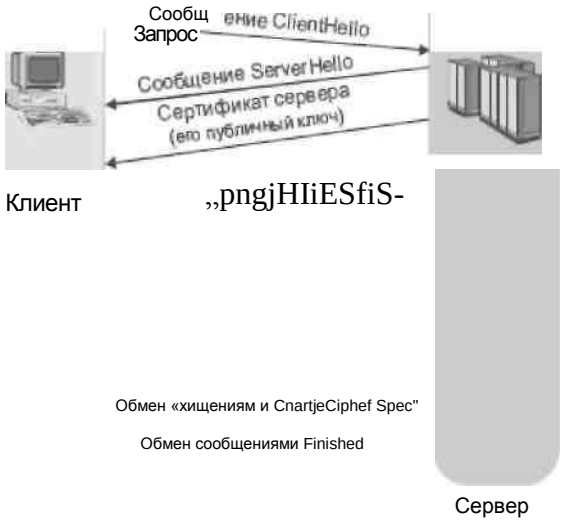


Рис. 18.7 - Алгоритм работы SSL

Необходимым условием успешной реализации этих шагов является заранее установленный на клиенте корневой сертификат, полученный от доверенного бюро сертификатов. При использовании сертификата, полученного от коммерческого CA, корневой сертификат которого уже имеется в Microsoft Internet Explorer и Netscape Communicator (например, Verisign), не нужно беспокоиться об этом. При использовании сертификатов клиентов серверу необходимо установить клиентский корневой сертификат, выпущенный клиентским бюро сертификатов.

*Протокол диалога SSL имеет две основные фазы. Первая фаза используется для установления конфиденциального канала коммуникаций. Вторая служит для аутентификации клиента (*смотри также http://book.itep.ru/6/ssl_65.htm).

Фаза 1.

Первая фаза является фазой инициализации соединения, когда оба партнера посылают сообщения **hello**. Клиент инициирует диалог посылкой сообщения **CLIENT-HELLO**. Сервер, получив это сообщение, обрабатывает его и откликается сообщением **SERVER-HELLO**.

К этому моменту, как клиент, так и сервер имеют достаточно информации, чтобы знать, нужен ли новый **мастерный ключ**. Когда новый мастерный ключ не нужен, клиент и сервер немедленно переходят в **фазу 2.**

Когда нужен новый мастерный ключ, сообщение **SERVER-HELLO** будет содержать достаточно данных, чтобы клиент мог сформировать такой ключ. Сюда входит:

- подписанный сертификат сервера,
- список базовых шифров (см. ниже),
- идентификатор соединения (последний представляет собой случайное число, сформированное сервером и используемое на протяжении сессии).

Клиент генерирует мастерный ключ и посылает сообщение **CLIENT-MASTER-KEY** (или сообщение **ERROR**, если информация сервера указывает, что клиент и сервер не могут согласовать базовый шифр).

Здесь следует заметить, что каждая оконечная точка SSL использует пару шифров для каждого соединения (т.е. всего 4 шифра). На каждой конечной точке, один шифр используется для исходящих коммуникаций и один — для входящих. Когда клиент или сервер генерирует ключ сессии, они в действительности формируют два ключа, **SERVER-READ-KEY** (известный также как **CLIENT-WRITE-KEY**) и **SERVER-WRITE-KEY** (известный также как **CLIENT-READ-KEY**). Мастерный ключ используется клиентом и сервером для генерации различных ключей сессий.

Наконец, после того как мастерный ключ определен, сервер посылает клиенту сообщение **SERVER-VERIFY**. Этот заключительный шаг аутентифицирует сервер, так как только сервер, который имеет соответствующий общедоступный ключ, может знать мастерный ключ.

Фаза 2.

Вторая фаза является фазой аутентификации. Сервер уже аутентифицирован клиентом на первой фазе, по этой причине здесь осуществляется аутентификация клиента. При типичном сценарии серверу необходимо получить что-то от клиента, и он посылает запрос. Клиент пришлет позитивный отклик, если располагает необходимой информацией, или пришлет сообщение об ошибке, если нет. Эта спецификация протокола

не определяет семантику сообщения **ERROR**, посылаемого в ответ на запрос сервера (например, конкретная реализация может игнорировать ошибку, закрыть соединение, и т.д. и, тем не менее, соответствовать данной спецификации). Когда один партнер выполнил аутентификацию другого партнера, он посылает сообщение **finished**. В случае клиента сообщение **CLIENT-FINISHED** содержит зашифрованную форму идентификатора **CONNECTION-ID**, которую должен верифицировать сервер. Если верификация терпит неудачу, сервер посылает сообщение **ERROR**.

Раз партнер послал сообщение **finished** он должен продолжить воспринимать сообщения до тех пор, пока не получит сообщение **finished** от партнера. Как только оба партнера послали и получили сообщения **finished**, протокол диалога SSL закончил свою работу. С этого момента начинает работать прикладной протокол.

18.3 Обеспечение безопасности беспроводных сетей

В беспроводных локальных сетях главным образом используется группа стандартов 802.11x (a, b, g и т. д.) технологии Wi-Fi. Эти стандарты позволяют соединять рабочие станции каналами с пропускной способностью до 54 Мбит/с с использованием беспроводной точки доступа, которая подключается к кабельной сети или напрямую к другой рабочей станции (см. рис. 18.8).

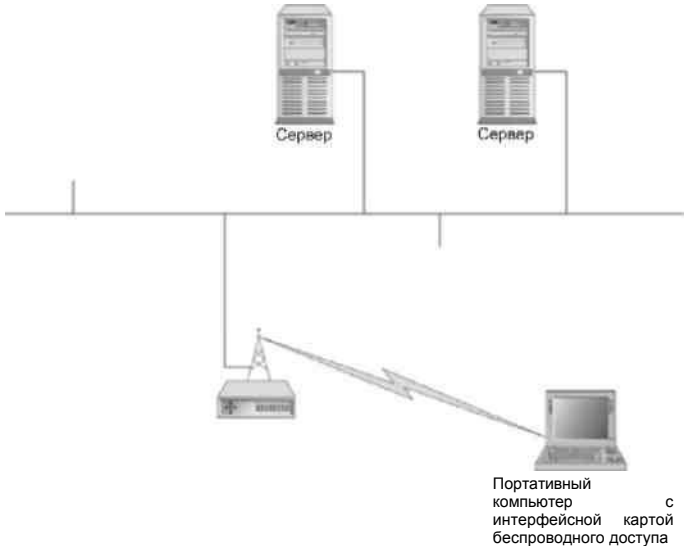


Рис. 18.8 - Типичная архитектура беспроводной сети

Так как беспроводные сети используют воздух и пространство для передачи и приема информации (сигналы являются открытыми для любого лица, находящегося в зоне действия), безопасность передачи данных является очень важным аспектом безопасности всей системы в целом. Без обеспечения должной защиты конфиденциальности и целостности информации при ее передаче между рабочими станциями и точками доступа нельзя быть уверенным в том, что информация не будет перехвачена

злоумышленником, и что рабочие станции и точки доступа не будут подменены посторонним лицом.

18.3.1 Угрозы безопасности беспроводных соединений

18.3.1.1 Обнаружение беспроводных сетей

Обнаружить WLAN очень легко. Действительно, именно для этой цели был разработан ряд средств. Одной из таких утилит является NetStumber (http://www.netstumber.com/); она работает в операционных системах семейства Windows и может использоваться совместно со спутниковым навигатором (ресивером глобальной системы позиционирования, GPS) для обнаружения беспроводных сетей WLAN. Данная утилита идентифицирует SSID сети WLAN, а также определяет, используется ли в ней WEP. Существуют и другие средства, идентифицирующие рабочие станции, подключенные к точке доступа, а также их MAC-адреса например, Kismet (http://www.kismetwireless.net/).

18.3.1.2 Прослушивание

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. Такой подход позволит подключиться к беспроводной сети организации, располагающейся в здании, человеку, сидящему в машине на стоянке рядом с ним (см. рис. 18.10).

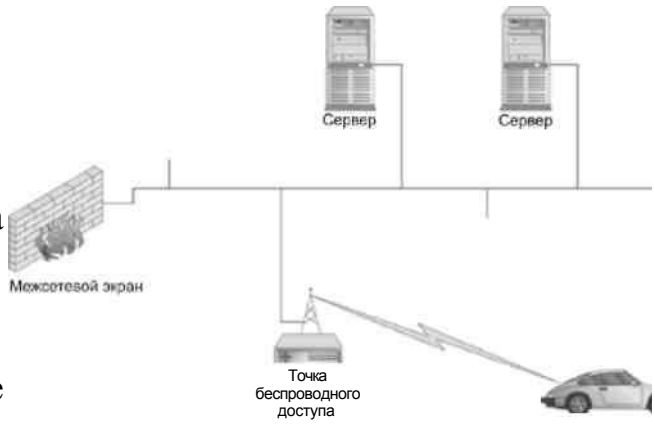


Рис. 18.10 - Прослушивание сети WLAN

18.3.1.3 Активные атаки

Несмотря на то, что прослушивание сети представляет серьезную опасность, активные атаки могут быть еще более опасными. Основной риск, связанный с беспроводными сетями, состоит с том, что злоумышленник может успешно преодолеть периметр сетевой защиты организации. Не следует полагать, что атаки с использованием уязвимостей - это

единственный способ злонамеренного воздействия злоумышленников. Если хакер прослушивает сеть, он может также перехватить пароли и пользовательские идентификаторы. Основные атаки проводимые на WLAN связанны с перехватом информации передаваемой по сети за счет низкой криптостойкости алгоритмов шифрования WEP.

18.3.2 Протокол WEP

Стандарт 802.11x определяет протокол Wired Equivalent Privacy (WEP) для защиты информации при ее передаче через WLAN.

WEP предусматривает обеспечение трех основных аспектов обеспечивающих безопасность.

- ***Аутентификация.*** Служба аутентификации WEP используется для аутентификации рабочих станций на точках доступа. В аутентификации открытых систем рабочая станция рассматривается как аутентифицированная, если она отправляет ответный пакет с MAC-адресом в процессе начального обмена данными с точкой доступа. В реальных условиях данная форма аутентификации не обеспечивает доказательства того, что к точке доступа подключается именно конкретная рабочая станция, а не какой-либо другой компьютер.
- ***Конфиденциальность.*** Механизм обеспечения конфиденциальности базируется на RC4. RC4 - это стандартный мощный алгоритм шифрования, поэтому атаковать его достаточно сложно. WEP определяет систему на базе RC4, обеспечивающую управление ключами, и другие дополнительные службы, необходимые для функционирования алгоритма. WEP поддерживает ключи длиной 40 бит и 128 бит (непосредственный ключ комбинируется с вектором инициализации алгоритма). К сожалению, WEP не определяет механизм управления ключами. Это означает, что многие инсталляции WEP базируются на использовании статических ключей. Действительно, часто на всех рабочих станциях сети используются одни и те же ключи.
- ***Целостность.*** Спецификация протокола WEP включает контроль целостности для каждого пакета. Используемая проверка целостности представляет собой циклическую 32-битную проверку избыточности (CRC). CRC вычисляется для каждого пакета перед его шифрованием, после чего данные в комбинации с CRC шифруются и отправляются в пункт назначения. Несмотря на то что CRC с криптографической точки зрения небезопасна, она защищается шифрованием. Используемая здесь система шифрования может быть достаточно надежной, если алгоритм шифрования обладает достаточной мощностью. Однако недостатки WEP представляют угрозу и для целостности пакетов.

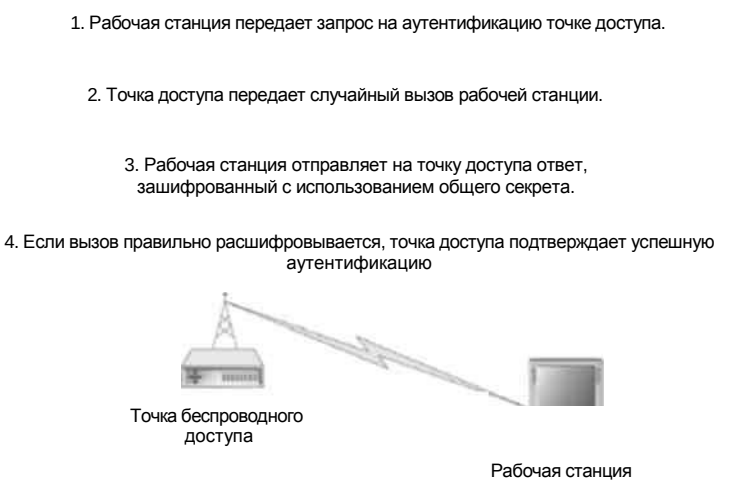


Рис. 18.11 - Аутентификационный обмен WEP

WEP предусматривает использование службы аутентификации. К сожалению, эта служба осуществляет только аутентификацию рабочей станции относительно AP. Она не обеспечивает взаимную аутентификацию, поэтому рабочая станция не получает доказательства того, что AP действительно является авторизованной точкой доступа в данной сети. Таким образом, использование WEP не предотвращает перехват данных или атаки через посредника (см. рис. 18.12).

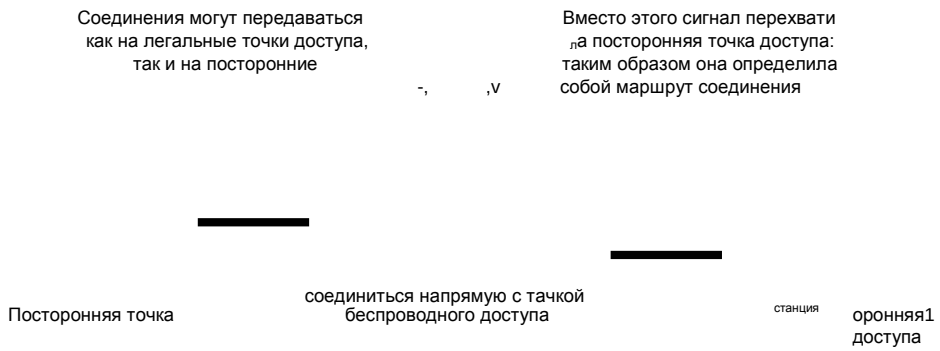


Рис. 18.12 - Атака на WEP через посредника **18.3.3**

Протокол 802.1X - контроль доступа в сеть по портам

Протокол 802.1X разработан в качестве надстройки для всех протоколов контроля доступа 2 уровня, включая Ethernet и WLAN. Так как данный протокол был разработан в то время, когда создатели WLAN искали решения проблем, связанных с WEP, он пришелся как нельзя кстати.

Протокол предназначен для обеспечения обобщенного механизма аутентификации при доступе в сеть и предусматривает следующий набор элементов:

1. **Аутентификатор**. Сетевое устройство, осуществляющее поиск других объектов для аутентификации; для WLAN это может быть AP.

2. **Соискатель**. Объект, которому требуется доступ. В случае с WLAN это может быть рабочая станция.
3. **Сервер аутентификации**. Источник служб аутентификации. 802.1X разрешает централизацию этой функции, поэтому данный сервер является, например, сервером RADIUS.
4. **Сетевая точка доступа**. Точка присоединения рабочей станции к сети. По сути, это порт на коммутаторе или концентраторе. В беспроводной технологии является связью между рабочей станции и точкой доступа.
5. **Процесс доступа через порт (PAE).** PAE - это процесс, выполняющий протоколы аутентификации. PAE есть как у аутентификатора, так и у соискателя.
6. **Расширяемый протокол аутентификации (EAP).** Протокол EAP (определен в стандарте RFC 2284) представляет собой протокол, используемый при обмене аутентификационными данными. Поверх EAP могут работать и другие протоколы аутентификации более высокого уровня.

Использование протокола 802.1X позволяет применить более надежный механизм аутентификации, нежели возможности, доступные в 802.11x. При использовании совместно с сервером RADIUS становится возможным централизованное управление пользователями.

18.4 Обеспечение безопасности элекгонной почты

18.4.1 Риски, связанные с использованием электронной почты

Электронная почта — один из наиболее широко используемых видов сервиса, как в корпоративных сетях, так и в Интернет. Она является не просто способом доставки сообщений, а важнейшим средством коммуникации, распределения информации и управления различными процессами в бизнесе. Роль электронной почты становится очевидной, если рассмотреть функции, которые выполняет почта:

- Обеспечивает внутренний и внешний информационный обмен;
- Является компонентом системы документооборота;
- Формирует транспортный протокол корпоративных приложений;
- Является средством образования инфраструктуры электронной коммерции.

Благодаря выполнению этих функций электронная почта решает одну из важнейших на настоящий момент задач — **формирует единое информационное пространство**. В первую очередь это касается создания общей коммуникационной инфраструктуры, которая упрощает обмен информацией между отдельными людьми, подразделениями одной компании и различными организациями.

Электронная почта обладает рядом преимуществ по сравнению с обычными способами передачи сообщений (традиционная почта или факсимильная связь). К ним относятся следующие.

1. Оперативность и легкость использования.
2. Доступность практически в любом месте.
3. Универсальность форматов писем и вложений.
4. Дешевизна сервиса.
5. Надежность и скорость инфраструктуры доставки.
6. Использование для обработки электронной почты прикладного специального программного обеспечения.

Электронная почта обладает многочисленными достоинствами, но именно из-за этих достоинств возникают основные риски, связанные с ее использованием. К примеру, доступность электронной почты превращается в недостаток, когда пользователи начинают применять почту для рассылки спама, легкость в использовании и бесконтрольность приводит к утечкам информации, возможность пересылки разных форматов документов — к распространению вирусов и т.д.

В конечном итоге любой из этих рисков может привести к серьезным последствиям для компании. Это и потеря эффективности работы, и снижение качества услуг информационных систем, и разглашение конфиденциальной информации. Недостаточное внимание к данной проблеме грозит значительными потерями в бизнесе, а в некоторых случаях даже привлечением к юридической ответственности в связи с нарушением законодательства.

Компания подвергается данным рискам в силу ряда свойств электронной почты. Например, благодаря применению MIME-стандарта электронная почта может переносить большие объемы информации различных форматов данных в виде прикрепленных к сообщениям файлов. Такой возможностью сразу воспользовались злоумышленники.

Достоинство электронной почты превратилось в угрозу, поскольку электронная почта стала представлять собой практически идеальную среду для переноса различного рода «опасных» вложений, а именно компьютерных вирусов, вредоносных программ, «троянских» программ и т.п.

Если надлежащий контроль за использованием электронной почты не обеспечен, это может привести к чрезвычайно серьезным последствиям и даже нанести непоправимый ущерб. Избавиться от данного риска можно лишь путем блокировки писем с «опасными» вложениями, а также антивирусной проверки прикрепленных файлов. На практике же оптимальным средством может оказаться **блокировка определенных типов файлов**. Это, как правило, исполняемые файлы (exe, com, bat) и файлы, содержащие макросы и OLE-объекты (файлы, созданные в приложениях MS Office).

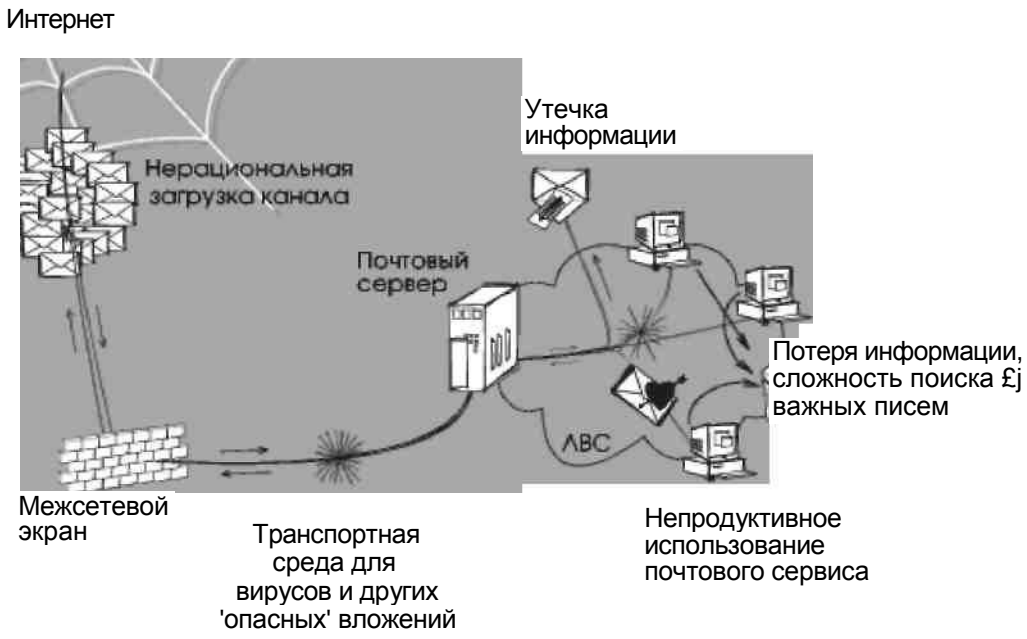


Рис. 18.12 - Негативное воздействие различных факторов на незащищенную почтовую систему

Серьезную опасность для корпоративной сети представляют различного рода **атаки с целью «засорения» почтовой системы.** Это, в первую очередь, пересылка в качестве вложений в сообщениях электронной почты файлов больших объемов или многократно заархивированных файлов. «Открытие» таких файлов или попытка «развернуть» архив может привести к «зависанию» системы. При этом одинаково опасны как умышленные атаки этого типа, например, «отказ в обслуживании» (Denial of Service) и «почтовые бомбы» (mail-bombs), так и «неумышленные», когда пользователи отправляют электронные письма с вложениями большого объема, просто не подумав о том, к каким последствиям может привести открытие подобного файла на компьютере адресата.

Действенный способ избавиться от «засорения» почтовой системы и ее перегрузки — фильтрация по объему передаваемых данных, по количеству вложений в сообщения электронной почты и глубине вложенности архивированных файлов.

Другой особенностью электронной почты является ее доступность и простота в использовании. Во многом результатом этого стало широкое и повсеместное применение этого вида сервиса Интернет. Стихийность развития и отсутствие единых правил функционирования почтового сервиса привели к неконтролируемому использованию электронной почты, а в связи с этим, и к возникновению целого ряда рисков, связанных с неуправляемой циркуляцией электронной почты в сети.

Отсутствие контроля над почтовым потоком, как правило, становится причиной того, что сотрудники компании **используют электронную почту в**

целях, не связанных с деятельностью компании (например, для обмена видео-файлами и графикой, частной переписки, ведения собственного бизнеса с использованием почтовых ресурсов компании, рассылки резюме в различные организации и т.п.).

Кроме того, к такому же результату может привести **непродуктивное использование почтовых ресурсов** в трудовой деятельности сотрудников (например, чрезмерное увлечение почтовой перепиской в случаях, когда необходимости в такой переписке нет, использование электронной почты не по назначению и т.п.). Причиной этого, как правило, является отсутствие в компании правил, регламентирующих использование системы электронной почты. Последствиями непродуктивного использования почтового сервиса являются снижение производительности труда в компании, а также излишние финансовые затраты. Сэкономить средства в значительной степени поможет **проведение анализа эффективности использования системы электронной почты, который основывается на базе статистических данных о функционировании системы. Подобную статистику возможно получить лишь в случае ведения архива электронной почты.** Обработка информации, содержащейся в архиве, позволяет получать отчеты о различных параметрах электронной почты, ее объемах и структуре, представить наглядную картину использования почтового трафика сотрудниками компании, а это, в свою очередь, поможет предотвратить использование электронной почты, несвязанное с деятельностью компании, и повысить эффективность работы корпоративной почтовой системы.

Передача в электронных письмах графических, видео и звуковых файлов, которые, как правило, имеют **большой объем** даже если такая передача предусмотрена условиями ведения бизнеса, приводит к значительной перегрузке сети, соответственно к дополнительным финансовым затратам на ее обслуживание. Избежать этого, а значит и добиться значительной экономии средств компании, поможет, так называемая, **отложенная доставка писем**, которая позволяет доставлять сообщения больших объемов в то время, когда загрузка сети не имеет критического значения (например, в ночное время, в выходные дни и т.п.).

К «засорению» трафика также ведет рассылка **спама**. Как правило, это письма, содержащие навязчивые предложения самых разнообразных услуг, товаров и т.п. Такого рода почта является «группой риска» с точки зрения переноса вирусов. Большое количество ненужной почты загружает каналы, «замусоривает» почтовые ящики, отнимает время на удаление ненужных писем и повышает вероятность случайного удаления нужных. Конечно рассылка, например, сообщений рекламного характера, напрямую не преследует цели «засорить» почтовую систему организации, однако косвенно приводит к негативным последствиям. Использование списков рассылки, в которую могут входить все пользователи одной корпоративной сети, и получение одновременно всеми этими пользователями сообщений рекламного характера грозит компании снижением производительности ее

сетевых ресурсов. **Блокировка спама**, в первую очередь, связана с контекстным анализом сообщений, то есть проверкой электронной почты на наличие ключевых слов и выражений, которые обычно употребляются в сообщениях рекламного характера.

Переписка с внешними корреспондентами представляет наибольшую угрозу из-за особенностей электронной почты (невозможность контролировать маршрут передачи писем, а также их копирование и перенаправление, осуществлять аутентификацию отправителя/получателя, возвращать письма после их отправления). Кроме того невозможен либо затруднен контроль количества отправляемых копий письма. Содержимое сообщения может быть прочитано в процессе передачи его по Интернету, поскольку заголовки и содержимое электронных писем часто передаются в открытом виде.

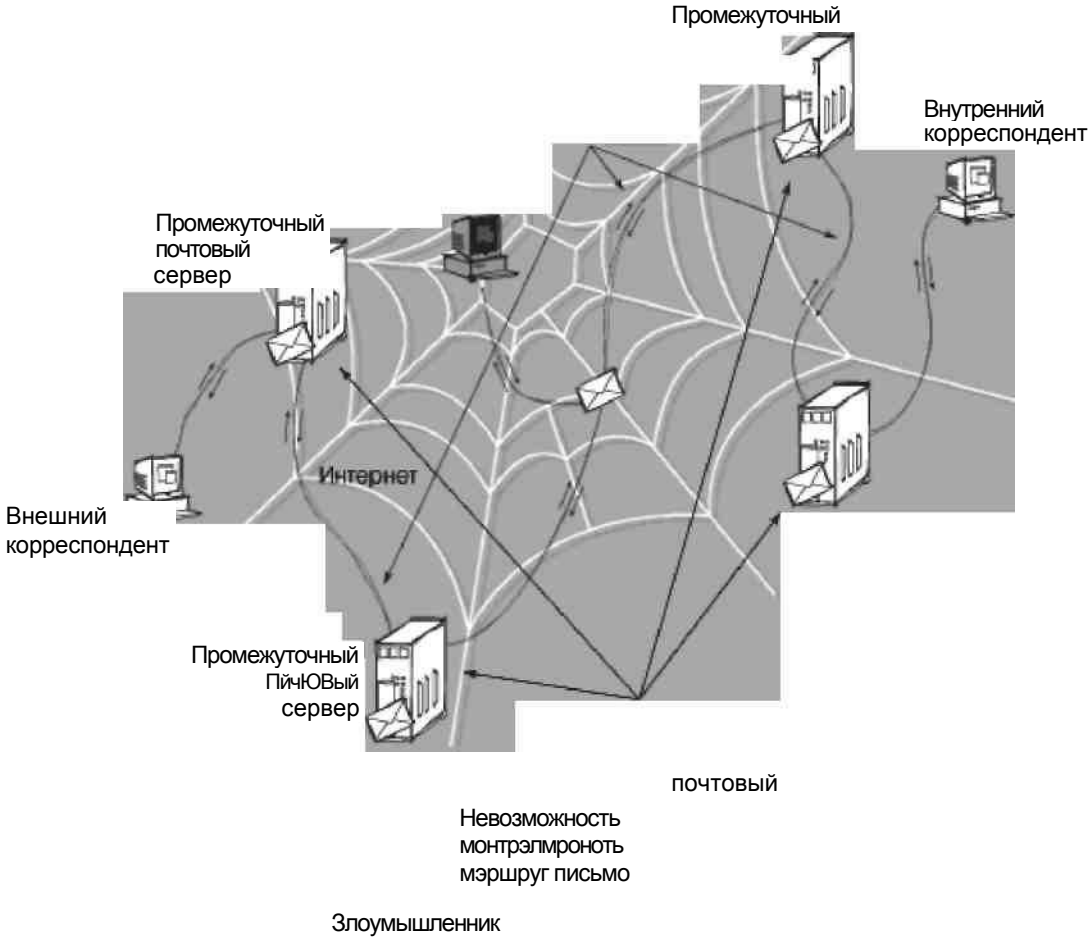
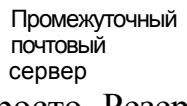


Рис. 18.13 - Проблемы, возникающие при пересылке электронной почты через Интернет

Другой проблемой, связанной с особенностями электронной почты, является то, что электронная почта позволяет неконтролируемое накопление информации в архивах и практически неуничтожима. В противоположность



бытующему мнению, удалить электронную почту непросто. Резервные копии сообщений могут оставаться на персональных компьютерах отправителя и

получателя или в сети компаний, где они работают. Если электронное почтовое сообщение отправлено через коммерческую службу или через Интернет, то оно будет передаваться через несколько различных серверов.

Каждый сервер в цепочке между отправителем и получателем может сохранить копию сообщения в своих архивах. Даже методичное выяснение местонахождения каждой копии электронного письма с последующим его удалением не дает никакой гарантии того, что сообщение не осталось на жестком диске компьютера или сервера.

Все эти особенности, а также простота копирования электронного сообщения и невозможность проконтролировать данную операцию приводят к тому, что сотрудник может передать корпоративную информацию любому количеству людей как внутри, так и за пределами компании анонимно и без соответствующего разрешения, сразу или по истечении какого-либо времени. При этом, такая информация может представлять собой служебную информацию компании это грозит серьезным нарушением конфиденциальности и может привести к неприятным для компании последствиям.

Чтобы обеспечить **защиту от утечки конфиденциальной информации** из сети, необходимо осуществлять контроль адресатов, **фильтрацию** передаваемых данных на наличие в текстах сообщений или в прикрепленных к электронному письму файлах **слов и выражений, имеющих отношение к «закрытой» тематике**, осуществлять разграничение доступа различных категорий пользователей к архивам электронной почты и т.п.

Одно из основных отличий электронной почты состоит в формальном к ней отношении (по сравнению с другими видами коммерческих коммуникаций):

- Во-первых, большинство пользователей относятся к электронной почте как к чему-то временному, то есть поступают с ней по принципу «прочитал и выкинул». При таком отношении существует риск **случайного удаления значимой информации**. Кроме того, существует опасность **потери переписки с важным клиентом**. Все эти проблемы решаются путем **создания в организации архива электронной почты.**
- Во-вторых, такое отношение к электронной почте приводит к тому, что из-за кажущейся недолговечности электронных сообщений люди часто используют их для того, чтобы выразить чувства и мнения в выражениях, которые они никогда не позволили бы себе употребить в традиционных письмах. Публикация таких писем в сети может нанести серьезный ущерб репутации компании или явиться причиной юридических исков к ней.

Еще одна область связана с возможностью привлечения к юридической ответственности компании и ее сотрудников — **за нарушение авторского права**. Защищенные этим правом материалы могут содержаться или в сообщении электронной почты, или в присоединенных файлах. К подобным материалам относятся графическая, аудио, видео и различная текстовая информация, т. е. любая информация, которая может быть представлена в

электронном виде и передана по компьютерным сетям. Копирование или распространение этих материалов без предварительного согласия автора или владельца авторских прав является нарушением закона. Если компания допускает, чтобы материалы почты, защищенные авторским правом, использовались сотрудниками, не имеющими на это полномочий, то она может быть привлечена к ответственности за прямое или косвенное пособничество нарушению авторского права.

18.4.2 Средства обеспечения безопасности электронной почты

Учитывая описанные выше риски, связанные с использованием электронной почты, организациям необходимо принять соответствующие меры для защиты от них.

Подход к защите должен быть всесторонним и комплексным — необходимо сочетать организационные меры с использованием соответствующих технических средств.

К организационным мерам относятся разработка и внедрение в компании политики использования электронной почты. Технические средства должны обеспечить выполнение данной политики как за счет мониторинга почтового трафика, так и за счет адекватного реагирования на нарушения.

Очень важно отметить, что политика использования электронной почты первична по отношению к средствам ее реализации, поскольку составляет основу для формирования комплекса мер по защите информационной системы от вышеперечисленных рисков. Сначала необходимо сформулировать политику, составить правила использования электронной почты, определить, как созданная система должна реагировать на определенные нарушения данной политики и только затем переводить правила на компьютерный язык того средства, которое используется для контроля выполнения положений политики использования электронной почты.

К таким техническим средствам относится специальное программное обеспечение, называемое **система контроля содержимого электронной почты** (content security software). В функции таких систем входит контроль почтового трафика и ведение архива переписки по электронной почте. К данным системам предъявляются следующие требования:

- Проведение текстового анализа;
- Фильтрация передаваемых данных:
  1. по размеру и объему данных;
  2. по количеству вложений в сообщения электронной почты;
  3. по типу файлов (вложенных в электронную почту);
  4. по адресу электронной почты;
- Контроль использования почтовых ресурсов и разграничение доступа к ним различных категорий пользователей;

- Отложенную доставку сообщений электронной почты по расписанию;
- Ведение полнофункционального архива электронной почты.

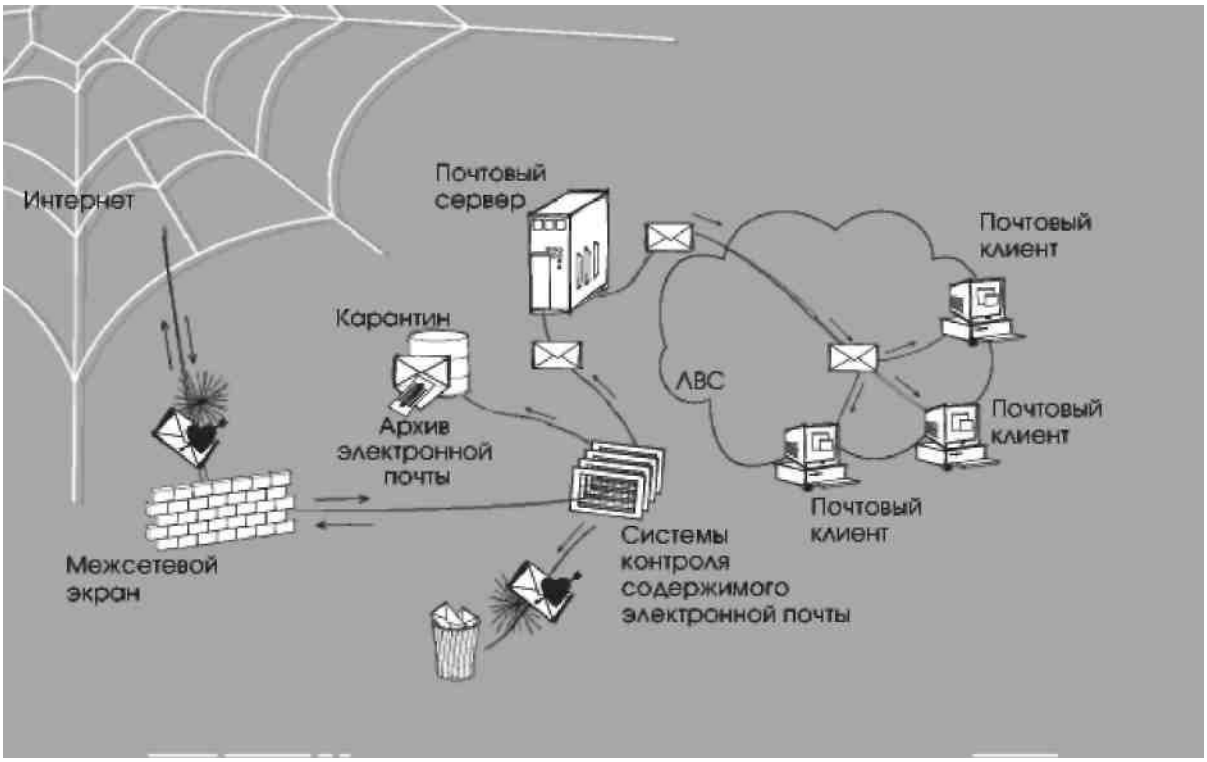


Рис. 18.14 - Решение проблем защиты почтовой системы

Выполнение этих требований обеспечивается применением в средствах защиты определенных механизмов. К таким механизмам могут относиться:

1. Рекурсивная декомпозиция (специальный алгоритм, применяемый для разбора сообщений электронной почты на составляющие компоненты с последующим анализом их содержимого);
2. Эвристическое определение кодировок текстов;
3. Определение типа файлов по сигнатуре;
4. Полнотекстовый поиск по архиву электронной почты и т.п.

18.4.3 Политика использования электронной почты

Средство защиты — система контроля содержимого электронной почты, само по себе никаких задач по обеспечению безопасности не решает. Это всего лишь «машина», которая помогает человеку в решении данной проблемы. Поэтому задачу по обеспечению безопасности необходимо такой «машине» поставить. Это означает, что должен быть выработан специальный набор правил, который в дальнейшем будет переведен на язык машины.
Данный набор правил называется «политикой использования электронной почты».

Во многих организациях такие правила существуют уже длительное время. Как и всякая ограничительная мера, они создают определенные

неудобства пользователям системы, а если пользователю что-то неудобно, он либо перестает этим пользоваться, либо старается обойти препятствия. Поэтому такого рода политики, не подкрепленные техническими средствами контроля за их выполнением, постепенно теряют силу. Программные системы, ориентированные на фильтрацию почты, следует позиционировать именно как инструмент для внедрения и контроля исполнения этих правил.

Таким образом, ***политика использования электронной почты — это закрепленные в письменном виде и доведенные до сотрудников инструкции и другие документы, которые регламентируют их деятельность и процессы, связанные с использованием системы электронной почты.*** Данные документы и инструкции обладают юридическим статусом и, как правило, предоставляются для ознакомления сотрудникам организации.

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности и неотделима от нее.

Политика должна соответствовать следующим критериям:

- Быть лаконично изложенной и понятной всем сотрудникам компании, простота написания не должна привести к потере юридического статуса документа;
- Исходить из необходимости защиты информации в процессе экономической деятельности компании;
- Быть согласованной с другими организационными политиками компании (регламентирующими финансовую, экономическую, юридическую и другие сферы деятельности компании);
- Иметь законную силу, т.е. политика, как документ, должна быть одобрена и подписана всеми должностными лицами руководящего звена компании, а ее выполнение должно быть детально продумано;
- Не противоречить федеральным и местным законам;
- Определять меры воздействия на сотрудников, нарушивших положения данной политики;
- Соблюдать баланс между степенью защищенности информации и продуктивностью деятельности компании;
- Детально определять мероприятия по обеспечению политики использования электронной почты в компании.

Политика использования электронной почты, как правило, рассматривается с двух сторон — как официально оформленный юридический документ и как материал, который описывает технику реализации политики.

Как документ политика должна включать:

- Положение, что электронная почта является собственностью компании и может быть использована только в рабочих целях.

- Указание на то, что применение корпоративной системы электронной почты не должно противоречить законодательству РФ и положениям политики безопасности.
- Инструкции и рекомендации по использованию и хранению электронной почты.
- Предупреждение о потенциальной ответственности сотрудников компании за злоупотребления при использовании электронной почты в личных целях и возможном использовании электронной почты в судебных и служебных разбирательствах.
- Письменное подтверждение того, что сотрудники компании ознакомлены с политикой использования электронной почты и согласны с ее положениями.

С технической точки зрения политика устанавливает правила использования электронной почты, то есть определяет следующее:	
Что контролируется	Прохождение каких сообщений входящей, исходящей или внутренней электронной почты должно быть разрешено или запрещено.
На кого распространяется	Категории лиц, которым разрешено или запрещено отправлять исходящие или получать входящие сообщения электронной почты.
Как реагирует система	Что необходимо делать с теми или иными сообщениями электронной почты, которые удовлетворяют или не удовлетворяют критериям, определенным правилами использования электронной почты.

18.4.4 Системы контроля содержимого электронной почты

Внедрение политики использования электронной почты требует от руководства компании понимания, что наличие только документально оформленной политики не гарантирует ее выполнения. Необходимо создание в компании соответствующих условий реализации данной политики. При этом важнейшим условием является наличие в корпоративной сети программно-технических средств контроля выполнения положений и требований политики. К таким средствам относятся системы контроля содержимого электронной почты.

Системы контроля содержимого электронной почты — это программное обеспечение, способное анализировать содержание письма по различным компонентам и структуре в целях реализации политики использования электронной почты.

К особенностям данных продуктов относятся:

1. Применение при анализе содержания специально разработанной политики использования электронных писем.

2. Способность осуществлять «рекурсивную декомпозицию» электронных писем.
3. Возможность распознавания реальных форматов файлов вне зависимости от различных способов их маскировки (искажение расширения файлов, архивирование файлов и т.п.).
4. Анализ множества параметров сообщения электронной почты.
5. Ведение архива электронной почты
6. Анализ содержимого сообщения электронной почты и прикрепленных файлов на наличие запрещенных к использованию слов и выражений.

Системы контроля электронной почты помимо основной своей задачи мониторинга почтового трафика способны выполнять и другие функции. Практика показала, что в настоящее время такие системы используются в качестве:

1. Средств управления почтовым потоком.
2. Средств управления доступом.
3. Средств администрирования и хранения электронной почты.
4. Средств аудита контента (важнейшую функцию которого осуществляет архив электронной почты).
5. Основы системы документооборота.

18.4.5 Требования к системам контроля содержимого электронной почты

Спектр возможностей всех категорий систем контроля содержимого электронной почты достаточно широк и существенно меняется в зависимости от производителя. Однако ко всем системам предъявляются наиболее общие требования, которые позволяют решать задачи, связанные с контролем почтового трафика.

Основныме требования предьявляемые к таким системам - полнота и адекватность

1. ***Полнота*** *— это способность систем контроля обеспечить наиболее глубокую проверку сообщений электронной почты.* Это предполагает, что фильтрация должна производиться по всем компонентам письма. При этом ни один из объектов, входящих в структуру электронного сообщения, не должен быть «оставлен без внимания». Условия проверки писем должны учитывать все проблемы, риски и угрозы, которые могут существовать в организации, использующей систему электронной почты.

2. ***Адекватность*** *— это способность систем контроля содержимого как можно более полно воплощать словесно сформулированную политику использования электронной почты, иметь все необходимые средства реализации написанных людьми правил в понятные системе условия фильтрации.*

К другим наиболее общим требованиям относятся:

3. ***Текстовый анализ электронной почты*** - анализ ключевых слов и выражений с помощью встроенных словарей. Данная возможность позволяет обнаружить и своевременно предотвратить утечку конфиденциальной информации, установить наличие запрещенного содержания, остановить рассылку спама, а также передачу других материалов, запрещенных политикой безопасности. При этом качественный анализ текста должен предполагать морфологический анализ слов, то есть система должна иметь возможность генерировать и определять всевозможные грамматические конструкции слова. Эта функция приобретает большое значение в связи с особенностями русского языка, в котором слова имеют сложные грамматические конструкции.

4. ***Контроль отправителей и получателей сообщений электронной почты.*** Данная возможность позволяет фильтровать почтовый трафик, тем самым реализуя некоторые функции межсетевого экрана в почтовой системе.

5. ***Разбор электронных писем на составляющие их компоненты*** (MIME-заголовки, тело письма, прикрепленные файлы и т.п.), устранение «опасных» вложений и последующий сбор компонентов письма воедино, причем с возможностью добавлять к сообщению электронной почты необходимые для администраторов безопасности элементы (например, предупреждения о наличии вирусов или «запрещенного» текста в содержании письма).

6. ***Блокировка или задержка сообщений большого размера*** *до того момента, когда канал связи будет менее всего загружен (например, в нерабочее время).* Циркуляция в почтовой сети компании таких сообщений может привести к перегрузке сети, а блокировка или отложенная доставка позволит этого избежать.

7. ***Распознавание графических, видео и звуковых файлов.*** Как правило, такие файлы имеют большой размер, и их циркуляция может привести к потере производительности сетевых ресурсов. Поэтому способность распознавать и задерживать данные типы файлов позволяет предотвратить снижение эффективности работы компании.

8. ***Обработка сжатых/архивных файлов.*** Это дает возможность проверять сжатые файлы на содержание в них запрещенных материалов.

9. ***Распознавание исполняемых файлов.*** Как правило, такие файлы имеют большой размер и редко имеют отношение к коммерческой деятельности компании. Кроме того, исполняемые файлы являются основным источником заражения вирусами, передаваемыми с электронной почтой. Поэтому способность распознавать и задерживать данные типы файлов позволяет предотвратить снижение эффективности работы компании и избежать заражения системы.

10. ***Контроль и блокирование спама.*** Циркуляция спама приводит к перегрузке сети и потере рабочего времени сотрудников. Функция контроля и блокирования спама позволяет сберечь сетевые ресурсы и предотвратить

снижение эффективности работы компании. Основными способами защиты от спама являются: проверка имен доменов и IP-адресов источников рассылки спама по спискам, запрос на указанный адрес отправителя (блокировка в случае отсутствия ответа), текстовый анализ спам-сообщения на наличие характерных слов и выражений в заголовках электронной почты (from/subject), проверка заголовков на соответствие спецификации RFC-822 и т.п.

11. ***Способность определять число вложений в сообщениях электронной почты.*** Пересылка электронного письма с большим количеством вложений может привести к перегрузке сети, поэтому контроль за соблюдением определенных политикой информационной безопасности ограничений на количество вложений обеспечивает сохранение ресурсов корпоративной сети.

12. ***Контроль и блокирование программ-закладок*** (cookies), вредоносного мобильного кода (Java, ActiveX, JavaScript, VBScript и т.д.), а также файлов, осуществляющих автоматическую рассылку (так называемые «Automatic Mail-to»). Эти виды вложений являются крайне опасными и приводят к утечке информации из корпоративной сети.

13. ***Категоризация ресурсов почтовой системы компании*** («административный», «отдел кадров», «финансы» и т.д.) и разграничение доступа сотрудников компании к различным категориям ресурсов сети (в т.ч. и в зависимости от времени суток).

14. ***Реализация различных вариантов реагирования***, в том числе: удаление или временная блокировка сообщения; задержка сообщения и помещение его в карантин для последующего анализа; «лечение» зараженного вирусом файла; уведомление администратора безопасности или любого другого адресата о нарушении политики безопасности и т.п.

15. ***Возможность модификации данных***, которая предусматривает, например, удаление неприемлемых вложений и замену их на тексты заданного содержания. Такая возможность позволит администратору удалять из писем прикрепленные файлы, тип которых запрещен политикой безопасности компании. К таким типам могут относиться исполняемые, видео и звуковые файлы, не имеющие отношения к деятельности компании. А это, в конечном итоге, позволит избежать заражения сети вирусами и добиться от сотрудников продуктивного использования почтового сервиса.

16. ***Ведение полнофункционального архива электронной почты,*** *способного обеспечить хранение в режиме on-line большого количества электронной почты с высоким уровнем доступности данных.* На основании хранящейся в архиве информации, возможно проводить дальнейший анализ почтового потока компании, корректировать работу системы, осуществлять анализ инцидентов, связанный с злоупотреблением сотрудниками компании почтовым сервисом и т.п.

На Рис. 18.15 представлена последовательность работы типичной системы контроля содержимого электронной почты. Схема обработки сообщения, как правило, включает в себя следующие этапы: рекурсивная декомпозиция электронного письма; анализ содержимого электронного письма; «категоризация» электронного письма (отнесение к определенной категории); действие над письмом по результатам присвоения категории.

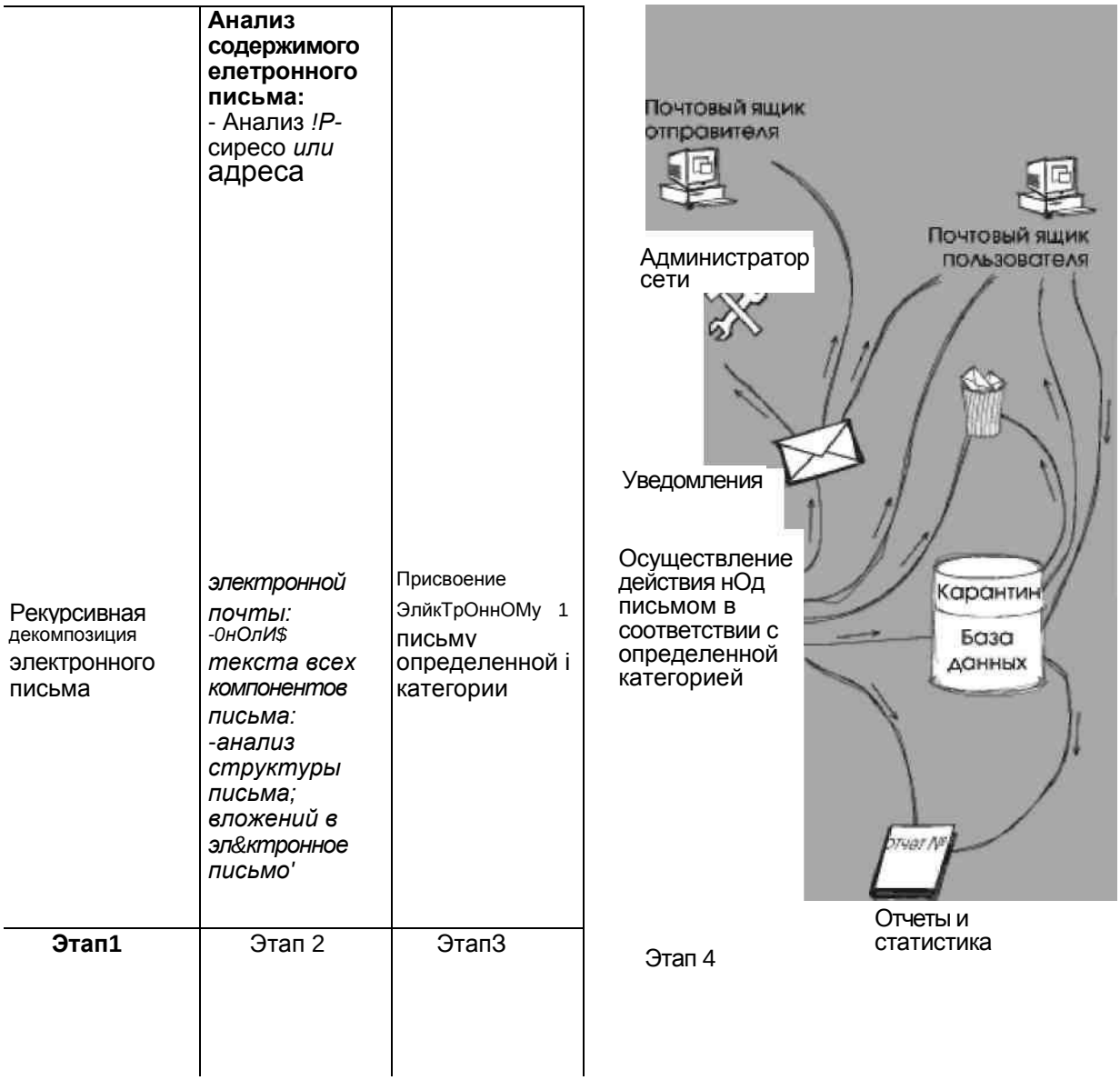


Рис. 18.15 - Схема обработки сообщения системой контроля содержимого электронной почты

18.4.6 Принципы функционирования систем контроля содержимого электронной почты

Каждое попадающее в систему электронное письмо должно проверяться на соответствие заданным условиям. При этом, по меньшей мере, должны выполняться следующие условия отбора писем:

- условия на почтовые заголовки;

- условия на структуру письма (наличие, количество и структура вложений);
- условия на типы вложений (MS Office, исполняемые, архивы и т.п.);
- условия на содержимое (текст) писем и вложений;
- условия на результат обработки письма.

Кроме того, система должна позволять анализировать почтовые сообщения по всем их составляющим: атрибутам конверта, заголовкам сообщения, MIME-заголовкам, телу сообщения, присоединенным файлам.

18.4.6.1 Категоризация писем и фильтрация спама

Рассмотрим вопрос категоризации писем. Важно отметить, что гибкость при фильтрации почтовых сообщений особенно необходима, когда это касается такой проблемы, как спам. Одним из главных критериев выбора системы контроля содержимого электронной почты в настоящее время является как раз ее способность как можно более качественно справляться с данной проблемой.

Существует четыре основные методики определения, какое письмо относится к спаму, а какое нет.

1. *Выявление спама по наличию в письме определенных признаков*, таких как наличие ключевых слов или словосочетаний, характерное написание темы письма (например, все заглавные буквы и большое количество восклицательных знаков), а также специфическая адресная информация.

2. *Определение адреса отправителя и его принадлежности к, так называемым, «черным спискам» почтовых серверов Open Relay Black List (ORBL).* В эти списки заносятся те серверы, которые замечены в массовых рассылках спама и идея состоит в том, чтобы вообще не принимать и не транслировать почту, исходящую с этих серверов.

3. *Совместное использование методик по фильтрации по определенным признакам и проыеркой «черных списко».* По продуктивности мало чем отличается от двух первых. Результаты тестирования хорошо настроенного фильтра с применением обеих методик показывают, что из 100% спам-сообщений обнаруживается только 79,7%. При этом был выявлен значительный процент ложных срабатываний, а это значит, что к спаму были отнесены обычные письма (1,2% от задержанных писем), а это грозит для компании потерей важной информации. Некачественное разделение спама и обычных писем обусловлено, в том числе и некоторой «однобокостью» стандартных фильтров. При отбраковке писем учитываются «плохие» признаки и не учитываются «хорошие», характерные для полезной переписки.

4. *автоматическая настройка фильтров согласно особенностям индивидуальной переписки, а при обработке учет признаков как «плохих»,*

так и «хороших» фильтров. Эта четвертая методика, предложенная американским программистом и предпринимателем Полом Грэмом. Методика основывается на теории вероятностей и использует для фильтрации спама статистический алгоритм Байеса. По имеющимся оценкам, этот метод борьбы со спамом является весьма эффективным. Так, в процессе испытания через фильтр были пропущены 8000 писем, половина из которых являлась спамом. В результате система не смогла распознать лишь 0,5% спам-сообщений, а количество ошибочных срабатываний фильтра оказалось нулевым.

Требование полного разбора письма при решении задачи категоризации следует дополнить требованием устойчивости.

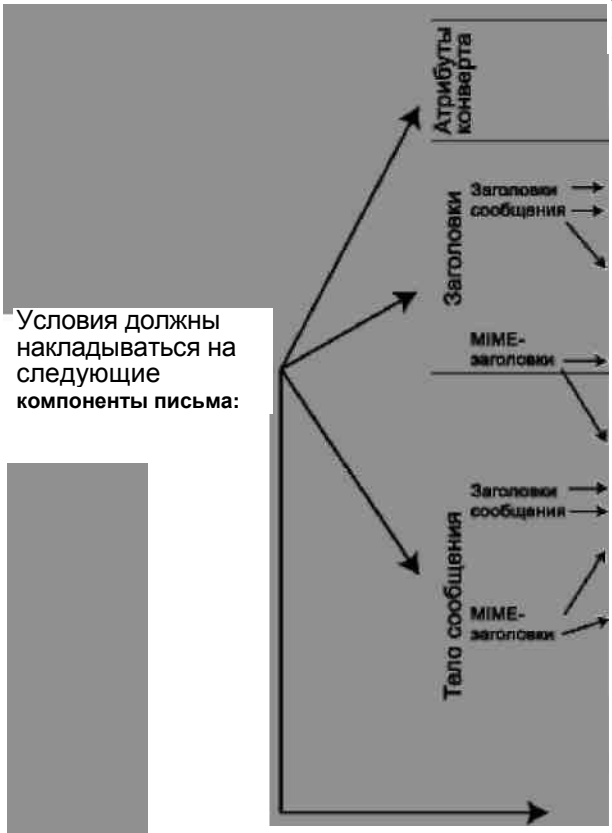
- *Во-первых, система должна быть устойчивой по отношению к обработке писем с некорректной стрктурой.* Структура письма подчиняется определенным правилам. Разбор письма на составляющие основан на применении этих правил к конкретному письму. Возможны случаи, когда почтовая программа автора письма формирует письмо с нарушением этих правил. В этом случае письмо не может быть корректно разобрано..
- *Во-вторых, система должна надежно определять типы файлов-вложений.* Под «надежностью» имеется в виду определение, не основанное на имени файла, а также на информации, вписываемой в письмо почтовым клиентом при прикреплении файла (mime-type). Такая информация может быть недостоверна либо в результате сознательных попыток обмануть систему контроля, либо в результате неправильных настроек почтовой программы отправителя. Бессмысленно запрещать пересылку файлов типа JPEG, если файл picture.jpg после переименования в page.txt пройдет незамеченным.
- *В-третьих, система болжна обеспечивать полноту проводимых проверок, то есть высокое количество и разнообразие критериев анализа электронной почты.* При этом система должна осуществлять фильтрацию по любым атрибутам сообщений, по объему сообщений и вложенных файлов, по количеству и типу вложений, по глубине вложенности, а также уметь анализировать содержимое прикрепленных файлов вне зависимости от того, являются ли эти файлы сжатыми или архивными. Существенным преимуществом многих продуктов является возможность создания собственного сценария обработки сообщений электронной почты.

При анализе текста нужно иметь возможность работать с нормализованными словоформами и т.д.

18.4.6.2 Реализациия политики использования

Рассмтрим не отдельные правила, а все множество правил, составляющих политику. Любая реалистичная политика состоит из целого множества правил, которые, естественно, объединяются в группы. Очевидно, что правила для исходящей почты отличаются от правил для входящей, правила для руководства компании — от правил для рядовых сотрудников и т.д. Более того, поскольку правила применяются к письму в определенной последовательности, хотелось бы, чтобы эта последовательность была логичной и могла зависеть от результатов анализа письма. Все это вместе приводит к требованию «прозрачности»: правила, заданные в системе, должны «читаться» как правила, написанные на естественном языке, понятном человеку.

Все сказанное выше относилось к анализу письма. Однако сам по себе анализ ничего не дает. По его результатам письмо должно быть отнесено к какой-нибудь категории (безопасное, важное, неразрешенное и т.п.). Если такая категоризация проведена, то можно говорить о каких-либо действиях по отношению к проанализированному письму, например, доставить его адресату, заблокировать, и т.д. Другими словами, необходима возможность задавать системе правила, по которым она обрабатывает письма.



Условия должны накладываться на следующие **компоненты письма:**

RGFTTO; first@dDrnBn.ru
RCPTTO: e«Ofld@dO*Tieri.ru
RGPT TO: thrld@dornen.ru
Mall From: aBndeen@domn.nj **Return Pith:** avh@tej.mfl|(.gu **D*Hwry-Dit*: Wed Aug IS 17:Gft24 Reeteved: From boaiheaL**
([127,0,0.1) l>«to*tejmtkju tdtnl4ltv
Subject: Полимеры
D*to: Mon, 14 Aug 200013:39:20*0400
Mme-v*nlon:0,1
CantucHype: pilnnmd: eftartfuoia-f
Сергей Анатольевич I
ПОСылбй **Вен** краткий Списание технологии в фермате pdf

---------- B8DB7M4
Context-Transfer-Encoding: в bit
To: pvn@tej.msk.BLj
Subject- Производство полимеров
CoAtext-typ*: нш^рал/гтннФй:
From: JrHhQt*),mtk.iu
---------- ЕиП)_1ев7«6Ы
CorrtexMyp PtakVtaxl; crwr#tt"koie-r**
Петр!
Посылаю вам подробней} описание технологии
***ш* формате rtf**
---------- ЕипМ5в76564
Corrl«rtt'D«t|MBJtKin; dUaohrnanU

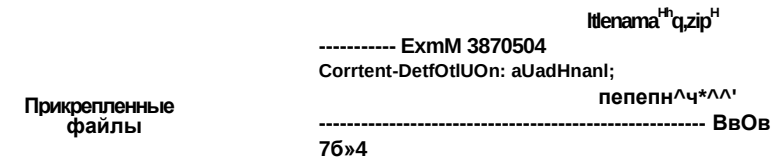


Рис. 18.16 - Фильтрация по всем компонентам письма

Любое правило можно представить себе как связку «условие + действие». Какие же действия нужны для того, чтобы обеспечить реализацию разумной политики?

Само по себе отнесение письма к определенной категории уже может рассматриваться как неявное действие. На этом действии следует остановиться подробнее. Дело в том, что жесткая категоризация как основа для принятия решений по электронному письму оказывается весьма непрактичной. Действительно, пусть мы выделили категорию писем «письмо, отправленное на запрещенный адрес» для того, чтобы блокировать доставку. С другой стороны, у нас может быть категория «письма руководства компании», которые надо отправлять безусловно. Что делать с письмом президента, отправленным по «запрещенному» адресу? Здравый смысл подсказывает, что приоритет должен быть отдан категории «письма руководства компании», что, безусловно, и будет сделано в системе с жесткой категоризацией. Однако будет потеряна существенная информация о письме. Разумный выход из таких ситуаций заключается в возможности относить письма сразу к нескольким категориям. Такая «свободная категоризация» позволит системе гибко реагировать на самые различные комбинации данных, содержащихся в письмах.

На Рис. 18.17 показана схема действий, поддерживаемых правилами фильтрации почтовых сообщений типичной системы контроля содержимого электронной почты.

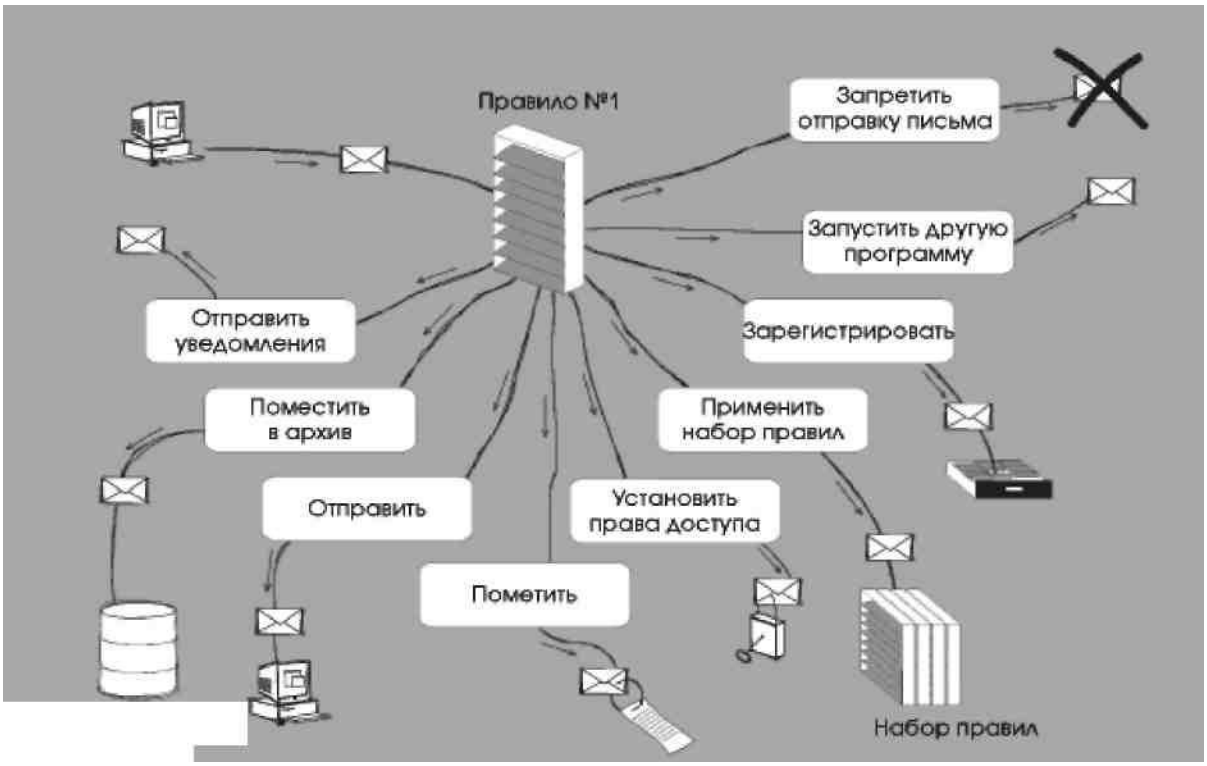


Рис. 18.17 - Схема реагирования типичной системы контроля содержимого электронной почты

18.4.6.3 Долговременное хранение и архивирование

В последнее время большое значение для обеспечения безопасности информационных систем приобрело наличие в компании архива почтовых сообщений. Некоторые разработчики систем контекстного анализа предусматривают прикрепление к своим продуктам специальных модулей архивирования. Именно наличие архива электронной почты и определяет в настоящее время полнофункциональность продуктов этой категории. При этом ведение архива — это не просто автоматическая архивация почтовых сообщений в файл, а способность регистрации сообщений и учета необходимой информации на протяжении всего жизненного цикла сообщения, возможность получения любых выборок и статистики из архива по запросам, созданным с использованием любых критериев.

Кроме того, долговременный архив предоставляет возможность ретроспективного анализа почтовых потоков и не только позволяет найти виновных в нарушении принятых в компании правил по прошествии определенного времени, но и дает материал для построения объективной и обоснованной политики использования электронной почты.

18.4.6.4 Контекстный контроль содержимого

Отличительным признаком средств контекстного анализа является способность накопления статистики и генерации отчетов. Многие продукты имеют в своем арсенале только встроенные формы отчетов, другие способны осуществлять только просмотр статистики работы конкретного пользователя системы электронной почты.

Одним из основных критериев оценки систем контекстного анализа для российского рынка является поддержка продуктом различных кодировок кириллицы (CP1251, CP866, ISO8859-5, KOI8-R, MAC), что дает возможность анализа русскоязычных текстов. Кроме того, «проклятие» множественных кодировок тяготеет над российскими информационными системами. Все осложняется тем, что разные части письма, включая почтовые заголовки, могут быть написаны в разных кодировках. Вдобавок эти кодировки не всегда указаны или не всегда указаны верно.

Рассмотрим вопрос, касающийся архитектуры систем контроля содержимого электронной почты. В подобных продуктах уникальной особенностью является открытая архитектура, которая позволяет разработчикам расширять функциональные возможности системы, интегрируя в нее дополнительные модули и не затрагивая ее ядра. Это дает возможность постоянно наращивать способности системы контроля содержимого по защите электронной почты и одновременно с этим экономить значительные средства, которые могут потребоваться на модернизацию всей системы.