Введение.

Вопрос безопасности всегда стоял перед компьютерными сетями, но сегодня как никогда растет осознание того, насколько важна безопасность компьютерных сетей в корпоративных инфраструктурах. В настоящее время для каждой корпоративной сети необходимо иметь четкую политику в области. Эта политика разрабатывается на основе анализа рисков, определения критически важных ресурсов и возможных угроз.

Базовыми элементами политики в области безопасности являются идентификация, целостность и активная проверка. Идентификация призвана предотвратить угрозу обезличивания и несанкционированного доступа к ресурсам и данным. Целостность обеспечивает защиту от подслушивания и манипулирования данными, поддерживая конфиденциальность и неизменность передаваемой информации. И наконец, активная проверка означает проверку правильности реализации элементов политики безопасности и помогает обнаруживать несанкционированное проникновение в сеть и атаки типа DoS.

В последнее время среди пользователей локальных сетей и частных граждан растет беспокойство по поводу гарантии безопасности информации, хранящейся в компьютерах. Озабоченность вполне оправдана, так как объем конфиденциальных сведений о компаниях и частных лицах, которую собирают и хранят в локальных сетях государственные учреждения, госпитали и финансовые организации, постоянно растет. Поэтому особую актуальность приобретает задача выработки правил, которые регламентировали бы передачу и обмен частной и корпоративной информации конфиденциального характера.

Революция в области вычислительной техники открыла перед множеством организаций возможность приобретать устройства для хранения больших массивов информации, затрачивая на такое оборудование значительно меньше средств, чем раньше. Эта сыграло решающую роль в увеличении объемов сохраняемых данных, имеющих коммерческий, частный или конфиденциальный характер. В результате, возросла и необходимость обеспечения безопасности данных.

Сетевые технологии облегчают доступ к информации, а значит, делают ее более открытой. Пожалуй, одним из наиболее фундаментальных достижений, которые обеспечили массовый доступ пользователей к локальным сетям, стало распространение открытых структурированных кабельных систем (СКС). Это, в свою очередь, привело к тому, что простота доступа к данным и широкое распространение настольных компьютеров и систем хранения информации снизили уровень безопасности и конфиденциальности данных.

Цели и методы безопасности.

Крайне важно понять, что безопасность - это не продукт, который можно купить в магазине и быть уверенным в собственной защищенности. "Безопасность" - особая комбинация как технических, так и административных мер. Административные меры также включают в себя не только бумаги, рекомендации, инструкции, но и людей. Невозможно считать свою сеть "безопасной", если вы не доверяете людям, работающим с этой сетью.

Идеальная безопасность - недостижимый миф, который могут реализовать, в лучшем случае, только несколько профессионалов. Есть один фактор, который невозможно преодолеть на пути к идеальной безопасности - это человек.

ОСНОВНЫЕ ЦЕЛИ СЕТЕВОЙ БЕЗОПАСНОСТИ

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основных целей обычно три:

- *Целостность данных.*
- *Конфиденциальность данных.*
- *Доступность данных.*

Рассмотрим более подробно каждую из них.

Схема 1. Основные цели сетевой безопасности

Целостность данных .

Одна из основных целей сетевой безопасности - гарантированность того, чтобы данные не были изменены, подменены или уничтожены. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных .

Второй главной целью сетевой безопасности является обеспечение конфиденциальности данных. Не все данные можно относить к конфиденциальной информации. Существует достаточно большое количество информации, которая должна быть доступна всем. Но даже в этом случае обеспечение целостности данных, особенно открытых, является основной задачей. К конфиденциальной информации можно отнести следующие данные:

- *Личная информация пользователей.*
- *Учетные записи (имена и пароли).*
- *Данные о кредитных картах.*
- *Данные о разработках и различные внутренние документы.*

- *Бухгалтерская информация.*

Доступность данных.

Третьей целью безопасности данных является их доступность. Бесполезно говорить о безопасности данных, если пользователь не может работать с ними из-за их недоступности. Вот приблизительный список ресурсов, которые обычно должны быть "доступны" в локальной сети:

- *Принтеры.*
- *Серверы.*
- *Рабочие станции.*
- *Данные пользователей.*
- *Любые критические данные, необходимые для работы.*

Рассмотрим угрозы и препятствия, стоящие на пути к безопасности сети. Все их можно разделить на две большие группы: технические угрозы и человеческий фактор.

Технические угрозы:

- *Ошибки в программном обеспечении.*
- *Различные DoS- и DDoS-атаки.*
- *Компьютерные вирусы, черви, троянские кони.*
- *Анализаторы протоколов и прослушивающие программы ("снифферы").*
- *Технические средства съема информации.*

Ошибки в программном обеспечении .

Самое узкое место любой сети. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, следовательно, оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляет никакой опасности, некоторые же могут привести к трагическим последствиям, таким, как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (хранение ненужных данных на сервере, использование в качестве плацдарма для атаки и т.п.). Большинство таких уязвимостей устраняется с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких обновлений является необходимым условием безопасности сети.

DoS- и DDoS-атаки .

Denial Of Service (отказ в обслуживании) - особый тип атак, направленный на выведение сети или сервера из работоспособного состояния. При DoS-атаках могут использоваться ошибки в программном обеспечении или легитимные операции, но в больших масштабах (например, посылка огромного количества электронной почты). Новый тип атак DDoS (Distributed Denial Of Service) отличается от предыдущего наличием огромного количества компьютеров, расположенных в большой географической зоне. Такие атаки просто перегружают канал трафиком и мешают прохождению, а зачастую и полностью блокируют передачу по нему полезной информации. Особенно актуально это для компаний, занимающихся каким-либо online-бизнесом, например, торговлей через Internet.

Компьютерные вирусы, троянские кони .

Вирусы - старая категория опасностей, которая в последнее время в чистом виде практически не встречается. В связи с активным применением сетевых технологий для передачи данных вирусы все более тесно интегрируются с троянскими компонентами и сетевыми червями. В настоящее время компьютерный вирус использует для своего распространения либо электронную почту, либо уязвимости в ПО. А часто и то, и другое. Теперь на первое место вместо деструктивных функций вышли функции удаленного управления, похищения информации и использования зараженной системы в качестве плацдарма для дальнейшего распространения. Все чаще зараженная машина становится активным участником DDoS-атак. Методов борьбы достаточно много, одним из них является все та же своевременная установка обновлений.

Анализаторы протоколов и "снифферы" .

В эту группу входят средства перехвата передаваемых по сети данных. Такие средства могут быть как аппаратными, так и программными. Обычно данные передаются по сети в открытом виде, что позволяет злоумышленнику внутри локальной сети перехватить их. Некоторые протоколы работы с сетью (POPS, FTP) не используют шифрование паролей, что позволяет злоумышленнику перехватить их и использовать самому. При передаче данных по глобальным сетям эта проблема встает наиболее остро. По возможности следует ограничить доступ к сети неавторизированным пользователям и случайным людям.

Технические средства съема информации.

Сюда можно отнести такие средства, как клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т.д. Данная группа используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия спецтехники, требует доступа к сети и ее составляющим.

Человеческий фактор:

- *Уволенные или недовольные сотрудники.*
- *Промышленный шпионаж.*
- *Халатность.*
- *Низкая квалификация.*

Уволенные и недовольные сотрудники .

Данная группа людей наиболее опасна, так как многие из работающих сотрудников могут иметь разрешенный доступ к конфиденциальной информации. Особенную группу составляют системные администраторы, зачастую недовольные своим материальным положением или несогласные с увольнением, они оставляют "черные ходы" для последующей возможности злонамеренного использования ресурсов, похищения конфиденциальной информации и т. д.

Промышленный шпионаж .

Это самая сложная категория. Если ваши данные интересны кому-либо, то этот кто-то найдет способы достать их. Взлом хорошо защищенной сети - не самый простой вариант. Очень может статься, что уборщица "тетя Глаша", моющая под столом и ругающаяся на непонятный ящик с проводами, может оказаться хакером весьма высокого класса.

Халатность .

Самая обширная категория злоупотреблений: начиная с не установленных вовремя обновлений, неизмененных настроек "по умолчанию" и заканчивая несанкционированными модемами для выхода в Internet, - в результате чего злоумышленники получают открытый доступ в хорошо защищенную сеть.

Низкая квалификация

Часто низкая квалификация не позволяет пользователю понять, с чем он имеет дело; из-за этого даже хорошие программы защиты становятся настоящей морокой системного администратора, и он вынужден надеяться только на защиту периметра. Большинство пользователей не понимают реальной угрозы от запуска исполняемых файлов и скриптов и считают, что исполняемые файлы -только файлы с расширением "exe". Низкая квалификация не позволяет также определить, какая информация является действительно конфиденциальной, а какую можно разглашать. В крупных компаниях часто можно позвонить пользователю и, представившись администратором, узнать у него учетные данные для входа в сеть. Выход только один -обучение пользователей, создание соответствующих документов и повышение квалификации.

МЕТОДЫ ЗАЩИТЫ

Согласно статистике потерь, которые несут организации от различных компьютерных преступлений, львиную долю занимают потери от преступлений, совершаемых собственными нечистоплотными сотрудниками. Однако в последнее время наблюдается явная тенденция к увеличению потерь от внешних злоумышленников. В любом случае необходимо обеспечить защиту как от нелояльного персонала, так и от способных проникнуть в вашу сеть хакеров. Только комплексный подход к защите информации может внушить уверенность в ее безопасности.

Однако в связи с ограниченным объемом данной статьи рассмотрим только основные из технических методов защиты сетей и циркулирующей по ним информации, а именно - криптографические алгоритмы и их применение в данной сфере.

Защита данных от внутренних угроз.

Для защиты циркулирующей в локальной сети информации можно применить следующие криптографические методы:

- *шифрование информации;*
- *электронную цифровую подпись (ЭЦП).*

Шифрование

Шифрование информации помогает защитить ее конфиденциальность, т.е. обеспечивает невозможность несанкционированного ознакомления с ней. Шифрование - это процесс преобразования открытой информации в закрытую, зашифрованную (что называется "зашифрование") и наоборот ("расшифрование"). Это преобразование выполняется по строгим математическим алгоритмам; помимо собственно данных в преобразовании также участвует дополнительный элемент - "ключ". В ГОСТ 28147-89 дается следующее определение ключа: "Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований". Иными словами, ключ представляет собой уникальный

элемент, позволяющий зашифровать информацию так, что получить открытую информацию из зашифрованной можно только определенному пользователю или группе пользователей.

Шифрование можно выразить следующими формулами:

C=Ek$_1$ (M) - *зашифрование,*
M"=Dk$_2$(C) - *расшифрование.*

Функция E выполняет зашифрование информации, функция D – расшифрование. В том случае, если ключ **k$_2$** *соответствует ключу* **k$_1$**, *примененному при зашифровании, удается получить открытую информацию, т.е. получить соответствие* **M"** = **M**.

При отсутствии же правильного ключа **k$_2$** *получить исходное сообщение практически невозможно.*

По виду соответствия ключей **k$_1$** *и* **k$_2$** *алгоритмы шифрования разделяются на две категории:*

1) Симметричное шифрование: **k$_1$** = **k$_2$**. *Для зашифрования и расшифрования информации используется один и тот же ключ. Это означает, что пользователи, обменивающиеся зашифрованной информацией, должны иметь один и тот же ключ. Более безопасный вариант - существует уникальный ключ шифрования для каждой пары пользователей, который неизвестен остальным. Ключ симметричного шифрования должен храниться в секрете: его компрометация (утеря или хищение) повлечет за собой раскрытие всей зашифрованной данным ключом информации.*

2) Асимметричное шифрование. Ключ **k$_1$**- *в данном случае называется "открытым", а ключ* **k$_2$** - *"секретным". Открытый ключ вычисляется из секретного различными способами (зависит от конкретного алгоритма шифрования). Обратное же вычисление* **k$_2$** *из* **k$_1$** *является практически невозможным. Смысл асимметричного шифрования состоит в том, что ключ* **k$_2$** *хранится в секрете у его владельца и не должен быть известен никому; ключ k1, наоборот, распространяется всем пользователям, желающим отправлять зашифрованные сообщения владельцу ключа* **k$_2$**; *любой из них может зашифровать информацию на ключе* **k$_1$**, *расшифровать же ее может только обладатель секретного ключа* **k$_2$**.

Оба ключа: ключ симметричного и секретный ключ асимметричного шифрования должны быть абсолютно случайными - в противном случае злоумышленник теоретически имеет возможность спрогнозировать значение определенного ключа. Поэтому для генерации ключей обычно используют датчики случайных чисел (ДСЧ), лучше всего - аппаратные.

Стоит сказать, что все государственные организации РФ и ряд коммерческих обязаны для защиты данных использовать отечественный алгоритм симметричного шифрования ГОСТ 28147-89. Это сильный криптографический алгоритм, в котором пока еще не найдено недостатков за более чем 12 лет применения.

ЭЦП
ЭЦП позволяет гарантировать целостность и авторство информации (схема 2). Как видно из схемы, ЭЦП также использует криптографические ключи: секретный и открытый. Открытый ключ вычисляется из секретного по достаточно легкой формуле, например: $y=a^x \bmod p$ (где x - секретный ключ, y - открытый ключ, a и p- параметры алгоритма ЭЦП), обратное же вычисление весьма трудоемко и считается неосуществимым за приемлемое время при современных вычислительных мощностях.

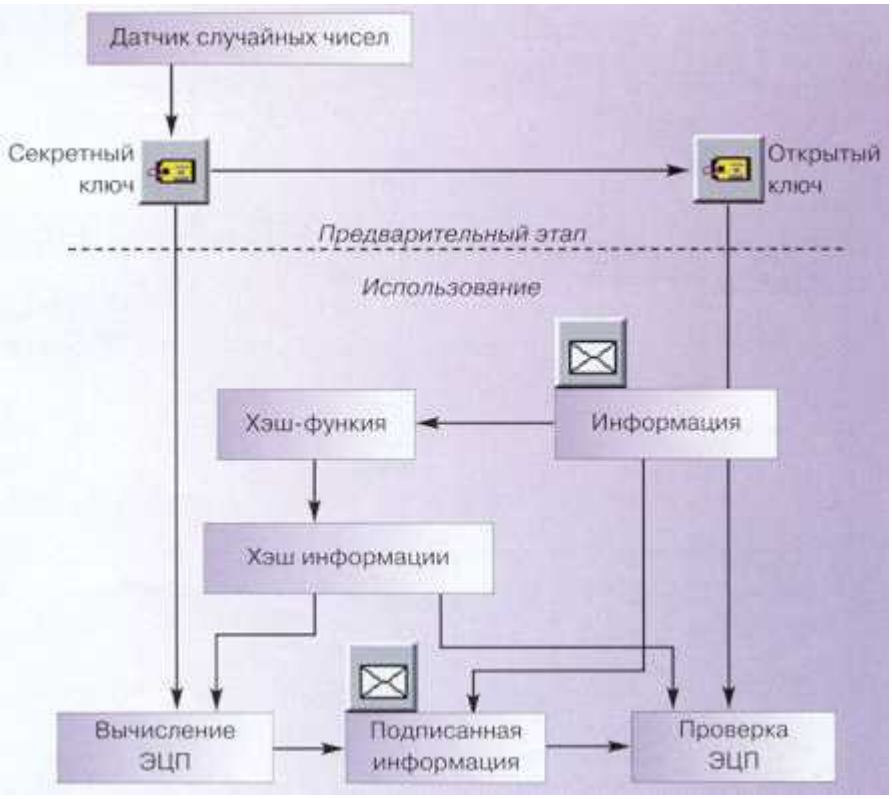

Схема 2. Схема применения ЭЦП

Схема распространения ключей ЭЦП аналогична схеме асимметричного шифрования: секретный ключ должен оставаться у его владельца, открытый же распространяется всем пользователям, желающим проверять ЭЦП владельца секретного ключа. Необходимо обеспечивать недоступность своего секретного ключа, ибо злоумышленник легко может подделать ЭЦП любого пользователя, получив доступ к его секретному ключу.

Электронной подписью можно подписать любую информацию. Предварительно информацию обрабатывают функцией хэширования, цель которой - выработка последовательности определенной длины, однозначно отражающей содержимое подписываемой информации. Данная последовательность называется "хэш", основное свойство хэша таково, что исключительно сложно модифицировать информацию так, чтобы ее хэш остался неизменным. Отечественный стандарт хэш-функций ГОСТ Р 34.11-94 предусматривает хэш размером 256 бит.

На основе хэша информации и секретного ключа пользователя вычисляется ЭЦП. Как правило, ЭЦП отправляется вместе с подписанной информацией (ЭЦП файла чаще всего просто помещают в конец файла перед его отправкой куда-либо по сети). Сама ЭЦП, как и хэш, является бинарной последовательностью фиксированного размера. Однако, помимо ЭЦП, к информации обычно добавляется также ряд служебных полей, прежде всего, идентификационная информация о пользователе, поставившем ЭЦП; причем, данные поля участвуют в расчете хэша. При проверке ЭЦП файла в интерактивном режиме результат может выглядеть так:

"Подпись файла "Document.doc" верна: Иванов А.А. 25.02.2003".

Естественно, в случае неверной ЭЦП выводится соответствующая информация, содержащая причину признания ЭЦП неверной. При проверке ЭЦП также вычисляется хэш информации; если он не совпадает с полученным при вычислении ЭЦП (что может означать попытку модификации информации злоумышленником), ЭЦП будет неверна.

Наряду с ГОСТ 28147-89 существует отечественный алгоритм ЭЦП: ГОСТ Р 34.10-94 и его более новый вариант ГОСТ Р 34.10-2001. Государственные организации РФ и ряд коммерческих обязаны использовать один из этих алгоритмов ЭЦП в паре с алгоритмом хэширования ГОСТ Р 34.11 -94.

Существует и более простой способ обеспечения целостности информации - вычисление имитоприставки. Имитоприставка - это криптографическая контрольная сумма информации, вычисляемая с использованием ключа шифрования. Для вычисления имитоприставки используется, в частности, один из режимов работы алгоритма ГОСТ 28147-89, позволяющий получить в качестве имитоприставки 32-битную последовательность из информации любого размера. Аналогично хэшу информации имитоприставку чрезвычайно сложно подделать. Использование имитоприставок более удобно, чем применение ЭЦП: во-первых, 4 байта информации намного проще добавить, например, к пересылаемому по сети IP-пакету, чем большую структуру ЭЦП, во-вторых, вычисление имитоприставки существенно менее ресурсоемкая операция, чем формирование ЭЦП, поскольку в последнем случае используются такие сложные операции, как возведение 512-битного числа в степень, показателем которой является 256-битное число, что требует достаточно много вычислений. Имитоприставку нельзя использовать для контроля авторства сообщения, но этого во многих случаях и не требуется.

Комплексное применение криптографических алгоритмов.

Для безопасной передачи по сети каких-либо файлов, их достаточно подписать и зашифровать. На схеме 3 представлена технология специализированного архивирования, обеспечивающая комплексную защиту файлов перед отправкой по сети.

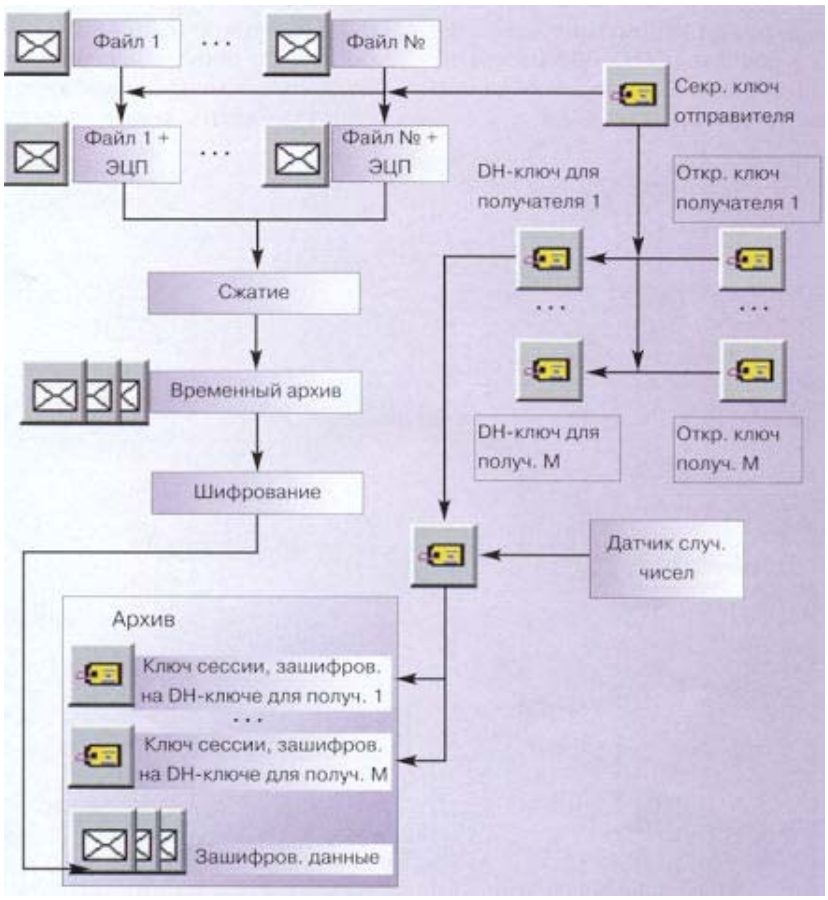

Схема 3. Технология специализированного архивирования

Прежде всего, файлы подписываются секретным ключом отправителя, затем сжимаются для более быстрой передачи. Подписанные и сжатые файлы шифруются на случайном ключе сессии, который нужен только для зашифрования этой порции файлов -ключ берется с датчика случайных чисел, который обязан присутствовать в любом шифраторе. После этого к сформированному таким образом спецархиву добавляется заголовок, содержащий служебную информацию.

Заголовок позволяет расшифровать данные при получении. Для этого он содержит ключ сессии в зашифрованном виде. После зашифрования данных и записи их в архив, ключ сессии, в свою очередь, зашифровывается на ключе парной связи (DH-ключ), который вычисляется динамически из секретного ключа отправителя файлов и открытого ключа получателя по алгоритму Диффи-Хеллмана. Ключи парной связи различны для каждой пары "отправитель-получатель". Тот же самый ключ парной связи может быть вычислен только тем получателем, открытый ключ которого участвовал в вычислении ключа парной связи на стороне отправителя. Получатель для вычисления ключа парной связи использует свой секретный ключ и открытый ключ отправителя. Алгоритм Диффи-Хеллмана позволяет при этом получить тот же ключ, который сформировал отправитель из своего секретного ключа и открытого ключа получателя.

Таким образом, заголовок содержит копии ключа сессии (по количеству получателей), каждая их которых зашифрована на ключе парной связи отправителя для определенного получателя.

После получения архива получатель вычисляет ключ парной связи, затем расшифровывает ключ сессии, и наконец, расшифровывает собственно архив. После расшифрования информация автоматически разжимается. В последнюю очередь проверяется ЭЦП каждого файла.

Защита от внешних угроз.

Методов защиты от внешних угроз придумано немало - найдено противодействие практически против всех опасностей, перечисленных в первой части данной статьи. Единственная проблема, которой пока не найдено адекватного решения, - DDoS-атаки. Рассмотрим технологию виртуальных частных сетей (VPN - Virtual Private Network), позволяющую с помощью криптографических методов как защитить информацию, передаваемую через Internet, так и пресечь несанкционированный доступ в локальную сеть снаружи.

Виртуальные частные сети.

На наш взгляд, технология VPN является весьма эффективной защитой, ее повсеместное внедрение - только вопрос времени. Доказательством этого является хотя бы внедрение поддержки VPN в последние операционные системы фирмы Microsoft - начиная с Windows 2000.

Суть VPN состоит в следующем (см. схему 4):

1. *На все компьютеры, имеющие выход в Internet (вместо Internet может быть и любая другая сеть общего пользования), ставится средство, реализующее VPN. Такое средство обычно называют VPN-агентом. VPN-агенты обязательно должны быть установлены на все выходы в глобальную сеть.*
2. *VPN-агенты автоматически зашифровывают всю информацию, передаваемую через них в Internet, а также контролируют целостность информации с помощью имитоприставок.*

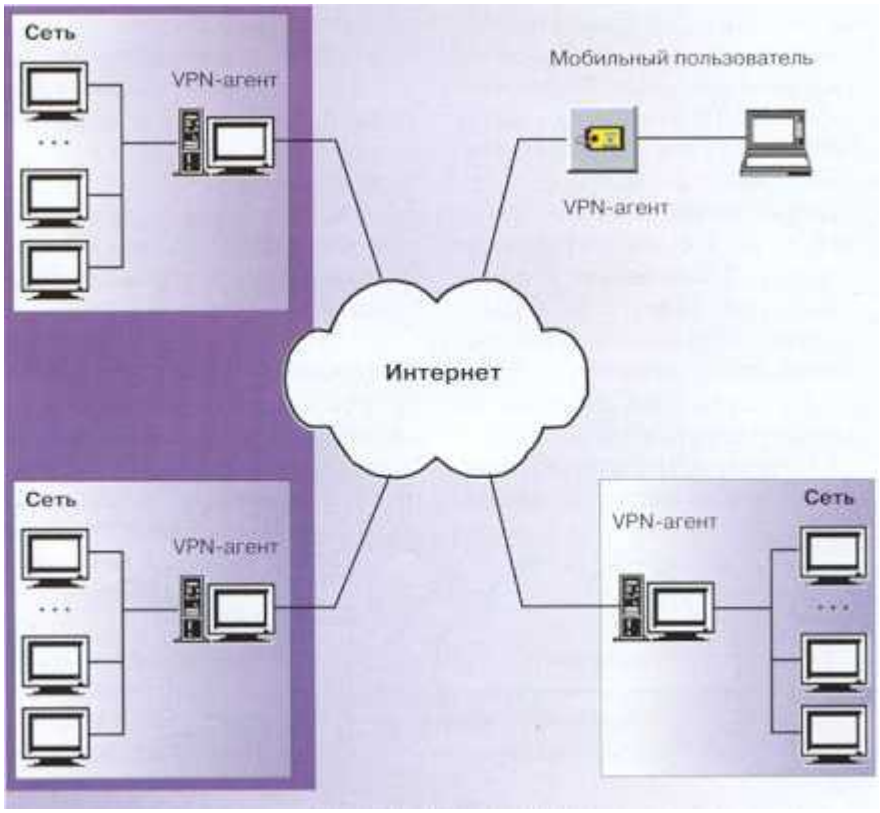

Схема 4. Технология VPN

Как известно, передаваемая в Internet информация представляет собой множество пакетов протокола IP, на которые она разбивается перед отправкой и может многократно переразбиваться по дороге. VPN-агенты обрабатывают именно IP-пакеты, ниже описана технология их работы.

1. Перед отправкой IP-пакета VPN-агент выполняет следующее:

- *Анализируется IP-адрес получателя пакета. В зависимости от адреса и другой информации (см. ниже) выбираются алгоритмы защиты данного пакета (VPN-агенты могут, поддерживать одновременно несколько алгоритмов шифрования и контроля целостности) и криптографические ключи. Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится.*
- *Вычисляется и добавляется в пакет его имитоприставка.*
- *Пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию).*
- *Формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента. Это называется инкапсуляцией пакета. При использовании инкапсуляции обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.*

2. При получении IP-пакета выполняются обратные действия:

- *Из заголовка пакета получается информация о VPN-агенте отправителя пакета. Если такой отправитель не входит в число разрешенных в настройках, то пакет*

отбрасывается. То же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком.

- *Согласно настройкам выбираются криптографические алгоритмы и ключи.*
- *Пакет расшифровывается, затем проверяется его целостность. Пакеты с нарушенной целостностью также отбрасываются.*
- *В завершение обработки пакет в его исходном виде отправляется настоящему адресату по локальной сети.*

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера - на котором установлен.

VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (к таким каналам обычно применяется термин "туннель", а технология их создания называется "туннелировани-ем"). Вся информация идет по туннелю только в зашифрованном виде. Кстати, пользователи VPN при обращении к компьютерам из удаленных локальных сетей могут и не знать, что эти компьютеры реально находятся, может быть, в другом городе, - разница между удаленными и локальными компьютерами в данном случае состоит только в скорости передачи данных.

Как видно из описания действий VPN-агентов, часть IP-пакетов ими отбрасывается. Действительно, VPN-агенты фильтруют пакеты согласно своим настройкам (совокупность настроек VPN-агента называется "Политикой безопасности"). То есть VPN-агент выполняет два основных действия: создание туннелей и фильтрация пакетов (см.схему 5).

Схема 5. Туннелирование и фильтрация

IP-пакет отбрасывается или направляется в конкретный туннель в зависимости от значений следующих его характеристик:

- *IP-адрес источника (для исходящего пакета - адрес конкретного компьютера защищаемой сети).*
- *IP-адрес назначения.*
- *Протокол более верхнего уровня, которому принадлежит данный пакет (например, TCP или UDP для транспортного уровня).*
- *Номер порта, с которого или на который отправлен пакет (например, 1080).*

Более подробно технология VPN описана в специальной литературе.

Криптография.

Уже мало кто сомневается в том факте, что незадолго до начала XXI века человечество вступило в новую технологическую эпоху — эру информационных технологий. IT-индустрия, занимающаяся вопросами производства, обработки, хранения и передачи информации, стала неотъемлемой частью мировой хозяйственной системы, вполне самостоятельным и довольно значительным сектором экономики. Зависимость современного общества от информационных технологий настолько высока, что сбои в информационных системах способны привести к значительным инцидентам в «реальном» мире.

Телекоммуникации — ключевая отрасль для информационных технологий, ведающая вопросами транспортировки информации. Однако именно при транспортировке информация более всего уязвима к различного рода злоупотреблениям. Действительно, узлы хранения и обработки данных ввиду их компактности можно физически защитить от доступа злоумышленников, чего не скажешь о линиях связи протяженностью многие сотни или тысячи километров -защитить их практически невозможно. Поэтому именно в телекоммуникационной сфере весьма актуальна проблема защиты информации.

Эта проблема была осознана еще в древние времена, когда в качестве канала связи выступал курьер, везущий письменное сообщение. Исторически первой задачей защиты информации стало обеспечение секретности данных в каналах связи, то есть защита этих данных от ознакомления с ними лиц, для которых они не предназначены. Тогда же были разработаны и средства защиты информации, среди которых важнейшую роль играет криптография.

Привлекательность криптографических методов состоит в том, что в отличие от других подходов они основаны на преобразовании самой информации и никак не связаны с характеристиками ее материальных носителей, вследствие чего наиболее универсальны и потенциально дешевы в реализации.

И хотя сейчас криптография используется для решения большого числа разных проблем, например для подписи цифровых данных или вручения сообщения «под расписку», обеспечение секретности до сих пор считается главной задачей криптографии и решается шифрованием передаваемых данных, то есть преобразованием к виду, в котором данные не могут быть адекватно прочитаны и интерпретированы посторонними. Получатель сможет восстановить данные в исходном виде, только владея секретом такого преобразования, недоступным всем остальным. Согласно принципу Керкхоффа, в соответствии с которым строятся все современные криптосистемы, секретной частью шифра является его ключ — отрезок данных определенной длины. Этот же самый ключ требуется и отправителю для шифрования сообщения. В данном случае речь идет о симметричных или одноключевых шифрах.

Проблема распределения ключей в криптографии

Указанный подход порождает своего рода замкнутый круг: чтобы разделить секрет (передаваемое сообщение) отправитель и получатель уже должны обладать общим секретом (ключом шифрования). Раньше данная проблема решалась некриптографическим методом — передачей ключа по физически защищенным от прослушивания каналам связи (Схема 6). Однако создание подобного канала и поддержание его в оперативной готовности на случай экстренной необходимости передачи ключа является довольно трудоемким и затратным делом. Поэтому в

условиях постоянно возрастающей интенсивности информационных потоков такой способ распределения ключей становился все менее приемлемым и удовлетворительным.

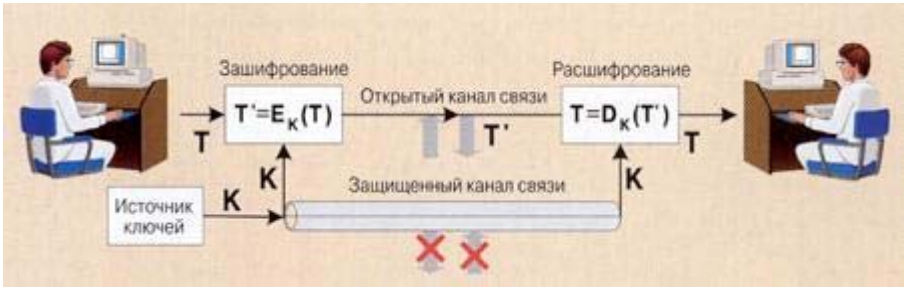

Схема 6. Схема защиты информации с помощью симметричного шифрования и физически защищенного канала связи для распределения ключей

Проблема была успешно разрешена в рамках возникшей чуть более четверти века назад современной криптографии», называемой так в противовес уже известной к тому моменту «традиционной криптографии» [1]. Решение заключается в использовании асимметричных (двухключевых) шифров или схем распределения ключа по открытым каналам связи.

В первом случае процедуры за- и расшифрования выполняются на разных ключах, поэтому нет надобности держать ключ зашифрования в секрете. Однако из-за крайне низких характеристик эффективности и подверженности некоторым специальным видам атак такие шифры оказались малопригодны для закрытия непосредственно пользовательской информации. Вместо этого асимметричные шифры используются в составе комбинированных схем, когда массив данных шифруется симметричным шифром на разовом ключе, который в свою очередь шифруется двухключевым шифром и в таком виде передается вместе с данными.

Схемы распределения ключей по открытым каналам связи решают ту же проблему несколько иным способом: в ходе сеанса взаимодействия два корреспондента вырабатывают общий секретный ключ, который затем используется для зашифрования передаваемых данных симметричным шифром. Причем перехват информации в канале во время сеанса выработки такого ключа не дает противнику возможности получить сам ключ: K=K(X,Y) невычислимо (Схема 7).

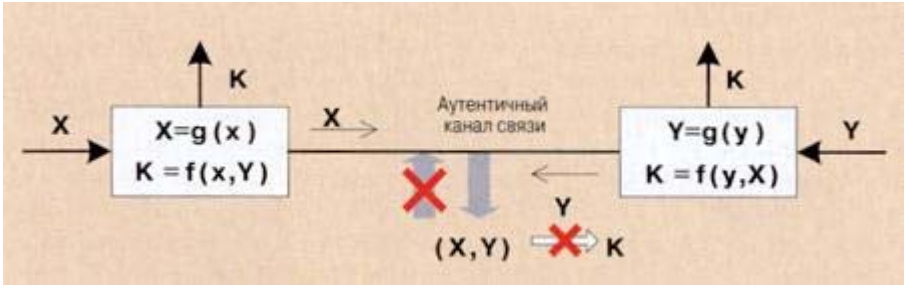

Схема 7. Распределение ключей по открытым каналам связи с использованием асимметричной криптографии

Проблемы асимметричной криптографии

На сегодняшний день асимметричная криптография вполне успешно решает задачу распределения ключей по открытым каналам связи. Тем не менее существует несколько проблем, вызывающих определенное опасение за ее будущее. Стойкость всех схем асимметричной криптографии основана на невозможности эффективного вычислительного решения ряда таких математических задач (так называемых NP-проблем), как факторизация (разложение на множители) больших чисел и логарифмирование в дискретных полях большого размера. Но указанная невозможность является всего лишь предположением, которое в любой момент может быть опровергнуто, если будет доказана противоположная ему гипотеза, а именно NP=P. Это привело бы к краху всей современной криптографии, так как задачи, на нерешаемости которых она базируется, достаточно тесно связаны, и взлом даже одной криптосистемы будет означать взлом большинства других. В этом направлении ведутся интенсивные исследования, однако проблема до сих пор остается открытой.

Другая угроза современным криптосистемам исходит от так называемых квантовых компьютеров — устройств обработки информации, построенных на принципах квантовой механики, идея которых впервые была предложена известным американским физиком Р. Фейнманом. В 1994 г. П. Шор предложил алгоритм факторизации для квантового компьютера, который позволяет разложить число на множители за время, зависящее полиномиальным образом от размера числа [2]. А в 2001 г. этот алгоритм был успешно реализован на созданном специалистами фирмы IBM и Стэнфордского университета первом действующем макете квантового вычислителя [3].

По оценкам специалистов, квантовый компьютер, способный взломать криптосистему RSA, может быть создан примерно через 15-25 лет.

Еще одним неприятным фактом в асимметричных криптосистемах является то, что минимальный «безопасный размер» ключей постоянно растет вследствие прогресса в соответствующей области. За всего четвертьвековую историю таких систем он вырос уже примерно в 10 раз, тогда как за этот же период для традиционных симметричных шифров размер ключа изменился менее чем вдвое.

Все вышеперечисленное делает долгосрочные перспективы систем асимметричной криптографии не вполне надежными и вынуждает искать альтернативные способы решения тех же самых задач. Некоторые из них могут быть решены в рамках так называемой квантовой криптографии, или квантовой коммуникации.

Основы квантовой криптографии

Квантовая криптография — это сравнительно новое направление исследований, позволяющее применять эффекты квантовой физики для создания секретных каналов передачи данных [4]. С чисто формальной точки зрения данное направление нельзя назвать разделом криптографии, скорее, оно должно быть отнесено к техническим методам защиты информации, так как в квантовой криптографии в основном используются свойства материальных носителей информации. Указанный факт находит свое подтверждение еще и в том, что основной прогресс в данной области достигается инженерами-физиками, а не математиками и криптографами. Тем не менее термин «квантовая криптография» вполне устоялся и используется наряду с более корректным аналогом — «квантовая коммуникация».

В квантовой криптографии используется фундаментальная особенность квантовых систем, заключающаяся в принципиальной невозможности точного детектирования состояния такой системы, принимающей одно из набора нескольких неортогональных состояний. Это вытекает из факта, что достоверно различить подобные состояния за одно измерение не получается. Например, нельзя определить длину отрезка в пространстве только по его проекции на одну ось, а более одного измерения сделать невозможно, потому что после первого же измерения система непредсказуемым образом изменяет свое состояние. Кроме того, в квантовой механике справедлива теорема о запрете точного клонирования систем, что делает невозможным изготовление нескольких копий исследуемой системы и последующее их тестирование.

Для начала рассмотрим работу идеального квантового канала [5], принцип действия которого предполагает, что приемно-передающая аппаратура и каналы связи идеальны. В качестве носителей информации в квантовой криптографии, как правило, используются отдельные фотоны, или связанные фотонные пары. Значения 0 и 1 битов информации кодируются различными направлениями поляризации фотонов. Для передачи сигнала отправитель случайным образом выбирает один из двух или в некоторых схемах из трех взаимно неортогональных базисов. При этом однозначно правильное детектирование сигнала возможно, если только получатель правильно угадал базис, в котором отправитель подготовил сигнал. В случае, если базис угадан неверно, исход измерения не определен. На рис. 3 показано, что получатель пытается детектировать сигнал 1_0 (квант, поляризованный вдоль оси Y_0) в неверном базисе 1 (оси X_1, Y_1, повернуты на 45°), в итоге он может получить с равной вероятностью как 0, так и 1, то есть результат измерения полностью недостоверен.

Схема 8. Использование квантовых эффектов для секретной передачи данных

Поскольку отправитель выбирает базис случайным образом, получатель неизбежно будет ошибаться в выборе базиса детектирования, и часть измерений окажется неверной. Затем получатель и отправитель проводят обсуждение исходов передачи по аутентичному, но, возможно, несекретному каналу связи. Что именно при этом передается зависит от использованного квантового протокола, но в любом случае указанная информация позволяет корреспондентам исключить случаи, когда получатель неверно угадал базис, и не дает противнику никаких сведений относительно правильно переданных данных.

Если противник попытается подслушать информацию, передаваемую через квантовый канал, то он, так же как и получатель, будет неизбежно ошибаться в выборе базиса. Поскольку квант, несущий информацию, при детектировании разрушается, противник испускает новый квант, поляризованный тем или иным образом в использованном им базисе. В определенных случаях этот базис не будет совпадать с тем, который использовался отправителем, что приведет к искажению данных. Наличие искажений будет обнаружено в ходе сверки корреспондентами выработанного общего отрезка данных, и это будет означать попытку прослушивания.

Таким образом, системы квантовой криптографии обладают рядом принципиальных особенностей. Во-первых, нельзя заранее сказать, какой из передаваемых битов будет корректно принят получателем, так как этот процесс носит вероятностный характер. Во-вторых, существенной особенностью системы является использование низкоэнергетических импульсов, в идеале состоящих из одного фотона, что сильно снижает скорость передачи по тому же каналу в сравнении с обычным уровнем оптических сигналов. В силу указанных причин квантовый канал связи малопригоден для передачи пользовательских данных, а больше подходит для выработки ключа симметричного шифра, который будет использован корреспондентами для зашифрования передаваемых данных. В этом отношении он подобен асимметричному шифрованию или схемам открытого распределения ключей.

Проблемы реальных систем квантовой криптографии

В идеальных системах квантовой коммуникации перехват данных невозможен, так как он моментально обнаруживается участниками обмена по возникающим ошибкам в передаче. Однако реальные системы отличаются от идеальных.

Во-первых, аппаратура участников информационного обмена несовершенна, что приводит к появлению ошибок приема-передачи. В этих обстоятельствах наличие определенного уровня ошибок не должно восприниматься системой как попытка подслушивания. А наличие собственного фона ошибок позволяет противнику осуществлять перехват, маскируя неизбежно возникающие при этом искажения под собственные ошибки системы.

Во-вторых, в реальных линиях передачи существует затухание сигнала, что вынуждает отправителя увеличивать мощность импульса, т.е. число фотонов в нем, либо приводит к потере части импульсов в канале. В первом случае, если импульс содержит много фотонов, поляризованных одинаковым образом, с помощью светоделителя от него можно сделать отвод и тестировать уже его, не трогая основной сигнал. Понятно, что такой перехват следует осуществлять как можно ближе к отправителю — там уровень сигнала выше (рис. 4). Во втором случае затухание сигнала приводит к увеличению общего уровня ошибок, и у противника увеличиваются шансы замаскировать перехват под собственные ошибки системы.

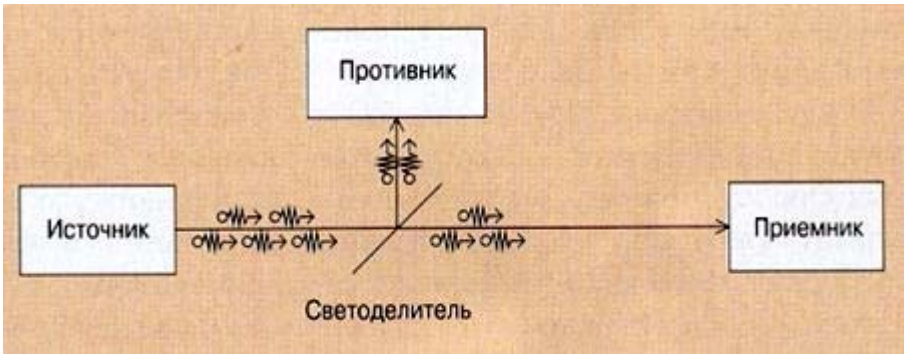

Схема 9. Использование многофотонных импульсов для передачи сигнала делает возможным перехват данных путем «отвода» части фотонов

В-третьих, у противника есть лучшая стратегия перехвата, чем простое угадывание базиса. Дело в том, что законы квантовой механики запрещают лишь идеальное клонирование квантовой системы, неидеальное клонирование при этом остается возможным. В настоящее время доказана теоретическая возможность успешного однократного копирования состояния квантовой системы с вероятностью успеха 5/6, а с ростом числа копий эта вероятность снижается до 2/3. Эксперименты по клонированию фотонов показывают результат, близкий к предсказанному теорией. Это дает противнику возможность копировать фотон и затем анализировать его поляризацию в двух различных базисах. Конечно, при этом будут возникать ошибки, но их уровень будет ниже, чем при простом угадывании базиса. И если базис окажется сопоставим с собственным фоном ошибок системы, прослушивание становится возможным. Поэтому в распоряжении противника всегда есть возможность перехватить какую-то часть передаваемых битов, замаскировав неизбежно сопровождающие такой перехват ошибки под собственные ошибки системы.

Для отсеивания собственных ошибок в реальных системах квантовой криптографии необходимо применять различные протоколы коррекции, а для снижения значимости перехваченных противником битов нужно использовать процедуру усиления секретности. Для этого проще всего вырабатывать несколько «слепков» ключа, а итоговый рабочий ключ получать простым побитовым суммированием по модулю 2 этих «слепков». Тогда, чтобы наверняка определить хотя бы один бит ключа, злоумышленнику нужно знать соответствующие биты во всех «слепках». Другой возможный способ заключается в том, чтобы вырабатывать ключи из сформированного битового вектора с помощью хэш-функций.

Таким образом, в отличие от идеальных реальные системы квантовой коммуникации не способны обеспечить абсолютную секретность передаваемых данных. Это обусловлено наличием у них фона собственных ошибок, под которые можно замаскировать попытки перехвата, а также затуханием в каналах связи из-за необходимости использования многофотонных импульсов. Последнее делает возможным неразрушающий перехват данных и является практически неустранимым фактором, так как качество каналов не всегда поддается контролю, например в радиоканале между наземным центром управления и низкоорбитальным спутником.

Настоящее и будущее квантовой криптографии

Вышеперечисленные проблемы реальных систем квантовой коммуникации требуют принятия специальных мер. Решить проблему многофотонного импульса можно путем изменения способа кодирования сигнала. Например, предложены схемы, в которых число фотонов в импульсе (то есть его энергия) является одним из параметров состояния квантовой системы и его изменение при «отводе» части квантов становится обнаруживаемым.

Для борьбы с ошибками системы используются различные коды коррекции, а для снижения значимости перехваченных битов — процедура усиления секретности. Кроме того, могут приниматься дополнительные меры защиты чисто технического характера. Так, трудность перехвата сигнала можно существенно увеличить, распараллелив его на несколько путей распространения, как в интерферометре Маха — Цендера. Возможны и более сложные схемы, в которых распараллеленный сигнал мультиплексируется по времени в один канал связи [6]. Эти меры никак не ограничивают теоретическую возможность перехвата данных, но чрезвычайно осложняют практическое осуществление такого перехвата, делая его технически невозможным на данный момент времени.

На пути практической реализации систем квантовой коммуникации возникает ряд таких технических трудностей, как разработка стабильных источников одиночных фотонов и

детекторов одиночных фотонов, которые были бы работоспособны в обычном диапазоне температур и не нуждались в охлаждении жидкими газами. Кроме того, для реального использования важно создание так называемых plug&play-систем, начинающих работать сразу после включения и не нуждающихся в сложной юстировке аппаратуры. Все эти задачи необходимо решить, чтобы перейти от экспериментальных установок к промышленным образцам.

В настоящее время уже несколько фирм (например, компании id Quantique, Magic Technologies) предлагают первые коммерческие системы квантового распределения ключей [7, 8]. Эти системы имеют сходные характеристики: использование оптоволокна в качестве среды передачи, максимальная дальность связи в несколько десятков километров и невысокая скорость выработки ключа (порядка единиц килобит в секунду). С технической точки зрения эти системы еще весьма далеки от совершенства. Основное неудобство в их использовании: необходимость применения сложной физической аппаратуры, которая должна быть заранее размещена у корреспондентов, и ограничение среды передачи данных оптическими каналами. Это делает установку канала «по требованию» практически невозможной: как, например, установить аппаратуру на низкоорбитальном спутнике, если он был запущен без нее или старая аппаратура вышла из строя?

Очевидно, что по массовости применения системы квантовой коммуникации еще очень не скоро смогут приблизиться к асимметричной криптографии: по крайней мере до тех пор, пока возможный прорыв в квантовых вычислениях либо в теории вычислительной сложности не изменит ситуацию. Скорее всего, этот процесс займет не один десяток лет, и вполне вероятно, что мы станем свидетелями постепенного проникновения квантовой криптографии на рынок средств защиты информации, начиная с верхних сегментов этого рынка. Однако уже сейчас системы квантовой коммуникации могут найти применение для защиты особо важных каналов связи или информационных магистралей между крупными центрами обработки данных, то есть там, где чрезвычайно высоки требования к стойкости или очень велик трафик.

Отечественный стандарт шифрования.

Рассмотрим один из наиболее актуальных в настоящее время алгоритмов шифрования информации — отечественный стандарт ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Несмотря на то, что ГОСТ 28147-89 был принят в далеком 1989 году, в наши дни он является весьма широко используемым как в России, так и в мире в целом. Во-первых, этому способствует отечественное законодательство. Государственные организации и ряд коммерческих обязаны использовать для защиты информации только сертифицированные ФАПСИ криптосредства, а получение сертификата ФАПСИ подразумевает, что «в указанных криптосредствах реализованы криптографические алгоритмы, объявленные государственными или отраслевыми стандартами Российской Федерации...». Несмотря на упразднение ФАПСИ в текущем году, нормативные документы, устанавливающие данные требования, действительны и сейчас. Во-вторых, данный алгоритм разрабатывался с огромным запасом в криптостойкости, причем с совсем небольшим ущербом скорости шифрования.

Алгоритм ГОСТ 28147-89 является классическим алгоритмом симметричного шифрования на основе сети Фейстеля (см. схему 10). Данный алгоритм шифрует информацию блоками по 64 бита (такие алгоритмы называются «блочными»). Смысл сети Фейстеля состоит в том, что блок шифруемой информации разбивается на два или более субблоков, часть которых

обрабатывается по определенному закону, после чего результат этой обработки накладывается (операцией побитового сложения по модулю 2) на необрабатываемые субблоки. Затем субблоки меняются местами, после чего обрабатываются снова и т.д. определенное для каждого алгоритма число раз -раундов.

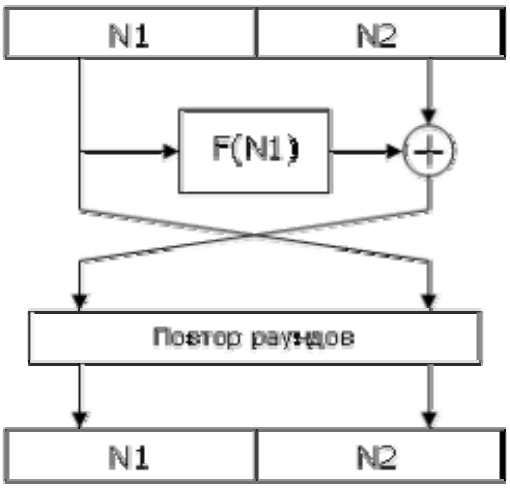

Схема 10. Сеть Фейстеля

Основное отличие алгоритмов симметричного шифрования друг от друга состоит именно в различных функциях обработки субблоков. Данная функция часто называется «основным криптографическим преобразованием», поскольку именно она несет основную нагрузку при шифровании информации. Основное преобразование алгоритма ГОСТ 28147-89 является достаточно простым, что обеспечивает высокое быстродействие алгоритма; в нем выполняются следующие операции (см. схему 11):

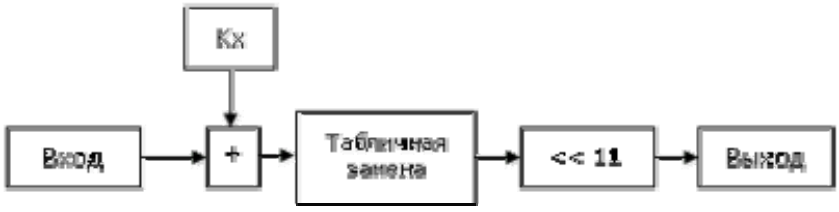

Схема 11. Основное преобразование алгоритма ГОСТ 28147-89

1. Сложение субблока с определенным фрагменом ключашифрования по модулю 2^{32}. Кх — это 32-битная часть («подключ») 256-битного ключа шифрования, который можно представить как конкатенацию 8 подключей: $K = K_0K_1K_2K_3K_4K_5K_6\ K_7$. В зависимости от номера раунда и режима работы алгоритма (о них — ниже), для данной операции выбирается один из подключей.

2. Табличная замена. Для ее выполнения субблок разбивается на 8 4-битных фрагментов, каждый из которых прогоняется через свою таблицу замены. Таблица замены содержит в определенной последовательности значения от 0 до 15 (т.е. все варианты значений 4-битного фрагмента данных); на вход таблицы подается блок данных, числовое представление которого определяет номер выходного значения. Например, подается значение 5 на вход следующей таблицы: «13 0 11 74 91 10 143 5 122 15 8 6». В результате на выходе получается значение 9 (поскольку 0 заменяется на 13, 1 — на 0, 2 — на 11 и т.д.).

3. Побитовый циклический сдвиг данных внутри субблока на 11 бит влево.

Алгоритм ГОСТ 28147-89 имеет 4 режима работы:

1. *Режим простой замены.*
2. *Режим гаммирования.*
3. *Режим гаммирования с обратной связью.*
4. *Режим выработки имитовставок.*

Все режимы используют одно и то же основное преобразование, но с разным числом раундов и различным образом.

Режим простой замены предназначен для шифрования ключей (существует множество схем применения алгоритмов симметричного шифрования, использующих несколько ключей различного назначения; в этих случаях требуется шифрование одних ключей на другие). В данном режиме выполняется 32 раунда основного преобразования. В каждом из раундов, как было сказано выше, используется определенный подключ, который выбирается следующим образом:

$K_{((r-1)\ \%\ 8)}$ *— для раундов с 1 -го по 24-й (r обозначает номер раунда, а % — операция вычисления остатка от деления), т.е.* $K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1, K_2$ *и т. д.;*

$K_{((32-r)\ \%\ 8)}$ *— для раундов с 25-го по 32-й, т.е. в обратном порядке:* $K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0$.

Для расшифровывания информации в режиме простой замены также выполняется 32 раунда основного преобразования, но с использованием подключей по другой схеме:

- *в прямом порядке в раундах с 1-го по 8-й;*
- *в обратном порядке в последующих раундах.*

Для собственно шифрования информации используются режимы гаммирования и гаммирования с обратной связью. В данных режимах шифрование информации производится побитовым сложением по модулю 2 каждого 64-битного блока шифруемой информации с блоком гаммы шифра. Гамма шифра — это псевдослучайная последовательность, вырабатываемая с использованием основного преобразования алгоритма ГОСТ 28147-89 следующим образом (см. Схему 12):

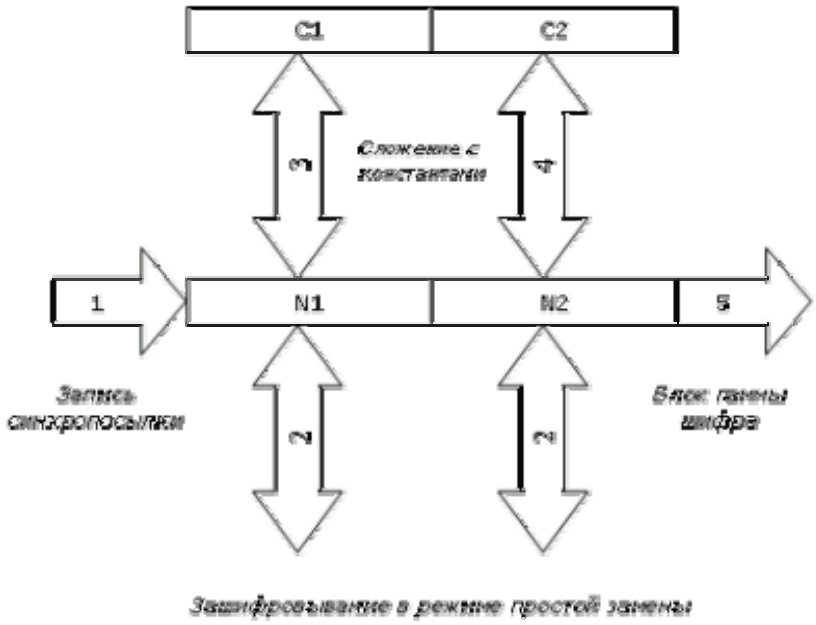

Схема 12. Режим гаммирования

1. В регистры N1 и N2 записывается их начальное заполнение — 64-битная величина, называемая «синхропосылкой».

2. Выполняется зашифровывание содержимого регистров N1 и N2 (в данном случае — синхропосылки) в режиме простой замены.

3. Содержимое N1 складывается по модулю (2^{32} — 1) с константой C1 = $2^{24} + 2^{16} + 2^8 + 2^4$, результат сложения записывается в регистр N1.

4. Содержимое N2 складывается по модулю 2^{32} с константой C2 = $2^{24} + 2^{16} + 2^8 + 1$, результат сложения записывается в регистр N2.

5. Содержимое регистров N1 и N2 подается на выход в качестве 64-битного блока гаммы шифра (т.е. в данном случае N1 и N2 образуют первый блок гаммы).

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

Для последующего расшифровывания аналогичным образом вырабатывается гамма шифра и складывается с зашифрованной информацией. В результате получается исходная информация, поскольку известно, что:

A ? B ? B=A

для любых последовательностей одинаковой размерности A и B, где ? — операция побитного сложения по модулю 2.

Ясно, что для расшифровывания информации необходимо иметь тот же ключ шифрования и то же самое значение синхропосылки, что и при зашифровывании. Существуют реализации алгоритма ГОСТ 28147-89, в которых синхропосылка также является секретным элементом,

наряду с ключом шифрования. Фактически в этом случае можно считать, что ключ шифрования увеличивается на длину синхропосылки (64 бита), что усиливает стойкость алгоритма.

Режим гаммирования с обратной связью отличается от режима гаммирования только тем, что перед возвратом к шагу 2 (для выработки следующего блока гаммы) в регистры N1 и N2 записывается содержимое блока зашифрованной информации, для зашифровывания которого использовался предыдущий блок гаммы.

С помощью режима выработки имитовставок вычисляются имитовставки — криптографические контрольные суммы информации, вычисленные с использованием определенного ключа шифрования. Имитовставки обычно вычисляются до зашифровывания информации и хранятся или отправляются вместе с зашифрованными данными, чтобы впоследствии использоваться для контроля целостности. После расшифровывания информации имитовставка вычисляется снова и сравнивается с хранимой; несовпадение значений указывает на порчу или преднамеренную модификацию данных при хранении или передаче или на ошибку расшифровывания.

В режиме выработки имитовставки выполняются следующие операции:

1. Первый 64-битный блок информации, для которой вычисляется имитовставка, записывается в регистры N1 и N2 и зашифровывается в сокращенном режиме простой замены, в котором выполняется 16 раундов основного преобразования вместо32-х.

2. Полученный результат суммируется по модулю 2 со следующим блоком открытого текста и сохраняется в N1 и N2.

3. И т.д. до последнего блока открытого текста.

В качестве имитовставки используется результирующее содержимое регистров N1 и N2 или его часть (в зависимости от требуемого уровня стойкости) — часто имитовставкой считается 32-битное содержимое регистра N1.

При разработке алгоритма ГОСТ 28147-89 криптографами отечественных спецслужб была заложена избыточная стойкость — до сих пор не известны более эффективные методы взлома данного алгоритма, чем метод полного перебора возможных вариантов ключей шифрования. А полный перебор 2256 ключей (не считая секретной синхропосылки) при современном развитии компьютерной техники за реальное время осуществить невозможно.

Заключение.

В результате проделанного анализа можно сделать выводы:

1. Необходимо понимать важность политики безопасности ЛВС и то, как эта политика влияет на решения, принимаемые относительно защиты ЛВС. Понимать важность определения адекватной степени безопасности для различных типов информации, которой владеет функциональное руководство (или за которые несет ответственность).
2. Понимать, что ЛВС является ценным ресурсом для организации, который требует защиты. Понимать важность обеспечения адекватной защиты (через финансирование, укомплектовывание персоналом, и т.д.).
3. Понимать во всех аспектах, как работает ЛВС. Быть способны отличать нормальную работу системы от ненормальной работы системы.
4. Понимать роль администратора ЛВС в реализации политики безопасности ЛВС.
5. Понимать, как работают службы и механизмы безопасности. Быть способны распознать неправильное использование механизмов защиты пользователями.
6. Повсеместно использовать криптография для конфиденциальной информации

Список используемой литературы:

1. *Diffie W., Hellman M. New Directions in cryptography.*
   // IEEE Transactions on Information Theory ГТ-22. Vol. 6. Nov. 1976
2. *Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.*
   // Proc. the 35th Annual Symp. FOCS. 1994.
3. *Lieven M.K. et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance.*
   // Nature 414. 20-27 Dec. 2001
4. *Bennett C., Brassard G. Quantum Cryptography, Public key distribution and coin tossing.*
   // Proc. Int. Conf. Computer Systems and Signal Processing. Bangalore. 1984.
5. *Bennett C.H. et al. Experimental quantum cryptography.*
   // Journal of Cryptology. Vol. 5. № 1,1992.
6. *Muller A. et al. Plug-and-play systems for quantum cryptography.*
   //Appl, Phys.Lett. Vol. 70. № 7.1997.
7. *Ресурс: www.idquantique.com.*
8. *Ресурс: www.magiqtech.com.*
9. *Мир и безопасность, № 5, 2003 С. Панасенко.*
10. *ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.*
11. *Винокуров А., Применко Э. Новые подходы в построении блочных шифров с секретным ключом.*
12. *PIPS PUB 197. Advanced Encryption Standard (AES).*
13. *NIST Special Publication 800-38A. Recommendation for Block Cipher Modes of Operation.*
14. *Варфоломеев А. и др. Блочные криптосистемы. Основные свойства и методы анализа стойкости. М.: МИФИ, 1998.*