
ДМК
АйТи
СИСТЕМНЫЙ ИНТЕГРАТОР
Петров А. А.
КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
Криптографические методы защиты
информационные технологии для инженеров
ИТИ

**ББК 32.973.26-018.2**
**П30**

**Петров А. А.**
П30 Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК Пресс, 2008. – 448 с.: ил.

**ISBN 5-89818-064-8**

В книге рассматриваются актуальные вопросы защиты данных при создании распределенных информационных систем масштаба предприятия, приводятся подробные описания принципов применения современных криптографических средств, имеющихся на рынке («Криптон», «Верба», «Шип», «Игла» и др.). Значительное место уделяется проблемам сохранения тайны при финансовых обменах через Internet, а также электронной коммерции.

Завершают книгу приложения, посвященные практическим рекомендациям по самым острым вопросам обеспечения защиты информации.

ББК 32.973.26-018.2



ISBN 5-89818-064-8

# Содержание

# Предисловие

В настоящее время первостепенным фактором, влияющим на политическую и экономическую составляющие национальной безопасности, является степень защищенности информации и информационной среды. Вот почему важное значение приобретают вопросы обеспечения безопасности информационных и телекоммуникационных технологий и гарантированной защиты данных в компьютерных сетях экономически значимых структур. О необходимости надежной защиты свидетельствуют многочисленные компьютерные преступления, совершаемые как в кредитно-финансовой сфере, так и в государственных органах. При этом заметно увеличилось число противоправных деяний, совершенных путем удаленных атак с использованием территориально-распределенных сетей передачи данных. Подобные правонарушения опасны тем, что на сегодняшний день устоявшейся практики борьбы с ними не существует.

Вместе с тем необходимо отметить, что, несмотря на резкое возрастание интереса к проблемам защиты информации, в отечественной научно-технической литературе данная тема освещена слабо, и автор в меру своих сил попытался заполнить этот пробел. В предлагаемой книге рассматриваются вопросы применения криптографии для защиты информации в современных информационно-телекоммуникационных системах, отражающие только одну из областей компьютерной безопасности, однако, на взгляд автора, на сегодняшний день наиболее значимую. В книге освещаются как теоретические аспекты применения классической криптографии (глава 1) и современных криптографических протоколов (глава 2), так и практические вопросы (глава 3), которые возникают при осуществлении защиты информации криптографическими методами и средствами.

В данной книге также затрагиваются проблемы защиты платежных систем в Internet, безопасность современных операционных систем (Windows NT и Novell NetWare) и ряд других актуальных вопросов компьютерной безопасности.

Во введении обсуждается терминология, а также цели и задачи, возникающие при обеспечении информационной безопасности. Здесь определяется роль криптографических протоколов как наиболее перспективного

средства защиты в общей задаче сохранения конфиденциальности, целостности и достоверности информационных потоков.

В главе 1 рассматриваются некоторые теоретические аспекты криптографии и описаны способы построения часто используемых на сегодняшний день криптографических алгоритмов. Раздел 1.1 посвящен теоретическим основам применения и реализации криптографических алгоритмов в современных информационно-телекоммуникационных системах. В разделе 1.2 представлены традиционные блочные алгоритмы шифрования; здесь же изложены принципы блочного шифрования и виды применения подобных алгоритмов, а также конкретные алгоритмы – DES и ГОСТ 28147-89. Раздел 1.3 знакомит с асимметричными алгоритмами шифрования; в нем уделяется внимание математическим идеям, а также получившему широкое распространение алгоритму RSA (с точки зрения уязвимости и возможности проведения на него теоретических атак и с точки зрения эффективности его реализации). В разделе 1.4 рассказывается об электронно-цифровой подписи (ЭЦП); при этом разбираются не только конкретные схемы (ГОСТ Р 34.10-94 и DSA), но и атаки на схемы ЭЦП, а также вопросы, связанные с арбитражем ЭЦП. В разделе 1.5 описываются хэш-функции, используемые совместно с алгоритмами ЭЦП, и затрагиваются вопросы их стойкости. В разделе 1.6 излагаются вопросы, связанные с генерацией, хранением и распределением ключей. Здесь также рассматривается актуальный на сегодняшний день вопрос о минимальной длине ключа, необходимой для обеспечения адекватного уровня безопасности.

Вторая глава посвящена интересным и острым на сегодняшний день проблемам построения, реализации и применения криптографических протоколов, таких как протоколы аутентификации, протоколы распределения и управления ключевой информацией и специфические протоколы. В разделе 2.1 излагаются основные принципы их построения и безопасного использования, а также формальные методы их анализа. Несмотря на то что подобные протоколы до сих пор считаются мощным средством обеспечения безопасности в современных информационно-телекоммуникационных системах, в настоящий момент в хорошо известных протоколах уже найдено немало уязвимых мест. В разделе 2.2 обсуждаются различные схемы аутентификации, начиная с простой аутентификации и заканчивая аутентификацией, обладающей свойством нулевого знания. В разделе 2.3 рассматривается недостаточно освещенная в отечественной литературе проблема распределения и управления ключевой информацией, причем описываются протоколы с использованием симметричных и асимметричных алгоритмов. Одной из главных трудностей, возникающих при построении криптографической системы защиты информации в распределенных

системах, как раз является распределение ключевой информации, поэтому данный раздел в современном контексте развития Internet особенно актуален. Кроме этих проблем в разделе 2.3 затронуты вопросы сертификатов открытых ключей, центров сертификации, междоменные отношения и т.д. Раздел 2.4 посвящен интересным, но малоизученным на практике специфическим криптографическим протоколам, призванным решать вопросы безопасности легитимного голосования, группового разделения знания секрета. Приведенные в этом разделе результаты можно активно использовать как в кредитно-финансовой сфере, так и в повседневной жизни.

В главе 3 рассматриваются практические вопросы применения криптографических средств защиты информации для решения типовых задач информационной безопасности. Обсуждение ведется на основе анализа проблемных вопросов информационной безопасности и средств защиты информации, применяемых на сегодняшний день в России и за рубежом. В качестве законченных решений для конкретных задач приводятся некоторые корпоративные решения. В данной главе также затронута область электронной коммерции в Internet, так как эта сфера в последние годы становится наиболее активным потребителем новых идей и средств криптографической защиты информационных потоков. Раздел 3.1 представляет собой своеобразный путеводитель по этой специфической области переработки и накопления данных; здесь также описывается общая проблематика и подходы к решению задач обеспечения информационной безопасности в современных информационно-телекоммуникационных системах. Приведен обзор стандартов в области криптографической защиты обрабатываемых и передаваемых сведений. Раздел 3.2 посвящен проблемам защиты информации локальных рабочих станций (не подключенных к каналам передачи данных). В качестве конкретных средств криптографической защиты информации рассматриваются семейство «Верба», программно-аппаратные комплексы «Аккорд», «Криптон» и др. Также затрагиваются вопросы и задачи информационной безопасности, возникающие при использовании современных операционных систем (на примере Windows NT). Раздел 3.3 посвящен защите информации в локальных сетях передачи данных на примере сетей Windows NT (в том числе и Windows NT 5.0) и Novell NetWare, широко распространенных на отечественном рынке. В данной части анализируются уязвимости протоколов PPTP и CIFS (от Microsoft). В качестве средства, позволяющего решить большинство задач информационной безопасности в локальных сетях передачи данных, рассмотрена система Secret Net NT. В разделе 3.4 освещаются вопросы, связанные с защитой информации в сетях, имеющих выход в другие сети передачи данных. Здесь приводятся общие сведения об угрозах

в распределенных IP-сетях и протоколах, применяемых для защиты информации в Internet, а также описываются функциональные возможности и применение криптографических средств защиты информации для построения виртуальных частных сетей («Шип», «ФПСУ», «Игла-П» и «Застава»). Раздел 3.5 посвящен не менее актуальным вопросам защиты информации в распределенных сетях – защите технологий «клиент-сервер». Многообразие средств защиты данных и задачи информационной безопасности в клиент-серверных технологиях тоже представлены в этом разделе. Здесь читатель познакомится как с хорошо известными средствами защиты информации SSL и Kerberos, так и с их реализацией в виде законченного продукта – Trusted Web. В разделе 3.6 описывается применение межсетевых экранов, proxy-серверов, а также подробно излагается реализация криптографических средств защиты информации в Check Point Firewall-1. Следующий раздел посвящен принципам защиты электронной почты, в том числе таким известным протоколам защищенной электронной почты, как PEM (и его разновидности) и PGP. Отдельно представлена интересная проблема – защита информации в архитектуре X.400, и в качестве конкретной реализации данного вида электронной почты рассмотрен Messenger 400. Раздел 3.8 рассказывает об опыте обеспечения информационной безопасности в виде отдельных корпоративных решений. Причем на этих страницах рассматриваются системы перевода денежных средств и средства обеспечения финансовых операции – SWIFT и Smart City. Раздел 3.9 рассказывает об электронной коммерции в Internet и обеспечении информационной безопасности глобальной сети. Здесь читатель познакомится с понятием электронных денег и с проблемами информационной безопасности, возникающими при использовании смарт-карт.

В приложениях представлены результаты тестирования отечественных средств построения виртуальных частных сетей[1] и приведен общий обзор проблемы санкционированного доступа к ресурсам корпоративной информационной системы предприятия[2].

Автор надеется, что книга окажется полезной не только пользователям, начинающим осваивать данную область человеческих знаний, но и специалистам в сфере компьютерной безопасности.

[1] Авторы И. Гвоздев, В. Зайчиков, Н. Мошак, М. Пеленицин, С. Селезнев, Д. Шепелявый.

[2] Авторы В. С. Лаптев, С. П. Селезнев, М. Ю. Шувалов.

# Глава II

# Теоретические аспекты создания и применения криптографических протоколов

## 2.1. Общие сведения

### 2.1.1. Область применения

Одним из важнейших средств решения задач информационной безопасности в сетях передачи данных являются *криптографические протоколы* (далее – *криптопротоколы*). Их применение обусловлено использованием обширных механизмов межсетевого взаимодействия, причем под межсетевым взаимодействием следует понимать обмен информацией как на сетевом уровне модели взаимодействия открытых систем, так и на вышележащих уровнях.

В общем случае под криптопротоколом будем понимать распределенный алгоритм, реализованный при помощи последовательности действий, позволяющий двум или более участникам информационного обмена решать определенные задачи.

При этом под безопасным будем понимать криптопротокол, в котором участники достигают своей цели, а злоумышленник – нет.

Большинство криптопротоколов в своей основе используют криптографические алгоритмы (блочного шифрования, ЭЦП и хэш-функции), хотя это утверждение не является обязательным – вместо криптографических алгоритмов могут применяться необратимые преобразования, такие как модульное возведение в степень.

Использование криптографических алгоритмов в криптопротоколах (причем в некоторых протоколах используются несколько различных

алгоритмов) приводит к необходимости решить задачу согласования используемых алгоритмов и их параметров между сторонами информационного обмена.

Многообразие механизмов межсетевого взаимодействия, в свою очередь, способствует появлению различных криптопротоколов. Причем они могут решать задачи информационной безопасности как в виде отдельных механизмов (SSL, SHTTP и др.), так и входить в состав других продуктов, связанных с этой областью (например, в TrustedWeb используется Kerberos). Типичным примером использования криптопротоколов может являться решение такой распространенной задачи: клиент (например, HTTP-клиент) хочет получить доступ к серверу (например, к Web-серверу) через открытые сети передачи данных и установить с ним защищенный канал передачи данных. Данная проблема эффективно разрешима только с применением криптопротоколов.

В свою очередь, средства обеспечения информационной безопасности в сетях передачи данных тоже требуют решения ряда специфических задач, поддерживающих их надежное функционирование, что также расширяет сферу применения криптопротоколов. Типичным примером их использования является обеспечение ключевого обмена и согласование параметров безопасности (тип алгоритма, режим применения и т.д.).

Основными задачами сегодняшнего дня, которые решаются криптопротоколами в сетях передачи данных, являются:

- аутентификация и идентификация (см. раздел 2.2);
- ключевой обмен (см. раздел 2.3).

Существует также целый ряд криптопротоколов, предназначенных для решения более специфических задач (см. раздел 2.4).

Следует иметь в виду, что один и тот же криптопротокол может применяться в самых разных областях. Например, криптопротокол Kerberos в ходе своей работы позволяет произвести аутентификацию пользователей и осуществить ключевой обмен между участниками.

В качестве примера можно привести достаточно простой криптопротокол ключевого обмена. Его участники, A и B, хотят выработать общий секретный ключ для симметричного алгоритма шифрования, используя открытые каналы передачи данных. Для этого они используют следующую последовательность действий:

1. Участник B выбирает схему асимметричного шифрования, создает пару ключей для данной схемы – открытый и секретный.
2. Участник B посылает свой открытый ключ участнику A.

3. Участник A создает секретный ключ для симметричного алгоритма шифрования; зашифровывает его на открытом ключе участника B и отсылает ему полученный результат.
4. Участник B, получив зашифрованный секретный ключ от участника A, расшифровывает его на своем секретном ключе для асимметричного алгоритма.

Теперь A и B, используя симметричный алгоритм шифрования, могут обмениваться зашифрованной информацией по открытым каналам связи. Приведенный выше криптопротокол не является безопасным, но хорошо отражает саму идею построения подобных средств защиты информации.

### 2.1.2. Вопросы безопасности криптопротоколов

Как и в случае использования криптографических алгоритмов, главный вопрос, который задают заинтересованные пользователи, заключается в том, насколько стойким является тот или иной криптопротокол. Ответ на него можно найти при сравнении целого ряда факторов, которые мы рассмотрим ниже. Однако, поскольку в основе многих криптопротоколов лежат именно криптографические алгоритмы, очевидно, что окончательная стойкость будет не больше стойкости используемых криптографических алгоритмов. Она может быть существенно снижена в следующих случаях:

- использование слабых криптографических алгоритмов и некорректная реализация некоторых ее составляющих;
- некорректная логика работы криптопротокола;
- некорректное использование криптографических алгоритмов.

Трудности первой категории решаются в рамках классической криптографии. Типичным примером в этом смысле является использование слабых генераторов случайных чисел.

Проблемы, относящиеся ко второй категории, наиболее распространены. На практике именно по этим «болевым точкам» обычно проводятся атаки на криптопротоколы. Активный нарушитель может оказывать влияние на функционирование криптопротокола путем следующих атак:

- *атака с известным ключом*. Злоумышленник, получив ключ предыдущей сессии, пытается узнать ключ новой сессии;
- *повторная передача*. Перехватив в предыдущих сессиях определенную порцию информации, злоумышленник передает ее в последующих сессиях;

- *подмена стороны информационного обмена*. В процессе установления сеанса связи между легальными пользователями злоумышленник в случае подобной атаки пытается выдать себя за одного из них либо инициировать от имени легального пользователя установление связи;
- *атака со словарем*. Заключается в подборе пароля, содержащего наиболее часто встречающиеся слова или комбинацию букв/цифр. Обычно преобразованные при помощи неключевой хэш-функции пароли хранятся в файлах на компьютере. Задача злоумышленника состоит в том, чтобы получить искомый файл, преобразовать свой словарь посредством данной хэш-функции и произвести сравнения с целью найти совпадающие значения. Подобный тип атак может применяться и для сообщений;
- *подмена сообщений*. Производится путем замены во время работы криптопротокола сообщений или данных.

В качестве примера успешной атаки такого типа рассмотрим криптопротокол распределения секретных сеансовых ключей между двумя участниками информационного обмена (рис. 2.1). Авторами этого метода являются Нидхэм и Шредер. Уязвимость рассматриваемого криптопротокола впервые была обнаружена Денингом и Сакко. Каждый участник данного протокола должен разделить знание своего секретного ключа с сервером аутентификации. Протокол состоит из следующих шагов:

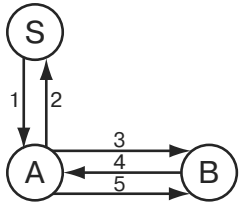


*Рис. 2.1. Протокол распределения секретных сеансовых ключей*

1. $A \rightarrow S$: A, B, $N_a$. Участник A посылает запрос серверу S, в котором он указывает, что необходимо установить сеанс связи с участником B. В данном запросе присутствуют следующие значения:
   – A и B – имена или идентификаторы участников;
   – $N_a$ – уникальное для данного сеанса число; используется для предотвращения повторных передач путем включения его в последующие сообщения.
2. $S \rightarrow A$: $\{N_a, B, K_{ab}, \{K_{ab}, A\}_{Kbs}\}_{Kas}$. Сервер отвечает сообщением, зашифрованным на секретном ключе сервер-участник A ($K_{as}$), в котором находится сеансовый ключ ($K_{ab}$), а также еще одна копия этого ключа, зашифрованного на секретном ключе сервер-участник B ($K_{bs}$).
3. $A \rightarrow B$: $\{K_{ab}, A\}_{Kbs.}$ Участник B расшифровывает данное сообщение, поскольку ему известен ключ $K_{bs}$; в результате он получает ключ $K_{ab}$.

4. B → A: $\{N_b\}_{Kab.}$ Данное сообщение участник B посылает для того, чтобы убедиться, что A владеет ключом $K_{ab}$, и показать участнику A свое знание $K_{ab}$.
5. A → B: $\{N_b - 1\}_{Kab}$. Участник A доказывает свое владение ключом $K_{ab}$, и на этом протокол заканчивает свою работу, в результате участники A и B получают общий секретный сеансовый ключ $K_{ab}$.

Уязвимость данного криптопротокола состоит в том, что если сеансовый ключ $K^1_{ab}$ из предыдущей сессии был скомпрометирован, то злоумышленник (обозначим его через C), получивший возможность контроля сетевого трафика на шаге 3 новой (нескомпрометированной) сессии, перехватывает сообщение (A → B: $\{K_{ab}, A\}_{Kbs}$) и вместо него посылает сообщение (C → B: $\{K^1_{ab}, A\}_{Kbs}$). Участник B отвечает сообщением (B → A: $\{N_b\}K^1_{ab}$), полагая, что A хочет установить с ним новую сессию с ключом $K^1_{a\,b}$. C, получая данное сообщение, расшифровывает его и отправляет B сообщение (C → B: $\{N_b - 1\}\ K^1_{a\ b}$). Таким образом, C устанавливает сессию с B от имени A.

С точки зрения понимания возможных последствий, возникающих при обнаружении недоработок в логике работы криптопротокола, этот пример является очень показательным. Для устранения подобных проблем были специально разработаны средства и методы анализа корректности построения логики работы криптопротоколов. Применение формальных методов позволяет также обнаружить коммуникационную избыточность в криптопротоколах, что является немаловажным плюсом в условиях постоянно возрастающих требований к оперативности обработки информации в современных сетях передачи данных.

Третья группа атак, существенно понижающих уровень безопасности при использовании криптопротоколов, является наименее распространенной. Об этом, по крайней мере, можно судить по частоте их использования злоумышленниками. Но с другой стороны, в силу их трудного обнаружения, такие попытки являются наиболее опасными, поскольку они во многом зависят от математических свойств используемых криптографических алгоритмов. Подобные уязвимые места не поддаются формальному анализу и поэтому не могут обнаруживаться даже при использовании хорошо изученных криптопротоколов. Особенно характерно появление слабых точек при использовании асимметричных алгоритмов, так как они в основном построены на невозможности эффективного решения некоторых математических задач и не поддаются строгим математическим доказательствам и исследованиям с помощью формальных методов.

Нам остается дать несколько полезных советов, с помощью которых в какой-то мере можно избежать отдельных атак на криптопротоколы.

### *Полезные советы*

Первый совет заключается в том, что перед зашифровыванием данных их необходимо подписывать. Если добавить подпись к уже зашифрованным данным, то может возникнуть ситуация, когда нельзя убедиться в том, что подписывающий имел представление о содержании подписываемой информации, а это обстоятельство приводит к невозможности доказать арбитру аутентичность подписи.

Приведем следующий пример.

Предположим, что участник A сначала зашифровывает сообщение M на открытом ключе $e_B$ участника B, а затем подписывает его на своем секретном ключе $d_A$. Сообщение, передаваемое по открытым каналам связи, будет иметь вид:

$$((M^{eb} (\mathrm{mod}\ n_B))^{da}\ (\mathrm{mod}\ n_A)$$

Участник B имеет разложение $n_B$, и его множители могут оказаться длиной 200–300 бит. Тогда, используя теорему об остатках, участник B может найти такое x, что:

$$(M^1)^X = M (\mathrm{mod}\ n_B),$$

где $M^1$ – сообщение, на которое необходимо перенести подпись участника A.

Для успешного проведения атак участнику B нужно только зарегистрировать следующий открытый ключ ($xe_B$, $n_B$), после чего он может доказать, что участник A подписал сообщение $M^1$, а не M. Атака подобного рода может быть реализована на протоколе CCITT X.509, где подписываются сообщения вида $\{T_A, N_A, B, X, \{Y\}^{Eb} (\mathrm{mod}\ n_B)\}$, в которых X и Y – данные пользователя. Она также работает и в случае использования алгоритма Эль-Гамаля.

Следующий совет сводится к необходимости иметь механизмы, дающие пользователю возможность однозначно различать (идентифицировать) участников информационного обмена, а также позволяющие отличать разные сессии при использовании криптопротокола. Это требование особенно важно в том случае, когда подписание и расшифрование производится с применением асимметричного алгоритма (например, RSA), в котором используются одинаковые секретные ключи. Это вполне реальный вариант, поскольку в RSA, например, процессы генерации подписи и расшифрования являются одинаковыми математическими операциями.

Поэтому рекомендуется избегать ситуаций, когда для генерации подписи и для расшифрования сообщения используются одни и те же ключи или ключи, связанные друг с другом некоторым элементарным преобразованием.

Для обеспечения идентификации участника информационного обмена существует большое количество методов и средств. Необходимо отметить, что идентификация является синонимом термина «аутентификация пользователя» (см. раздел 2.2). Различие в сессиях протокола при этом реализуется, как правило, двумя методами:

- с помощью временных вставок;
- посредством случайного числа.

При этом, однако, сразу возникают сложности, связанные с доказательством того, что число, характерное для какой-либо сессии, ранее не использовалось. С временными вставками дело обстоит несколько иначе, поскольку проблемой в данном случае является синхронизация времени у всех участников информационного обмена.

Еще один совет (или принцип) заключается в том, чтобы каждый заинтересованный пользователь разумно применял избыточность в передаваемых сообщениях (например, в сообщениях установления сеансового ключа или передачи сертификата). Будьте уверены, что в данном контексте приложения вам необходима определенная избыточность и при этом наличие дополнительного количества битов не приводит к уязвимости системы, но и в этом вопросе следует соблюдать меру. Распространенным примером отыскивания злоумышленником слабых мест подобного вида является использование избыточной информации в протоколе «игра в покер по телефону», что позволяет установить, является ли переданное сообщение квадратичным вычетом, а далее, принимая во внимание свойства квадратичных вычетов, с большой долей вероятности «взломать» данный протокол.

Теперь необходимо упомянуть об обязательной проверке данных, пересылаемых в процессе выполнения протокола, на предмет установления истинного источника сообщения, и не принимать информацию без проведения соответствующих проверок. Это пожелание тоже очень важно для обеспечения безопасности передаваемой информации.

И наконец, используйте в работе только хорошо известные криптографические механизмы защиты информации.

### 2.1.3. Формальные методы анализа криптопротоколов

Выявление уязвимостей в известных криптопротоколах, которые до определенного момента считались надежными, предполагает разработку

формальных методов их анализа. Из существующих на сегодняшний день подходов к этому вопросу можно выделить четыре основных:

- моделирование и проверка работы протокола. Для этой цели полезно использовать специализированные языки и инструментарии, которые не создавались для анализа криптопротоколов;
- создание экспертных систем, которые разработчики криптопротоколов могут применить для апробирования различных сценариев функционирования криптопротокола;
- моделирование требований к семейству криптопротоколов. При этом можно употребить логику, разработанную специально для анализа таких свойств криптопротокола, как «знание» и «доверие»;
- разработка формальных моделей, основанных на алгебраических свойствах криптографических систем.

Каждый из перечисленных подходов не привязан к лежащим в основе криптопротоколов механизмам, а направлен только на анализ логики работы протокола.

### *Использование специализированных языков и инструментариев*

Данный подход является наименее распространенным, поскольку его основная идея заключается в представлении криптопротокола как программы с последующей попыткой доказательства его корректности. Однако тут же необходимо отметить, что из доказательства корректности протокола не следует доказательство его безопасности. Наиболее успешными в данном направлении считаются формальные методы, автором которых является Кеммерер, и формальный язык LOTOS (Language of Temporal/Ordering Specification), созданный для анализа протоколов аутентификации. Кеммерер в своих работах выделил две цели, для достижения которых можно использовать формальные методы анализа криптопротоколов:

- формальный анализ того, что криптопротокол удовлетворяет требованиям безопасности;
- обнаружение уязвимостей в криптопротоколах.

Формальная модель построена на использовании конечных автоматов, по отношению к которым криптопротокол рассматривается как набор различных состояний, отличающихся друг от друга значениями переменных состояния. При этом значения переменных могут быть изменены только с помощью строго определенных процедур.

Примером использования конечных автоматов является анализ протоколов аутентификации. Для каждой процедуры (итерации криптопротокола)

определяется состояние криптопротокола (системы), выражающееся в описании состояний участников и коммуникационных каналов между ними. После чего каждый набор состояний анализируется на предмет корректности и отсутствия тупиковых ситуаций.

### *Применение экспертных систем*

Использование экспертных систем для исследований криптопротоколов заключается в апробировании различных сценариев работы криптопротокола. В основе применения данных систем – задание некорректных состояний и изучение результатов их обработки криптопротоколом. Этот подход позволяет более эффективно, чем в первом случае, определять наличие в криптопротоколе уязвимостей, но не доказывает безопасность его использования, а также не дает возможности работать с ним в автоматических инструментариях для изучения различных атак на криптопротоколы. Другими словами, он позволяет определить, содержит ли криптопротокол известную уязвимость, но найти с его помощью новые уязвимости достаточно сложно.

На практике экспертные системы применяются совместно с BAN-логикой или формальными моделями. Так, например, метод, зафиксированный в данном подходе, реализован как часть протокольного анализатора NRL.

### *BAN-логика*

Это направление на сегодняшний день наиболее развивающееся. В его основе – логика, разработанная для анализа свойств «знания» и «доверия» работы криптопротокола в целом или его отдельных частей. Ярким представителем подобного метода является BAN-логика, которая и послужила началом развития этого же направления.

Использование BAN-логики позволяет найти ответы на следующие вопросы:

1. Каких результатов в конечном счете можно достичь с помощью криптопротокола?
2. Содержатся ли в данном криптопротоколе избыточные шаги, которых можно было бы избежать, сохранив безопасность работы криптопротокола на прежнем уровне?
3. Необходимо ли зашифровывать данное сообщение или его можно передать в открытом виде?
4. Нужно ли включить в данный криптопротокол дополнительные шаги?

**Постулаты, применяемые в BAN-логике**

*P believes X* – P верит в то, что X истинно.

*P sees X* – кто-либо послал P сообщение, содержащее X, и P может прочитать и повторить X (возможно после проведения процедуры расшифрования).

*P said X* – P когда-либо посылал сообщение, содержащее X, и при этом P доверял X в момент его передачи.

*P control X* – P имеет права на X.

*#(X)* – данная конструкция означает, что X не было использовано в предыдущих итерациях протокола.

$P \xleftrightarrow{K} Q$ – P и Q разделяют между собой ключ K, соответственно P и Q доверяют друг другу.

$\xrightarrow{K} P$ – P имеет открытый ключ K, соответствующий секретному ключу $K^{-1}$, который никогда не будет раскрыт другими участниками криптопротокола.

$P \xleftrightarrow{X} Q$ – X – секретная формула, известная только P и Q, и эту формулу P и Q могут использовать для идентификации друг друга.

$\{X\}_K$ *from P* – данная конструкция означает, что формула X была зашифрована на ключе K, принадлежащем P.

**Некоторые правила BAN-логики**

Приведенные правила при анализе криптопротоколов могут дополняться, однако в некотором роде их можно считать основополагающими, поскольку они описывают наиболее распространенные ситуации.

$$\frac{P believes Q \xleftrightarrow{K}, P sees \{X\}_K}{P believes Q said X}$$

Если P верит, что Q и P разделяют между собой секретный ключ K, и видит сообщение X, зашифрованное на ключе K, и к тому же P не зашифровывал данное X на ключе K, тогда P имеет основания верить, что X было послано Q.

$$\frac{P believes \#(X), P believes Q believes X}{P believes X}$$

Если P верит в то, что X до этого не использовалось и что Q посылал X, тогда P может полагать, что Q доверяет X.

$$\frac{P believes Q controls X, P believes Q believes X}{P believes X}$$

Если P верит, что Q имеет права на X, и P верит, что Q доверяет X, тогда P доверяет X.

Согласно BAN-логике, прежде чем приступить к анализу криптопротокола, его необходимо представить в идеализированной форме. Например, процесс передачи сообщения $A \rightarrow B$: $\{A, K_{ab}\}_{Kbs}$ в идеализированной форме может быть зафиксирован в следующем виде: $A \rightarrow B$: $\{A \xleftrightarrow{Kab} B\}_{Kbs}$. Когда же B получит это сообщение, его можно в соответствии с правилами BAN-логики записать так: B sees $\{A \xleftrightarrow{Kab} B\}_{Kbs}$. В идеализированной форме часть сообщения, которая не участвует в доказательстве, опускается. Значит, открытая часть сообщения не включается в идеализированную форму, поскольку она может быть изменена злоумышленником. В общем случае идеализированная форма сообщения выглядит так: $\{X_1\}_{K1} \ldots \{X_n\}_{Kn}$, где каждое зашифрованное сообщение представлено независимо от других.

Отсюда можно сделать вывод, что анализ предполагает следующие шаги:

1. Представление протокола в идеализированной форме.
2. Присвоение начальных значений.
3. Применение логических формул к состояниям протокола для получения утверждений о состоянии системы после каждого шага протокола.
4. Применение логических постулатов к начальным значениям и последовательности утверждений для изучения доверия частям протокола.

Итак, криптопротокол в BAN-логике – это последовательность состояний $S_1 \ldots S_n$, каждое из которых представляется в виде $P \rightarrow Q$: X, где $P \neq Q$. Между состояниями вставляется последовательность утверждений. Они заключаются в комбинировании постулатов вида P believes X. Структурно это может быть представлено в следующем виде:

Начальные значения
$S_1$[утверждение 1]$S_2$ ... [утверждение n –1]$S_n$

**Выводы**

На практике BAN-логика зарекомендовала себя с положительной стороны, особенно после того, как с ее помощью были найдены уязвимости в хорошо известных криптопротоколах, таких как Needham-Schroeder, CCITT X.509 и др. Точно так же была доказана избыточность в Kerberos, Yahalom, Andrew RPC handshake и CCITT X.509. Однако и в BAN-логике существует ряд проблемных вопросов. Нессет продемонстрировал простой пример, показывающий, что BAN-логика способна доказать свойства безопасности протокола, являющиеся заведомо ложными.