УДК 629.07.5

А.А. Кузнецов[1], С.П. Евсеев[1], Б.П. Томашевский[2], Ю.И. Жмурко[2]

[1]*Харьковский университет Воздушных Сил им. И. Кожедуба*
[2]*Львовский Военный институт Сухопутных войск имени гетмана Петра Сагайдачного*

ИССЛЕДОВАНИЕ ПРОТОКОЛОВ И МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

Исследуются протоколы защиты информации в компьютерных сетях. Анализируются перспективные направления развития криптографических преобразований для обеспечения конфиденциальности, аутентификации и целостности информации.

аутентификация, конфиденциальность, целостность, MAC-коды, хэш-функции

Введение

Постановка проблемы в общем виде и анализ литературы. Методы защиты информации динамически развиваются, усложняются и постепенно оформляются в отдельную отрасль информационно-коммуникационных технологий [1 – 5].

Для защиты информации с ограниченным доступом применяются различные криптографические средства [3 – 6]. **Целью статьи** является исследование протоколов и механизмов защиты информации в компьютерных системах и сетях, анализ перспективных направлений развития криптографических преобразований для обеспечения конфиденциальности, аутентификации и целостности информации.

Проблема защиты компьютерных сетей от несанкционированного доступа приобрела особую остроту. Развитие коммуникационных технологий позволяет строить сети распределенной архитектуры, объединяющие большое количество сегментов, расположенных на значительном удалении друг от друга. Все это вызывает увеличение числа узлов сетей и количества различных линий связи между ними, что, в свою очередь, повышает риск несанкционированного подключения к сети и доступа к важной информации. Особенно неблагоприятной такая перспектива может оказаться для государственных или военных структур, обладающих секретной информацией государственного или любого другого характера. В этом случае необходимы специальные средства идентификации пользователей в сети, обеспечивающие доступ к информации лишь в случае полной уверенности в наличии у пользователя прав доступа к ней. В табл. 1 приведены основные типы угроз нарушения защиты, возникающие при использовании компьютерных сетей (КС). Анализ табл. 1 показывает, что атакам подвержены все уровни эталонной модели ВОС.

В целях защиты информации в различных комбинациях используются контроль доступа, авторизация и шифрование информации, дополненные резервированием. Распределение услуг и механизмы безопасности по уровням эталонной модели взаимодействия открытых систем (ВОС) представлены на рис. 1 [1, 2, 6].

Таблица 1

Характеристики угроз нарушения защиты

Показатели	Угрозы	Последствия
Аутентификация	Попытки нарушителя выдать себя за легального пользователя. Фальсификация данных.	Неправильное представление пользователей. Доверие к искаженным данным.
Целостность	Изменение пользовательских данных. Внедрение “троянских коней”. Изменение информации в памяти. Изменение потока сообщений на пути их передачи.	Потеря информации Компрометация системы. Уязвимость в отношении угроз нарушения защиты всех остальных типов.
Конфиденциальность	Перехват данных в сети. Кража информации, хранящейся на сервере. Кража информации, хранящейся на компьютере Получение информации о конфигурации сети. Получение информации о пользователе, обращающемся к серверу.	Потеря информации. Нарушение тайны информации.
Отказ в обслуживании	Прекращение сеанса доступа пользователя. Перегрузка машины потоком фальшивых попыток доступа. Умышленное переполнение дискового пространства или оперативной памяти. Изоляция системы путем атак на DNS-сервер.	Разрушительные последствия для системы. Раздражение пользователей. Задержки в работе пользователей.

Рассмотрим основные механизмы и услуги, обеспечивающие аутентификацию, целостность и конфиденциальность передаваемой информации в компьютерных системах и сетях.

Аутентификация гарантирует, что сообщение действительно поступило из предполагаемого источника, а также защиту от модификаций, задержек, повторного воспроизведения и изменения порядка следования сообщений [4, 5]. Для обеспечения аутентификации используются алгоритмы *шифрования, цифровая подпись, коды аутентичности сообщения (MAC) и функции хэширования.* Рассмотрим механизмы и протоколы, обеспечивающие аутентификацию сообщений, подробнее.

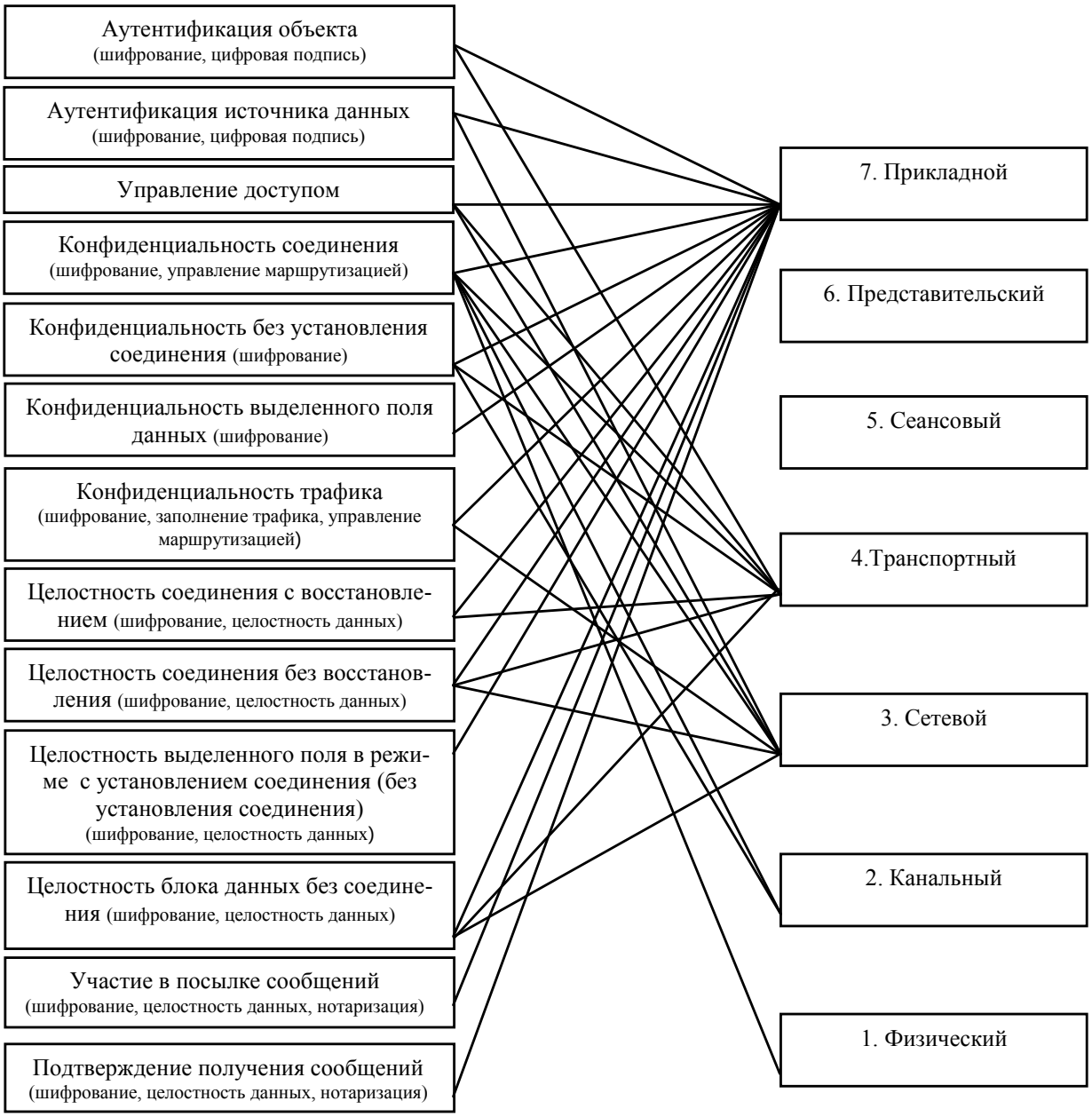


Рис. 1. Распределение услуг и механизмы безопасности по уровням эталонной модели ВОС

При использовании алгоритмов *симметричного шифрования* обеспечивается конфиденциальность и определенный уровень аутентификации. Алгоритмы *несимметричного шифрования* обеспечивают и конфиденциальность, и аутентификацию передаваемых сообщений.

На рис. 2 представлены три варианта защиты сообщений с использованием несимметричного шифрования. Первый вариант – передача сообщений с открытым ключом абонента В (KU_B) – представлен на рис. 2, а. При этом обеспечивается конфиденциальность сообщения (только абонент В имеет закрытый ключ KR_B), недостатком схемы является невозможность обеспечить аутентификацию (любой абонент может воспользоваться открытым ключом KU_B, чтобы объявить себя абонентом А).

Второй вариант – использование абонентом А при отправке сообщения своего секретного ключа (KR_A) – представлен на рис. 2, б. При этом обеспечивается аутентификация и цифровая подпись (только сторона А имеет секретный ключ KR_A). Недостатком схемы является возможность любого пользователя использовать открытый ключ RU_A, чтобы проверить подпись.

Третий вариант – использование абонентами своих ключей для обмена сообщениями – представлен на рис. 2, в. При этом обеспечивается конфиденциальность, цифровая подпись (поскольку используется открытый ключ KU_B) и аутентификация (поскольку используется закрытый ключ KR_A).

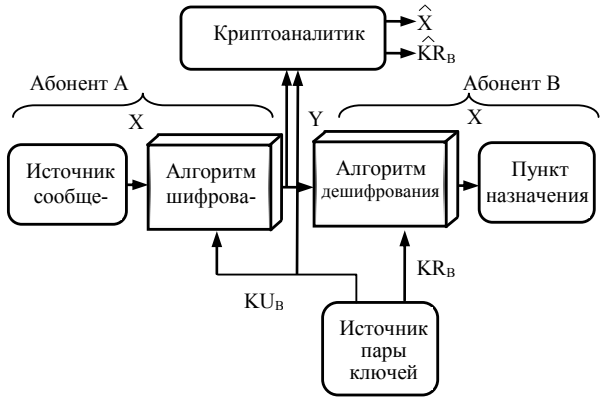


Рис 2, а. Криптосистема с открытым ключом: конфиденциальность

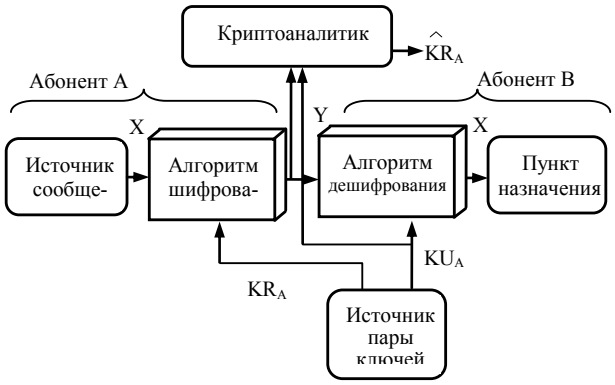


Рис 2, б. Криптосистема с открытым ключом: аутентификация

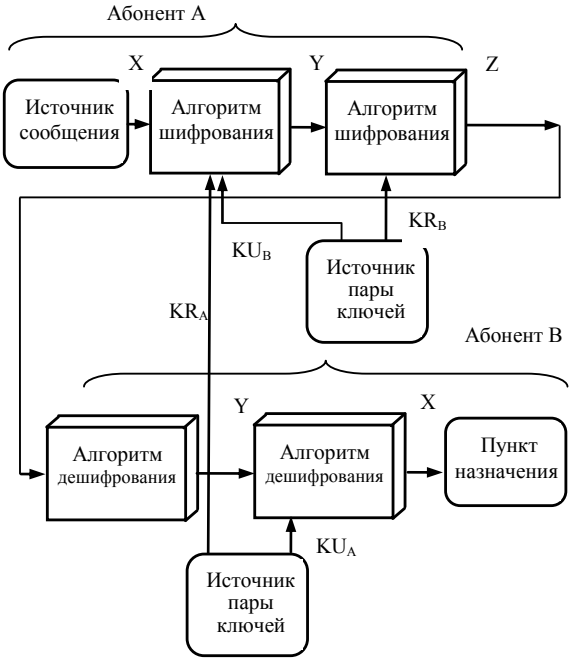


Рис 2, в. Криптосистема с открытым ключом: конфиденциальность и аутентификация

Общими недостатками при использовании симметричного шифрования и шифрования с открытым ключом являются невозможность изменения пути следования пакетов данных, и открытый доступ ко всей порции данных при ее обработке в промежуточных блоках (маршрутизаторах, шлюзах и т.д.).

Альтернативным вариантом шифрованию является присоединение к сообщению созданного с использованием секретного ключа небольшого блока данных фиксированного размера, называемого *криптографической контрольной суммой,* или *кодом аутентичности сообщения* MAC (MAC – Message Authentication Code).

При этом обеспечивается аутентификация, но не конфиденциальность, поскольку сообщение передается в открытом виде. Конфиденциальность передаваемого сообщения может быть обеспечена либо после, либо перед применением алгоритма MAC. Для некоторых приложений не требуется сохранять секретность, но важно проверить аутентичность сообщений. Примером может служить *протокол SNMP* версии 3, где функции конфиденциальности и аутентификации разделяются. В этом приложении гарантируется аутентификация поступающих SNMP-сообщений, в тоже время необходимость скрывать поток обмена данными SNMP может не требоваться.

Вариацией идеи использования кодов аутентичности сообщений является *односторонняя функция хэширования*, обеспечивающая аутентификацию, цифровую подпись и конфиденциальность. Рассмотрим способы защиты сообщений при использовании хэш-кода, представленных на рис.3:

1. Сообщение вместе с присоединенным к нему путем конкатенации хэш-кодом шифруется методами симметричного шифрования. При этом обеспечиваются конфиденциальность (только стороны А и В знают симметричный ключ (К)) и аутентификация (хэш-код H(M) криптографически защищен) (рис. 3, а).

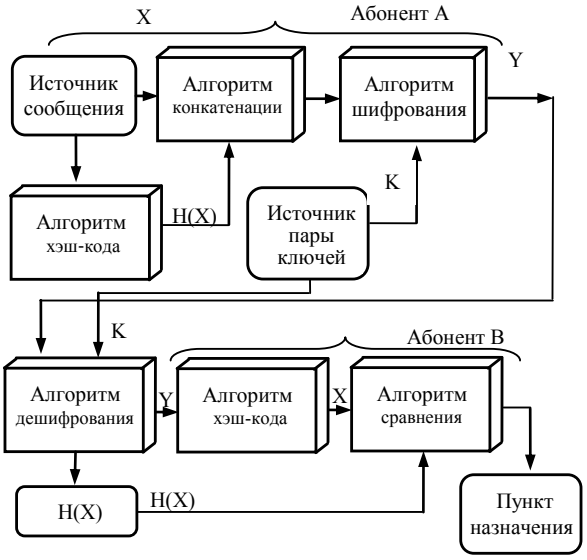


Рис. 3, а. Схема использования хэш-кода: конфиденциальность и аутентификация

2. Шифруется только хэш-код средствами симметричного шифрования. При этом хэширование и симметричное шифрование в комбинации фактически дают код аутентичности и обеспечивают аутентичность передаваемого сообщения (H(M) криптографически защищен) (рис. 3, б).

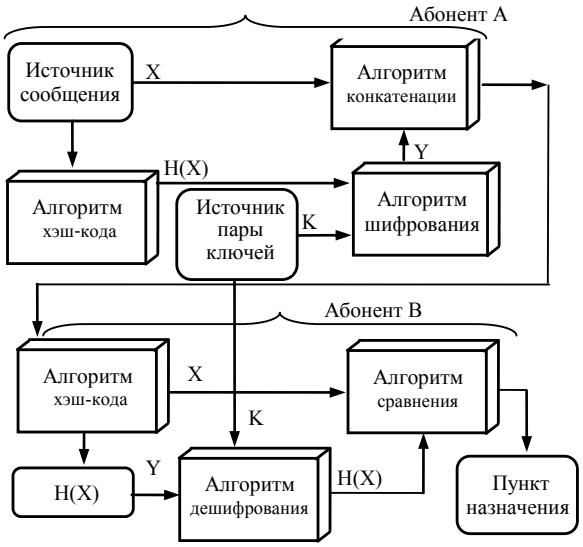


Рис. 3, б. Схема использования хэш-кода: аутентификация

3. Шифруется только хэш-код средствами шифрования с открытым ключом с использованием личного ключа отправителя. При этом обеспечивается не только аутентификация, но и цифровая подпись, так как только отправитель может произвести зашифрованный хэш-код (H(M) криптографически защищен (только сторона А может создать свой секретный ключ (KR_A)).

Фактически в этом и заключается суть техники использования цифровой подписи (рис. 3, в).

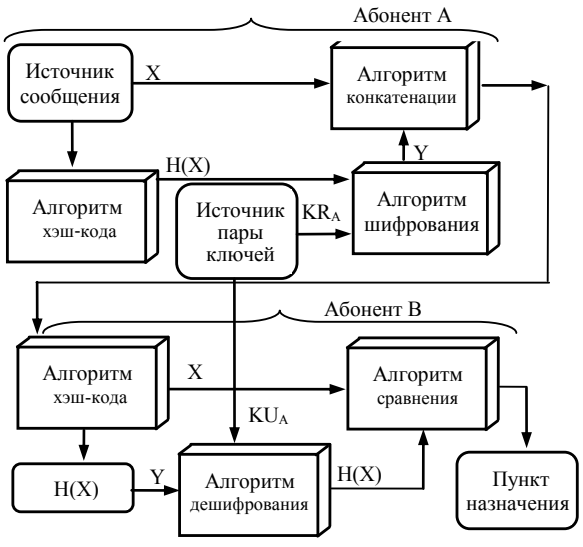


Рис. 3, в. Схема использования хэш-кода: аутентификация и цифровая подпись

4. Если требуется обеспечение не только конфиденциальности, но и цифровой подписи, можно зашифровать сообщение вместе с хэш-кодом, шифрованным открытым ключом. При этом обеспечивается аутентификация, цифровая подпись и конфиденциальность (только стороны А и В знают К) (рис. 3,г).

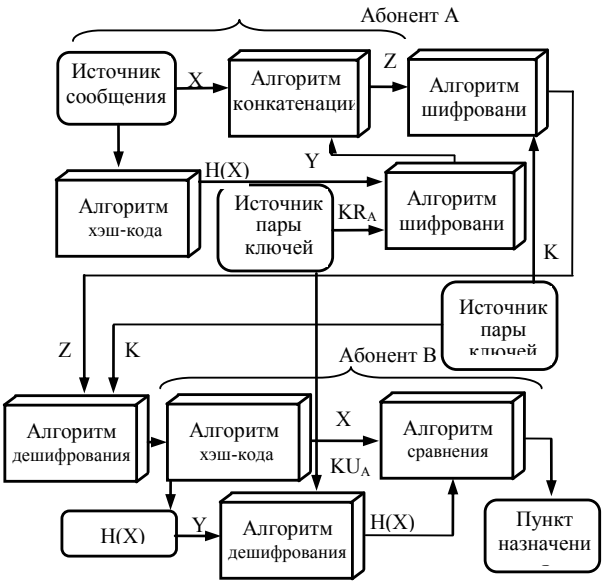


Рис. 3, г. Схема использования хэш-кода: конфиденциальность, аутентификация и цифровая подпись

5. В целях аутентификации сообщений можно использовать функцию хэширования без шифрования. В этом случае предполагается, что обе стороны используют известное им секретное значение S. Отправитель А вычисляет значение функции хэширования для результата конкатенации сообщения (X) и S, и присоединяет полученное значение функции хэширования к X. Получателю В значение S известно, поэтому он может вычислить значение функции хэширования. При этом обеспечивается аутентификация (только А и В знают S) (рис. 3, д).

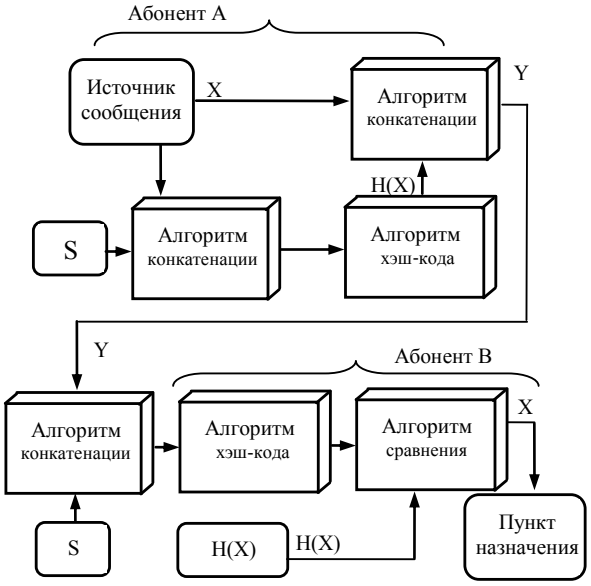


Рис. 3, д. Схема использования хэш-кода: аутентификация

6. Конфиденциальность может быть обеспечена при некоторой модификации подхода, описанного в п. 5, если зашифровать сообщение вместе с добавленным к нему хэш-кодом (рис. 3, е).

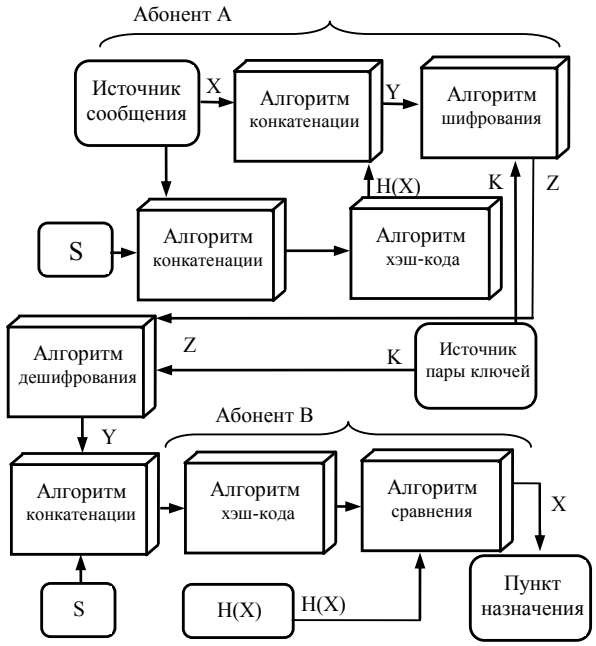


Рис. 3, е. Схема использования хэш-кода: конфиденциальность

Когда конфиденциальность не требуется, методы (б) и (в) оказываются предпочтительнее, поскольку требуют меньше вычислений.

Способность *функции хеширования* позволяет противостоять атакам с перебором всех вариантов, т.к. зависит исключительно от длины хеш-кода. При этом функция хеширования должна обладать следующими свойствами: односторонность, слабая сопротивляемость коллизиям, сильная сопротивляемость коллизиям. Для кода длины *n* порядок требуемых усилий пропорционален: односторонность – 2^n, слабая сопротивляемость коллизиям – 2^n, сильная сопротивляемость коллизиям – $2^{n/2}$ [4].

Одними из перспективных алгоритмов хэш-функций являются SHA-1 и RIPEMD-160. Основные их характеристики представлены в табл. 2 в сравнении с алгоритмом хэш-функции MD-5.

Таблица 2

Основные характеристики алгоритмов хэш-функций

Параметры	MD-5	SHA-1	RIPEMD-160
Длина профиля	128 битов	160 битов	160 битов
Базовая длина блоков	512битов	512битов	512битов
Число шагов/раундов	64 /4	80/4	160/5
Мах. длина сообщения	∞	2^{64} - 1 битов	2^{64} - 1 битов
Число прим. логических функций	4	4	5
Число аддитивных констант	64	4	9
Порядок следования битов	Прямой	Обратный	Прямой

Все три алгоритма неуязвимы в отношении атак, основанных на нарушении слабой сопротивляемости коллизиям. При 128-битовой длине алгоритм *MD-5* подвержен криптоанализу, а дополнительная сложность SHA-1 и RIPEMD-160 приводит к замедлению обработки алгоритмов. Дальнейшим применением MD-5 является *алгоритм HMAC*.

Алгоритм HMAC обеспечивает гарантированную защищенность при условии, что встроенная функция хэширования обладает определенной криптографической стойкостью.

Для обеспечения только функции цифровой подписи используется *стандарт DSS* (Digital Signature Standards – стандарт цифровой подписи), основанный на алгоритме хэширования *SHA*.

Подход DSS основан на функции хэширования. *Алгоритм цифровой подписи DSA* (Digital Signature Algorithm) создан на основе схемы Эль-Гамаля и Шнорра. Существенным его недостатком является сложность вычисления при возведении в степень $g^k mod\ p$. Для обеспечения аутентификации на каждом сервере используется *система Kerberos*, в которой применяется исключительно симметричное шифрование. Она обеспечивает идентификацию пользователей при каждом вызове соответствующего сервера и идентификацию серверов для пользователей. В системе Kerberos используются простейшие протоколы удаленного доступа *PAP* (Password Authentication Protocol) и *CHAP* (Challenge Handshake Authentication Protocol)**.**

Недостатком применения *PAP* является возможность перехвата нарушителем сведений о пароле. Поэтому протокол PAP используется совместно с протоколом *S/Key*, основанном на модели одноразовых паролей, получаемых последовательным применением необратимой функции.

Протокол CHAP основан на модели “рукопожатия” – передача клиентом пароля в хешированном виде с использованием полученного от сервера случайного числа. В качестве случайного числа выбирается значение текущих даты и времени в секундах, к которому присоединяется случайное число, полученное от генератора псевдослучайных чисел.

К достоинствам протокола Kerberos относятся:

- быстрое подсоединение клиента к серверу;
- возможность делегирования клиентом своих полномочий серверу для выполнения запроса;
- упрощение администрирования распределенной КС.

Основными недостатками протокола являются:

- отсутствие выделенного канала связи между объектами распределенной КС (наличие широковещательной среды передачи данных, например среды Ethernet), что позволяет нарушителю анализировать сетевой трафик в подобных системах;
- возможность взаимодействия объектов распределенной КС без установления виртуального канала между ними, что не позволяет надежно идентифи-

цировать объект или субъект распределенной КС и организовать защиту передаваемой информации;

• использование недостаточно надежных протоколов идентификации объектов распределенной КС перед установлением виртуального канала между ними, что позволяет нарушителю при перехвате передаваемых сообщений выдать себя за одну из сторон соединения;

• отсутствие контроля создания и использования виртуальных каналов между объектами распределенной КС, что позволяет нарушителю добиться реализации угрозы отказа в обслуживании в КС (любой объект распределенной КС может анонимно послать любое число сообщений от имени других объектов КС);

• отсутствие возможности контроля маршрута получаемых сообщений, что не позволяет подтвердить адрес отправителя данных и определить инициатора удаленной атаки на КС;

• отсутствие полной информации об объектах КС, с которыми требуется создать соединение, что приводит к необходимости отправки широковещательного запроса или подключения к поисковому серверу (нарушитель при этом имеет возможность внедрить ложный объект в распределенную КС и выдать один из ее объектов за другой);

• отсутствие шифрования передаваемых сообщений, что позволяет нарушителю получить несанкционированный доступ к информации в распределенной компьютерной сети [5].

Среди *программно-аппаратных* и *программных средств обеспечения аутентичности* распределенных КС можно выделить межсетевые экраны (МСЭ), средства анализа защищенности и средства обнаружения атак.

Межсетевые экраны (брандмауэры, firewall) реализуют набор правил, которые определяют условия прохождения пакетов данных из одной части распределенной КС (открытой) в другую (защищенную). В зависимости от уровня взаимодействия объектов сети основными разновидностями МСЭ являются фильтрующие *маршрутизаторы, шлюзы сеансового и прикладного уровней*. Основной функцией фильтрующих маршрутизаторов, работающих на сетевом уровне эталонной модели, является фильтрация пакетов данных, входящих в защищенную часть сети или исходящих из нее. Правила фильтрации определяют, разрешается или блокируется прохождение через МСЭ пакета с задаваемыми этими правилами параметрами.

К основным достоинствам фильтрующих маршрутизаторов относятся простота их создания, установки и конфигурирования; прозрачность для приложений пользователей КС и минимальное влияние на их производительность; невысокая стоимость. Недостатками фильтрующих маршрутизаторов являются:

• отсутствие аутентификации на уровне пользователей КС;

• уязвимость для подмены IP-адреса в заголовке пакета;

• незащищенность от угроз нарушения конфиденциальности и целостности передаваемой информации;

• сильная зависимость эффективности набора правил фильтрации от уровня знаний администратора МСЭ конкретных протоколов;

• открытость IP-адресов компьютеров защищенной части сети.

Шлюзы сеансового уровня предназначены для контроля виртуального соединения между рабочей станцией защищенной части сети и хостом ее незащищенной части, и трансляции IP-адресов компьютеров защищенной части сети.

В процессе выполняемой шлюзом сеансового уровня процедуры трансляции IP-адресов происходит их преобразование в один IP-адрес, ассоциированный с МСЭ. Это исключает прямое взаимодействие между хостами защищенной и открытой сетей и не позволяет нарушителю осуществлять атаку путем подмены IP-адресов.

К достоинствам шлюзов сеансового уровня относятся их простота и надежность программной реализации. Недостатком является отсутствие возможности проверять содержимое передаваемой информации. Это позволяет нарушителю пытаться передать пакеты с вредоносным программным кодом и обратиться затем напрямую к одному из серверов атакуемой КС.

Шлюзы прикладного уровня не только исключают прямое взаимодействие между уполномоченным пользователем из защищенной части сети и хостом из ее открытой части, но и фильтруют все входящие и исходящие пакеты данных на прикладном уровне (на основе анализа содержания передаваемых данных).

Основные функции шлюзов прикладного уровня:

• идентификация и аутентификация пользователя КС при попытке установить соединение;

• проверка целостности передаваемых данных;

• разграничение доступа к ресурсам защищенной и открытой частей распределенной КС;

• фильтрация и преобразование передаваемых сообщений (обнаружение вредоносного программного кода, шифрование и расшифрование и т.п.);

• регистрация событий в специальном журнале;

• кеширование запрашиваемых извне данных, размещенных на компьютерах внутренней сети (для повышения производительности КС).

Достоинствами шлюзов прикладного уровня также являются:

• скрытость структуры защищенной части сети для

остальных хостов;
• надежная аутентификация и регистрация проходящих сообщений;
• более простые правила фильтрации пакетов на сетевом уровне, в соответствии с которыми маршрутизатор должен пропускать только трафик, предназначенный для шлюза прикладного уровня, и блокировать весь остальной трафик;
• возможность реализации дополнительных проверок.

Основными недостатками шлюзов прикладного уровня являются более высокая стоимость, сложность разработки, установки и конфигурирования, снижение производительности КС, "непрозрачность" для приложений пользователей КС.

Межсетевые экраны являются основой для создания виртуальных частных сетей (Virtual Private Network, VPN), которые предназначены для скрытия топологии внутренних сетей организаций, обменивающихся информацией по сети Интернет, и защиты трафика между ними. При этом используются специальные системы маршрутизации.

Общим недостатком МСЭ любого вида является то, что эти программно-аппаратные средства защиты в принципе не могут предотвратить многих видов атак (например, угрозы несанкционированного доступа к информации с использованием ложного сервера службы доменных имен сети Интернет, угрозы анализа сетевого трафика, угрозы отказа в обслуживании). Нарушителю реализовать угрозу доступности информации в КС, использующей МСЭ, может оказаться даже проще, так как достаточно атаковать только хост с МСЭ для фактического отключения от внешней сети всех компьютеров защищенной части сети.

Для обеспечения конфиденциальности и сервиса аутентификации на прикладном уровне в компьютерных системах и сетях используются *схемы PGP* (Pretty Good Privacy) и *S/MIME* (Secure/Multipurpose Internet Mail Extension).

В пакет системы PGP включены алгоритмы шифрования с открытым ключом RSA, DSS и алгоритм Диффи-Хеллмана, алгоритмы симметричного шифрования IDEA и 3DES, а также алгоритм SHA-1. Комбинация SHA-1 и RSA обеспечивает эффективную схему цифровой подписи, алгоритм CAST-128 (IDEA или 3DES) обеспечивает конфиденциальность, для обмена ключами используется алгоритм Эль-Гамаля. Все это позволяет сократить время передачи ключевых данных и решить проблему передачи сеансовых ключей путем присоединения сеансового ключа к сообщению.

Система *S/MIME* является усовершенствованным стандартом защиты формата MIME электронной почты. Она обеспечивает упаковку данных и цифровую подпись, формируемую с помощью шифрования профиля сообщения, с использованием личного ключа отправителя. При этом алгоритм SHA-1 обеспечивает цифровую подпись, конфиденциальность обеспечивается алгоритмами симметричного шифрования 3DES и RC2/40, для обмена ключами используется алгоритм Диффи-Хеллмана.

Рассмотрим механизмы защиты с помощью *протокола IP* (Internet Protocol – протокол межсетевого взаимодействия), обеспечивающего аутентификацию, конфиденциальность и управление ключами.

Для обеспечения защиты обмена данными в локальных сетях (LAN), корпоративных и открытых глобальных сетях (WAN) и в Internet используется *протокол IPSec*.

Ключевым объектом в механизмах аутентификации и конфиденциальности для IP является *защищенная связь* (Security Association), обеспечивающая одностороннюю защиту потока данных на транспортном уровне и использующая при этом либо протокол *AH* (Authentication Header – заголовок аутентификации), либо *ESP* (Encapsulating Security Payload header – заголовок защиты полезного груза). Аутентификация в протоколах AH и ESP опирается на использование кода аутентичности MAC с длинной по умолчанию 96 битов (схемы HMAC-MD5-96 и HMAC-SHA-1-96), а сервис шифрования полей полезного груза протокола ESP использует алгоритмы шифрования: "тройной" DES с тремя ключами, RC5, IDEA, "тройной" IDEA с тремя ключами, CAST, Blowfish.

Протоколы AH и ESP поддерживают два режима использования: транспортный и туннельный.

Транспортный режим предназначен для защиты протоколов высшего уровня и обеспечивает сквозную связь двух главных узлов (пользователя и сервера или двух рабочих станций). Преимуществом транспортного режима является обеспечение конфиденциальности для любого применяющего этот режим приложения, что позволяет избежать необходимости реализации функций обеспечения конфиденциальности в каждом отдельном приложении. Недостатком является то, что при его использовании не исключается возможность анализа трафика пересылаемых пакетов.

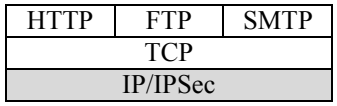
Туннельный режим обеспечивает защиту всего пакета IP и оказывается полезным в конфигурации сети, которая предполагает наличие брандмауэра или шлюза защиты. Преимуществом режима является разгрузка узлов внутренней сети от необходимости шифрования данных и упрощение процедуры распределения ключей. Недостатком является усложнение анализа потока данных к конкретному адресату.

Для обеспечения защиты данных на прикладном уровне в приложении *World Wide Web* существует несколько подходов. Все они схожи, но разли-

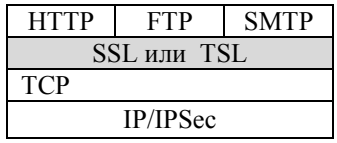
чаются по областям применения и размещению соответствующих средств защиты в стеке протоколов PSP/IP. Эти различия представлены на рис. 4. Первый метод защиты состоит в использовании протокола защиты IP (IPSec) (рис. 4, а). Преимущество IPSec заключается в его прозрачности для конечного пользователя (приложений) и в использовании фильтрации, позволяющей его использование только для той части потока данных, где это действительно необходимо.

Вторым методом защиты является размещение средств безопасности сразу над протоколом TCP (рис. 4, б). Примером такого подхода является стандарт SSL (Secure Socket Layer) и его более новая версия – TLS (Transport Layer Security) безопасной передачи данных в Internet. Внедрение средств SSL и TLS в набор соответствующих протоколов обеспечивает прозрачность средств защиты приложений.

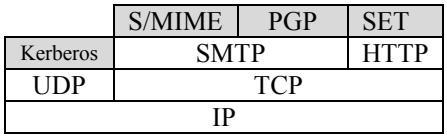
Различные средства защиты могут выстраиваться и в приложениях (рис. 4, в). Преимуществом такого метода является возможность оптимальной настройки средств защиты в зависимости от требований конкретного приложения.



а – сетевой уровень



б – транспортный уровень



в – уровень приложения

Рис. 4. Размещение средств защиты в стеке протоколов TCP/IP

Таким образом, для обеспечения аутентификации данных в протоколах могут применяться различные алгоритмы симметричного и несимметричного шифрования, MAC-коды и функции хеширования. Вместе с тем, для каждой отдельной компьютерной системы (сети) необходимо проведение оптимизации средств аутентификации в зависимости от требований конкретных приложений, использующихся в данных КС (сетях).

Целостность призвана обеспечить возможность модификации хранящейся и передаваемой в КС информации только пользователями, имеющими на это право. При этом под модификацией понимаются операции записи, изменения, изменения состояния, удаления, создания, задержки или повторные воспроизведения передаваемых данных [4 – 5].

Для обеспечения целостности данных используются алгоритмы шифрования и коды аутентификации. Протоколы защиты данных в *World Wide Web* обеспечивают также и целостность передаваемых данных на прикладном, сетевом и транспортных уровнях.

Протокол SSL предназначен для обеспечения защиты сквозной передачи данных с использованием протокола TCP. Строго говоря, SSL представляет собой не один протокол, а два уровня протоколов, как показано на рис. 5.

Рис. 5. Стек протоколов SSL

Протокол SSL предлагает базовый набор средств защиты, применяемых протоколами более высоких уровней, и обеспечивает конфиденциальность канала коммуникаций и аутентификацию пользователя.

Протокол квитирования определяет общий для пользователя и сервера секретный ключ, используемый симметричным алгоритмом шифрования, и обеспечивает конфиденциальность передаваемых данных. Кроме этого, протокол квитирования определяет общий секретный ключ для вычисления значений MAC, который обеспечивает целостность передаваемых сообщений.

Преимуществом SSL является его независимость от прикладного протокола. Протоколы приложения, такие как HTTP, FTP, TELNET и т.д. могут работать поверх протокола SSL совершенно прозрачно. Протокол SSL может согласовывать алгоритм шифрования и ключ сессии, а также аутентифицировать сервер до того, как приложение примет или передаст первый байт данных. Все протокольные прикладные данные передаются зашифрованными с гарантией конфиденциальности.

Протокол TLS предназначен для обеспечения конфиденциальности и целостности данных. Он имеет два уровня: протокол записей TLS и протокол диалога TLS. Протокол записей TLS обеспечивает конфиденциальность данных с использованием симметричных алгоритмов шифрования DES, RC4 и целостность данных с использованием хэш-функций SHA-1 или MD5. Протокол диалога TLS обеспечивает цифровую подпись, основанную на подходе RSA или DSS.

Таким образом, средства защиты целостности сообщений гарантировано обеспечивают, что при-

нятые сообщения будут в точности соответствовать отправленным, без изъятий, дополнений, изменений, в исходном порядке и без повторений. Вместе с тем, протоколы защиты целостности, работая с потоками сообщений, обеспечивают только обнаружение нарушения целостности потока данных и не обеспечивают восстановление поврежденной или утраченной информации.

Конфиденциальность призвана обеспечить защиту передаваемых данных от пассивных атак. В самой широкой форме служба защиты должна обеспечить защиту всех данных, передаваемых между любыми двумя пользователями в течение определенного времени. При этом обеспечивается общая защита, препятствующая утечке любых пользовательских данных при передаче. В более узкой форме служба защиты может обеспечивать защиту отдельных сообщений или даже отдельных частей сообщений. Другим аспектом конфиденциальности является защита потока данных от возможности его аналитического исследования (защита факта, места и способа передаваемых данных). Наиболее общим подходом к обеспечению безопасности в точках уязвимости компьютерных сетей (КС) является использование шифрования.

При передаче данных в КС с коммутацией пакетов, как правило, используется либо канальное шифрование, либо сквозное шифрование, основанные на симметричных кодах (алгоритмы CAST-128, IDEA или 3DES). На рис. 6 представлены основные возможности шифрования в сети с коммутацией пакетов.

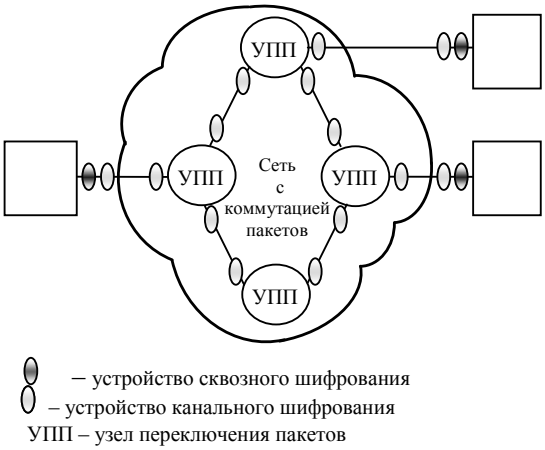


Рис. 6. Шифрование в сети с коммутацией пакетов

Для противодействия нарушениям защиты используется канальное и сквозное шифрование. Применительно к модели ВОС это означает, что канальное шифрование осуществляется либо на физическом, либо на уровне звена передачи (канальном уровне), сквозное шифрование используется на сетевом или транспортном уровне.

При использовании канального шифрования каждый уязвимый канал оборудуется на обоих концах устройствами шифрования. Недостатками *канального шифрования* являются необходимость дешифрования пакета данных при каждом его прохождении через пакетный переключатель, при этом сообщение становится уязвимым в каждом переключателе, необходимость использования множества устройств шифрования со своими уникальными ключами для каждой пары шифраторов.

Сквозное шифрование обеспечивает сквозную безопасность передачи данных в рамках любой отдельно рассматриваемой сети. При этом процесс шифрования выполняется только в двух конечных системах. Существенным недостатком является отсутствие шифрования всего потока данных, поскольку заголовки пакетов передаются в открытом виде (протокол X.25 или TCP). Кроме того, такое шифрование не может обеспечить необходимую безопасность для межсетевого обмена данными, при использовании электронной почты, электронного обмена данными или при передаче файлов. Для приложений типа электронной почты сквозное шифрование используется на прикладном уровне. Недостатком шифрования на уровне приложений является создание и распределение огромного количества секретных ключей. Для лучшей защиты требуется как канальное, так и сквозное шифрование [4 – 5], что позволит обеспечить конфиденциальность передаваемого пакета данных. Однако в момент времени, когда пакет находится в памяти свитча, заголовок пакета является открытым. На рис. 7 показан вариант схемы межсетевого обмена данными.

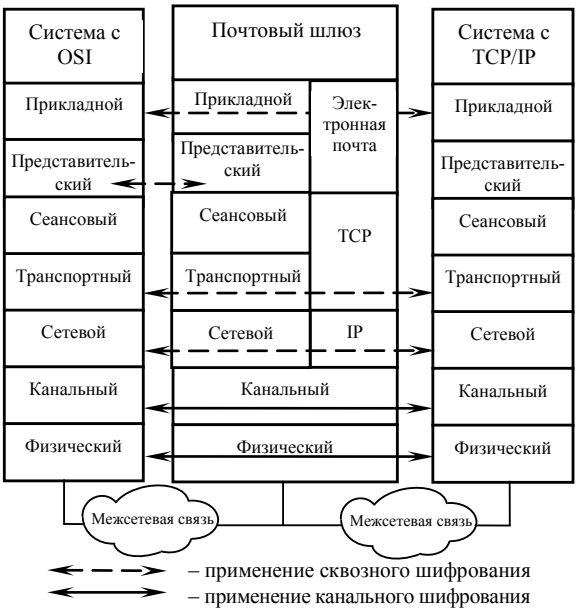


Рис. 7. Пределы применимости различных схем шифрования при межсетевом обмене данных

Таким образом, механизмы и протоколы конфиденциальности обеспечивают защиту передаваемых сообщений в полном объеме, отдельных сообщений или даже отдельных частей сообщений. Вме-

сте с тем, при прохождении пакетов через узлы коммутации информация становится уязвимой для нарушителя.

Проведенный анализ протоколов и механизмов защиты показал, что для обеспечения аутентификации, целостности и конфиденциальности передачи данных в компьютерных сетях используются криптографические методы, основанные на использовании симметричных и несимметричных алгоритмов преобразования информации. Вместе с тем, дальнейшее усиление угроз указывает на необходимость интегрированного подхода для обеспечения защиты передаваемой информации.

Для построения механизмов защиты традиционно используют криптографические методы. Их общая классификация представлена на рис. 8. Методы симметричной криптографии основаны на простых и легко реализующихся блоках подстановок и перестановок. Методы криптографии с открытым ключом основаны на использовании соответствующей теоретико-сложностной задачи (факторизации, дискретного логарифмирования и т.д.).

Рис. 8. Криптографические методы защиты информации

Среди известных примеров несимметричных криптосистем особое место занимают несимметричные секретные системы доказуемой стойкости (теоретико-кодовые схемы) на алгебраических блоковых кодах, имеющие существенное преимущество – высокую скорость криптографического преобразования информации [8 – 9].

Кроме того, как показано в работах [8 – 11], применение теоретико-кодовых схем позволяет совместить помехоустойчивое кодирование с маскировкой данных под случайную последовательность и, таким образом, интегрировано (одним приемом) обеспечить конфиденциальность и аутентификацию передаваемых данных.

Выводы

Таким образом, проведенные исследования показали, что для обеспечения защиты передаваемых данных в компьютерных сетях используются наборы протоколов защиты, которые не в полной мере обеспечивают конфиденциальность, аутентификацию и целостность данных.

Перспективным направлением интегрированного решения задач обеспечения требуемых показателей является использование в протоколах и механизмах защиты теоретико-кодовых схем на алгебраических блоковых кодах.

Список литературы

1. Горбенко И.Д., Потий А.В., Терещенко П.И. Рекомендации международных стандартов по оценке безопасности информационных технологий // Мат-лы третьей международн. научно-практич. конф. "Безопасность информации в информационно-телекоммуникационных системах" – К., 2000.-С. 150-160.

2. Бондаренко М.Ф., Черных С.П., Горбенко И.Д., Замула А.А., Ткач А.А. Методологические основы концепции и политики безопасности информационных технологий // Радиотехника. – 2001. – Вып.119. – С. 5-17.

3. Горбенко И.Д., Потий А.В., Терещенко П.И. Критерии и методология оценки безопасности информационных технологий // Радиотехника.

4. Вильям Столингс. Криптография и защита сетей. Принципы и практика. – М.: Изд. Дом "Вильямс" С-П.К, 2001. – 670 с.

5. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2005. – 256 с.

6. Стасєв Ю.В., Кузнецов О.О., Корольов Р.В. Аналіз існуючих послуг і механізмів захисту інформації // Системи озброєння і військова техніка. – Х.: ХУ ПС. – 2006.– 4(8) – С. 81-87.

7. Garfinkel,S., and Spafford, G. Web Security & Commerce. Camridge, MA: CTReilly fnd Associates, 1997.

8. Сидельников В.М. Криптография и теория кодирования. Мат-лы конф. «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с.

9. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // Дискретная математика. – 1992. – Т.4, №3. – С. 57-63.

10. Халимов Г.З., Северинов А.В. Обеспечение безопасности каналов передачи данных на основе помехоустойчивых кодов // Системы управления и связь. – Х.: ХВУ. – 1996. – С.116-119.

11. Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 5. – С. 127-132.

Поступила в редколлегию 14.03.2007

Рецензент: д-р техн. наук проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.