МЕХАНИЗМЫ И ПРОТОКОЛЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ И СИСТЕМАХ

Евсеев *Сергей* Петрович,
Дорохов *Александр* Васильевич,
Король *Ольга* Григорьевна,
Харьковский национальный экономический университет, кафедра информационных систем,
Харьков, Украина

ОБЛАСТ: Компьютерные науки, Криптография

Краткое содержание:

Исследуются протоколы защиты информации в компьютерных сетях и системах. Классифицируются основные типы угроз нарушения защиты, возникающие при использовании компьютерных сетей. Рассматриваются основные механизмы, услуги и варианты реализации криптосистем для обеспечения аутентификации, целостности и конфиденциальности передаваемой информации. Описываются их преимущества и недостатки. Определяются и анализируются перспективные направления развития криптографических преобразований для обеспечения защиты информации в компьютерных сетях и системах.

Ключевые слова: *защита информации, криптографические преобразования, конфиденциальность, аутентификация, целостность данных, алгоритмы шифрования.*

Введение

Создание современных военных компьютерных систем, появление глобальных информационно-телекоммуникационных сетей радикально изменило характер и диапазон проблем защиты информации. 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 ком-

aleks.dorokhov@meta.ua

пьютерных системах и сетях, анализ перспективных направлений развития криптографических преобразований для обеспечения конфиденциальности, аутентификации и целостности информации.

Проблемы и механизмы защиты компьютерных сетей от угроз и последствий несанкционированного доступа

Вопросы защиты компьютерных систем и коммуникационных сетей от несанкционированного доступа в последнее время приобрели особую остроту. Развитие компьютерных 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.

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 в табл. 2 [1, 2, 6].

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

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

Таблица 1

Характеристики угроз нарушения защиты данных

Table 1

Characteristics of threats of infringement of data protection

Показатели	Угрозы	Последствия
Аутентификация	Попытки нарушителя выдать себя за легального пользователя. Фальсификация данных.	Неправильное представление пользователей. Доверие к ложным данным.
Целостность	Изменение пользовательских данных. Внедрение “троянских коней”. Изменение информации в памяти. Изменение потока сообщений на пути передачи	Потеря информации Компрометация системы. Уязвимость от угроз нарушений защиты 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 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.

Таблица 2

Распределение услуг и механизмы безопасности по уровням эталонной модели

Table 2

Distribution of services and mechanisms of safety on levels of etalon model

№	Услуги	Механизмы
1	Аутентификация объекта (шифрование, цифровая подпись)	Физический № 4
2	Аутентификация источника данных (шифр., цифр. подпись)	
3	Управление доступом	Канальный №№ 4, 5
4	Конфиденциальность соединения (шифр., управление маршрутизацией)	
5	Конфиденциальность без установления соединения (шифр.)	Сеансовый
6	Конфиденциальность выделенного поля данных (шифр.)	Представительский
7	Конфиденциальность трафика (шифр., заполнение трафика, управление маршрутизацией)	Прикладной №№ 1 - 13
8	Целостность соединения с восстановлением (шифр., целостность данных)	
9	Целостность соединения без восстановления (шифр., целостность данных)	
10	Целостность выделенного поля в режиме с установлением соединения или без (шифр., целостность данных	Сетевой №№ 2, 3, 4, 11
11	Целостность блока данных без соединения, их шифрование	
12	Участие в посылке сообщений, шифрование, целостность данных, нотаризация	Транспортный №№ 1, 3, 4, 5, 8, 9, 11
13	Подтверждение получения сообщений, нотаризация	

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

На рис. 1-3 представлены три варианта защиты сообщений с использованием несимметричного шифрования. Первый вариант, передача сообщений с открытым ключом абонента В (KU_B), представлен на рис. 1. При этом обеспечивается конфиденциаль-ность сообщения (только абонент В имеет закрытый ключ KR_B), однако недостатком схемы является невозможность обеспечить аутентификацию (любой абонент может воспользоваться открытым ключом KU_B, чтобы объявить себя абонентом А).

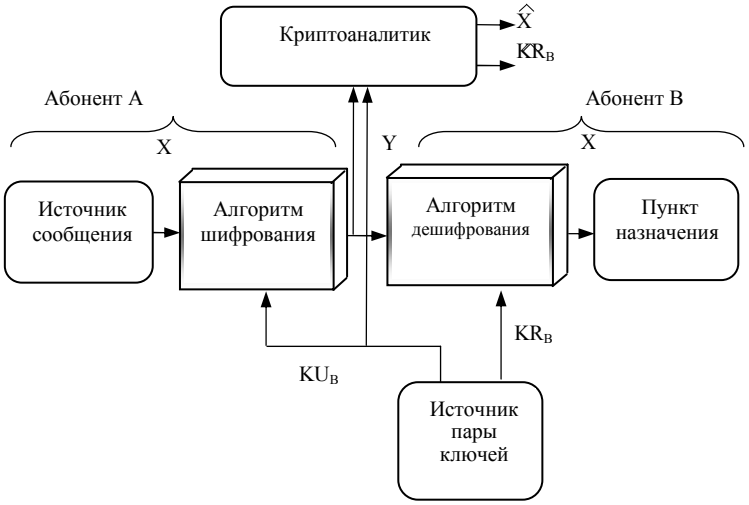

Рисунок 1 – криптосистема с открытым ключом: конфиденциальность
Figure 1 – cryptosystem with the open key: confidentiality

Второй вариант – использование абонентом А при отправке сообщения своего секретного ключа (KR_A) – представлен на рис. 2.

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. 3.

При этом обеспечивается конфиденциальность, цифровая подпись (поскольку используется открытый ключ KU_B) и аутентификация (поскольку используется закрытый ключ KR_A)

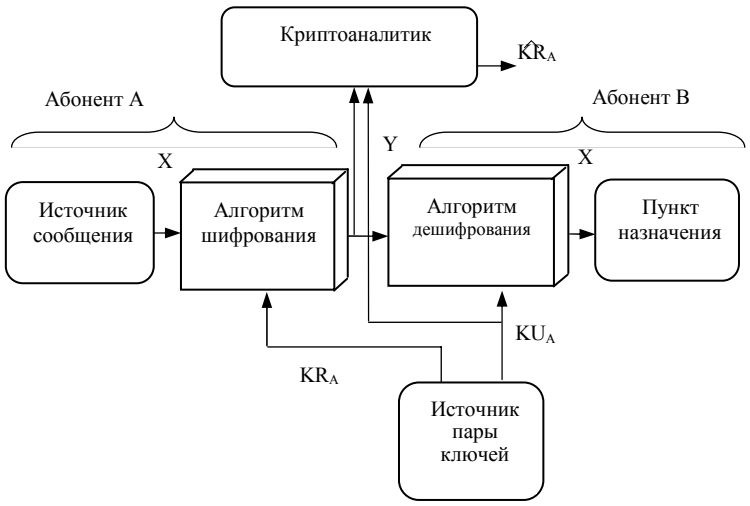

Рисунок 2 – криптосистема с открытым ключом: аутентификация
Figure 2 – cryptosystem with the open key: authentication

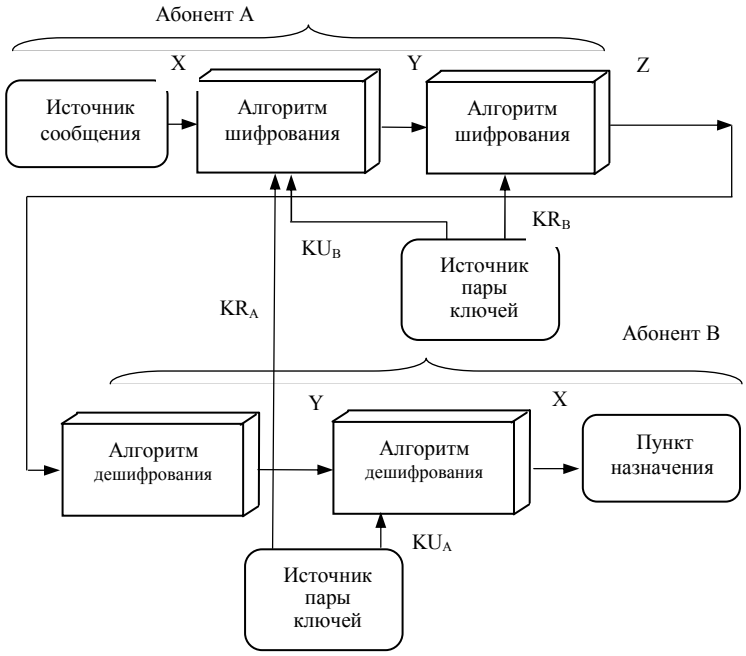

Рисунок 3 – криптосистема с открытым ключом:
конфиденциальность и аутентификация
Figure 3 – cryptosystem with the open key: confidentiality and authentication

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 (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 нем гарантируется аутентификация поступающих SNMP-сообщений, в то же 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. Далее рассмотрим способы защиты сообщений при использовании хэш-кода, представленные на рис. 4-9.

Так, на рис. 4 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).

В случае рис. 5 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).

На рис. 6 шифруется только хэш-код средствами шифрования с открытым ключом с использованием личного ключа отправителя. При этом обеспечивается не только аутентификация, но и цифровая подпись, т.к. 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.

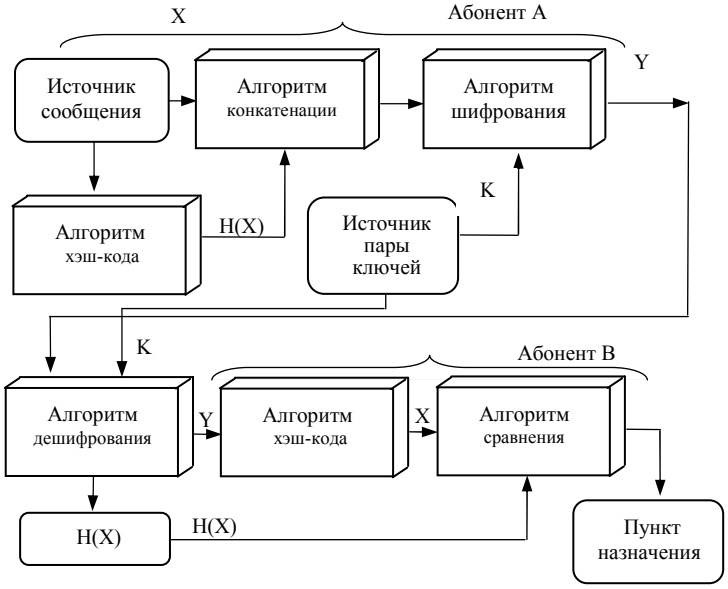

Рисунок 4 – схема использования хэш-кода: конфиденциальность и аутентификация
Figure 4 – scheme of hash-code usage: confidentiality and authentication

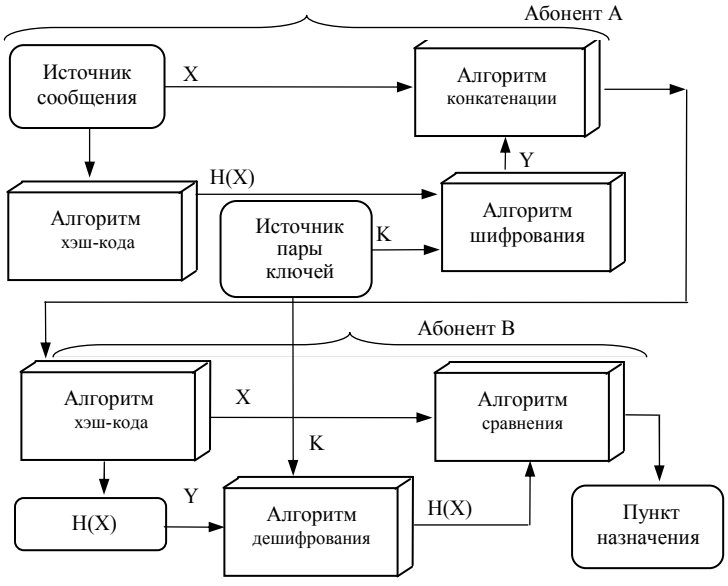

Рисунок 5 – схема использования хэш-кода: аутентификация
Figure 5 – scheme of hash-code usage: authentication

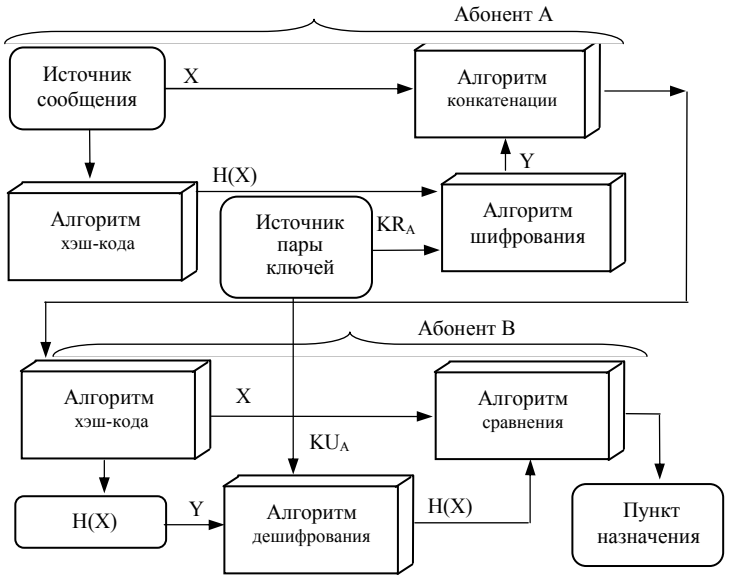

Рисунок 6 – схема использования хэш-кода: аутентификация и цифровая подпись
Figure 6 – scheme of hash-code usage: authentication and digital signature

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, то есть только стороны А и В знают К (рис. 7).

В целях аутентификации сообщений можно использовать функцию хэширования без шифрования (рис. 8). 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)

Конфиденциальность может быть обеспечена при некоторой модификации подхода описанного выше, если зашифровать сообщение вместе с добавленным к нему хэш-кодом (рис. 9).

Способность функции хэширования позволяет противостоять атакам с перебором всех вариантов, т.к. зависит исключительно от длины хэш-кода.

Одними из перспективных алгоритмов хэш-функций являются SHA-1 и RIPEMD-160. Основные их характеристики представлены в табл. 3 в сравнении алгоритмом хэш-функции MD-5.

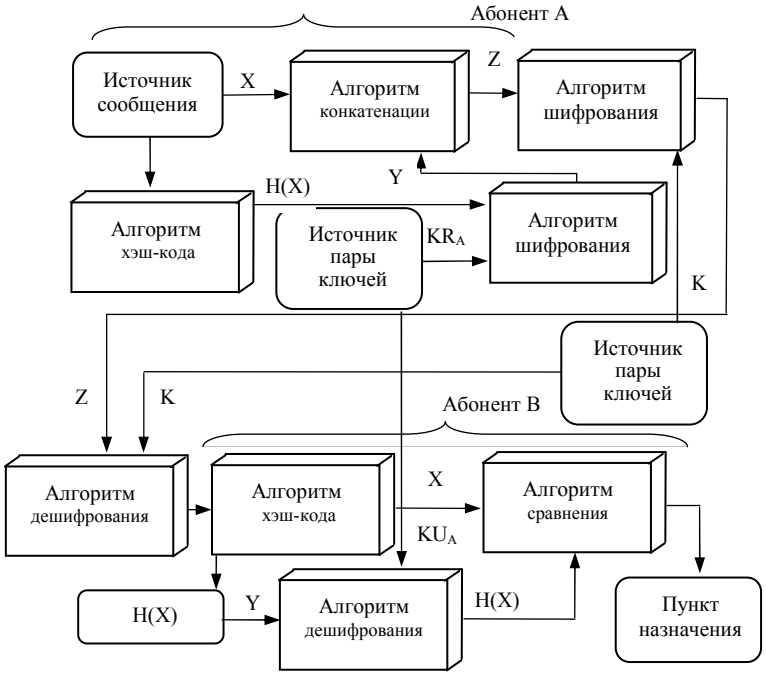

Рисунок 7 – схема использования хэш-кода: конфиденциальность, аутентификация и цифровая подпись
Figure 7 – scheme of hash-code usage: confidentiality, authentication, digital signature

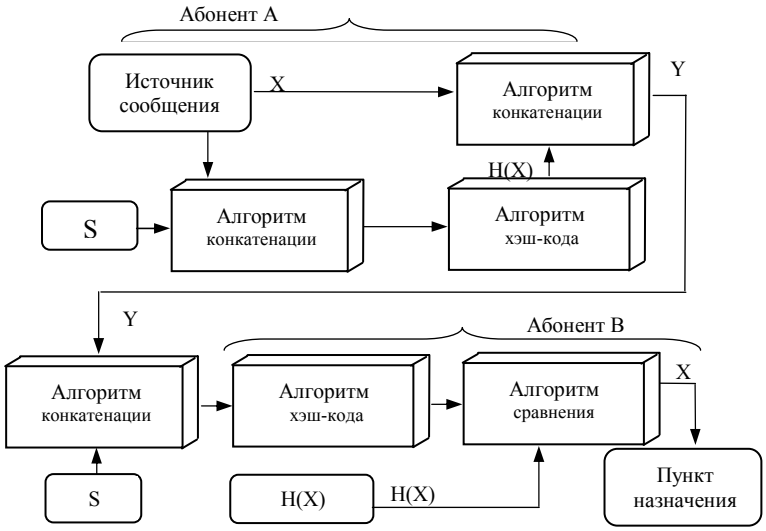

Рисунок 8 – схема использования хэш-кода: конфиденциальность
Figure 8 – scheme of hash-code usage: confidentiality

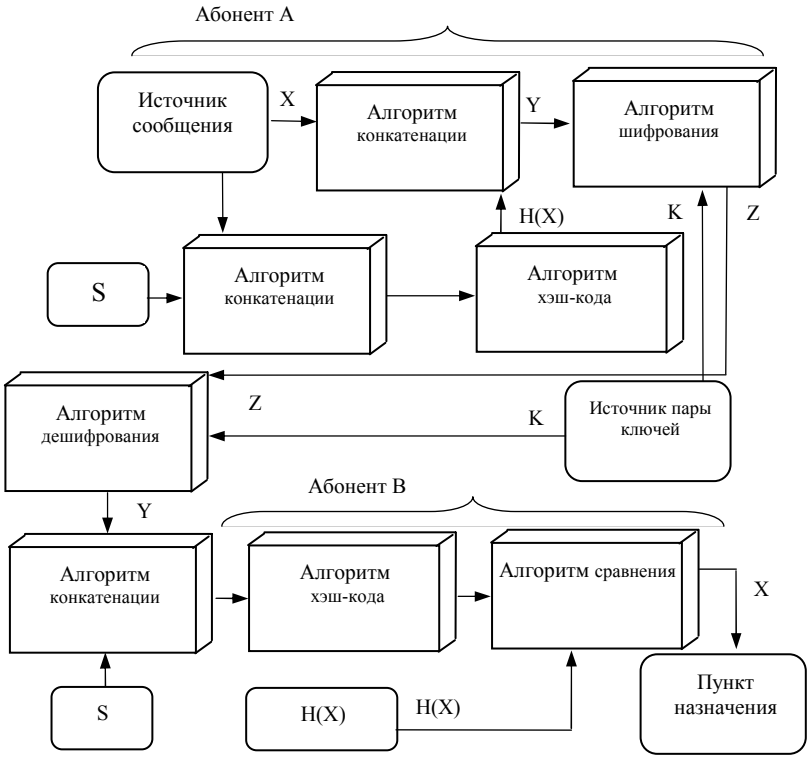

Рисунок 9 – схема использования хэш-кода: аутентификация
Figure 9 – scheme of hash-code usage: authentication

Таблица 3

Основные характеристики алгоритмов хэш-функций

Table 3

The basic characteristics of algorithms of hash-functions

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
Max. 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. Он 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 идентифицировать 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 внедрения ложного объекта 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].

Программные и аппаратные средства обеспечения аутентичности распределенных компьютерных сетей

Среди указанных средств следует выделить межсетевые экраны (МСЭ), средства анализа защищенности и 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 их основным достоинствам относятся простота создания, установки, конфигурирования; прозрачность для приложений пользователей, минимальное влияние на производительность; невысокая стоимость.

Недостатками же 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. При выполнении 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 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;

– кэширование запрашиваемых извне данных, размещенных на компьютерах внутренней сети (повышает производительности КС).

Достоинствами шлюзов прикладного уровня 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 сетей (Virtual Private Network, VPN), предназначеных для скрытия топологии внутренних сетей организаций, обменивающихся информацией по сети Интернет, 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 обеспечивают эффективную схему цифровой подписи, алгоритм CAST-128 (IDEA или 3DES) обеспечивают 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), обеспечивающие 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 использовании 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 различаются по областям применения и размещению соответствующих средств защиты в стеке протоколов PSP/IP. Эти различия представлены на рис. 10.

Первый метод защиты состоит в использовании протокола защиты IP (IPSec). 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.

Рисунок 10 – размещение средств защиты в стеке протоколов TCP/IP
Figure 10 – accommodation of means of protection in a stack of protocols TCP/IP

Вторым методом защиты является размещение средств безопасности сразу над протоколом TCP. 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. Преимуществом такого метода является возможность оптимальной настройки средств защиты в зависимости от требований конкретного приложения.

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. 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. На первом уровне находятся протоколы квитирования SSL, изменения параметров шифрования SSL, извещения SSL, HTTP. На последующих уровнях - протокол записи SSL, затем CP и далее IP.

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 принятые 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 их частей.

Другим аспектом конфиденциальности является защита потока данных от возможности его аналитического исследования (защита факта, места, способа передачи данных). Общим подходом к обеспечению безопасности в точках уязвимости является шифрование. 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. 11 представлены основные возможности шифрования в сети с коммутацией пакетов.

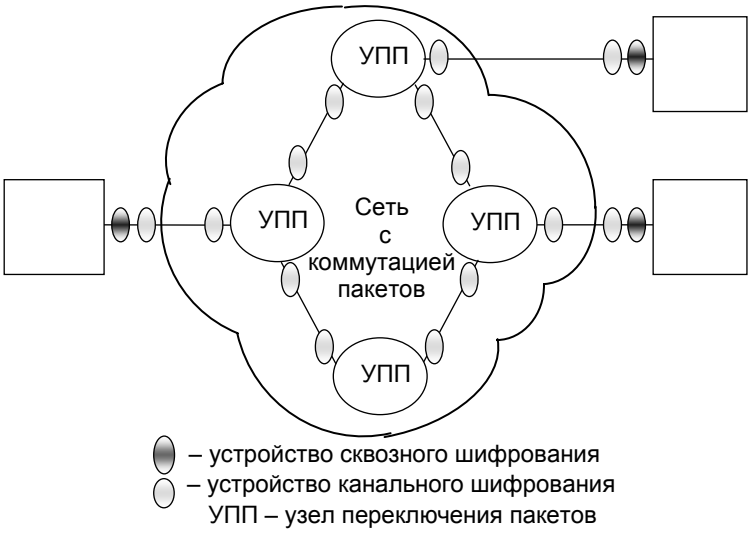

Рисунок 11 – шифрование в сети с коммутацией пакетов
Figure 11 – enciphering in a network with switching packages

Для противодействия нарушениям защиты используется канальное и сквозное шифрование. 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, сообщение становится уязвимым в каждом переключателе, требуется много устройств шифрования со своими уникальными ключами для каждой пары шифраторов.

Сквозное шифрование обеспечивает безопасность передачи данных в рамках отдельной сети. Сам процесс шифрования выполняется только в двух конечных системах. Недостатком является отсутствие шифрования всего потока данных, поскольку заголовки пакетов передаются в открытом виде (протокол X.25 или TCP). Такое шифрование не обеспечивает безопасность межсетевого обмена данными электронной почты, при электронной передаче файлов. Для электронной почты сквозное шифрование используется на прикладном уровне. Недостатком шифрования на уровне приложений является работа с большим количеством секретных ключей. Для лучшей защиты необходимо как канальное, так и сквозное шифрование, что обеспечивает конфиденциальность передаваемых данных.

Однако в момент времени, когда пакет находится в памяти свитча, заголовок пакета является открытым. На рис. 12 показана такая схема межсетевого обмена данными.

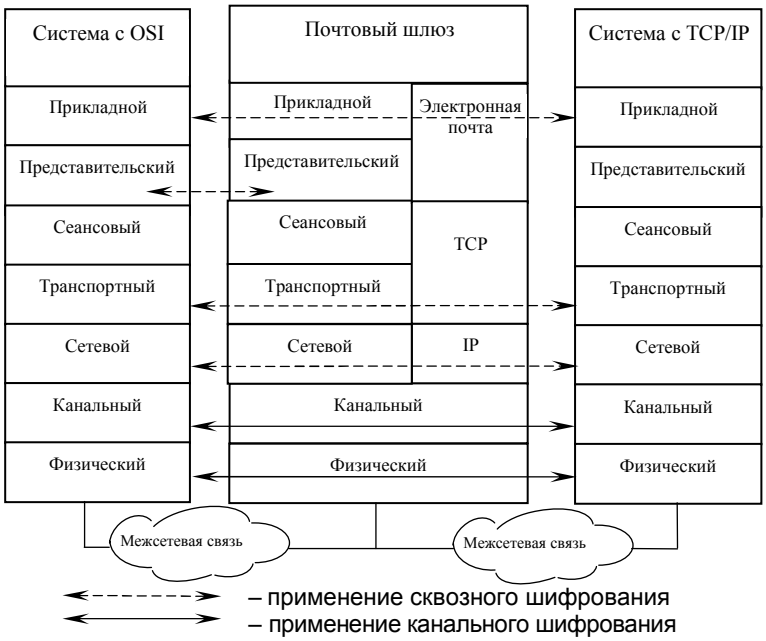

Рисунок 12 – применимость схем шифрования при межсетевом обмене данных
Figure 12 – applicability of schemes of enciphering at gateway data exchange

Таким образом, механизмы и протоколы конфиденциальности обеспечивают защиту передаваемых сообщений в полном объеме, отдельных сообщений или даже отдельных частей сообщений. Вместе с тем, при прохождении пакетов через узлы коммутации информация становится уязвимой для нарушителя.

Анализ протоколов и механизмов защиты показал, что для обеспечения аутентификации, целостности и конфиденциальности передачи данных в компьютерных сетях используются криптографические методы, основанные на симметричных и несимметричных алгоритмах преобразования информации.

Для построения механизмов защиты традиционно используют криптографические методы. Их общая классификация представлена на рис. 13. 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.).

Рисунок 13 – криптографические методы защиты информации
Figure 13 – cryptographic methods of protection of the information

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.

Заключение

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.

Литература

[1] Горбенко И. Д., Потий А. В., *Рекомендации международных стандартов по оценке безопасности информационных технологий, Матер. междунар. научно-практич. конфер. «Безопасность информации в информационно-телекоммуникационных системах»,* Киев, 2010.

[2] Бондаренко М. Ф., Черных С. П., Горбенко И. Д., *Методологические основы концепции и политики безопасности информационных технологий, Радиотехника. Всеукраинский научн.-техн.сб.*- Киев, 2010

[3] Хорев П. Б., *Методы и средства защиты информации в компьютерных системах, «*Академия», Москва,2005.

[4] Стасєв Ю. В., Кузнецов О. О., Корольов Р. В. *Аналіз існуючих послуг і механізмів захисту інформації, Системи озброєння і військова техніка, ХУПС,* Харьков, 2006.

[5] Кузнецов А. А., Евсеев С. П. *Разработка теоретико-кодовых схем с использованием эллиптических кодов, Системи обробки інформації, ХВУ,* Харків, 2004.

MEHANIZMI ZAŠTITE INFORMACIJA U KOMPJUTERSKIM MREŽAMA I SISTEMIMA

OBLAST: računarske nauke, kriptografija

Rezime:

U radu su dati protokoli za zaštitu informacija u kompjuterskim mrežama i sistemima kao i klasifikacija osnovnih tipova ugrožavanja zaštite do kojih dolazi prilikom korišćenja kompjuterskih mreža. Ispitani su osnovni mehanizmi, usluge i vrste realizacije kriptosistema za održavanje autentikacije, integriteta i tajnosti. Opisane su njihove prednosti i nedostaci. Definisani su i analizirani pravci razvoja kriptografskih transformacija za održavanje zaštite informacija u kompjuterskim mrežama i sistemima.

Uvod

Moderni vojni kompjuterski sistemi kao i postojanje globalnih telekomunikacionih mreža značajno su izmenili karakter i obim problema pri zaštiti informacija. Metode zaštite informacija postale su složene i predstavljaju važan deo informacionih tehnologija. U zaštiti informacija primenjuju se različita kriptogtafska sredstva.

Analizirani su protokoli i mehanizmi zaštite informacija u kompjuterskim sistemima i mrežama, kao i mogući pravci razvoja kriptografskih transformacija za održavanje tajnosti, autentikacije i integriteta informacija.

Problemi i mehanizmi zaštite kompjuterskih mreža od pretnji i posledica neovlašćenog pristupa

Problemi zaštite kompjuterskih sistema i komunikacionih mreža od neovlašćenog pristupa izuzetno su aktuelni. Razvoj kompjuterskih tehnologija omogućava građenje mreža određenih arhitektura s mnoštvom segmenata međusobno znatno udaljenim. Posledica je povećanje broja mrežnih jedinica i količine raznovrsnih komunikacionih linija među njima, što, opet, povećava rizik od neovlašćenog priključivanja na mreže i pristupa važnim informacijama.

Osnovni tipovi ugrožavanja zaštite informacija tokom korišćenja kompjuterskih mreža razmatrani su u radu kao i osnovni mehanizmi i usluge kojima se obezbeđuje autentikacija, integritet i poverljivost informacija u kompjuterskim sistemima i mrežama. Izvršena je komparativna analiza i dobijeni su blok dijagrami različitih algoritama kako simetričnog tako i asimetričnog kodiranja. Ispitane su njihove mogućnosti s aspekta održavanja poverljivosti i zahtevanog nivoa autentikacije poslatih poruka.

Jedna od najefikasnijih varijanti korišćenja autentikacije koda poruke je jednosmerna heš funkcija kojom se obezbeđuje autentikacija, digitalni potpis i tajnost. Opisane su metode zaštite poruke pomoću heš kodova. Predstavljene su osnovne karakteristike najčešće korišćenih heš algoritama i heš funkcija.

Detaljno je razmatrana primena protokola Kerber za autentikaciju pomoću simetričnog kodiranja.

Programski i hardverski alat za autentikaciju kompjuterskih mreža

Razmatrani su getvej ekrani, alati za analizu bezbednosti i detekciju napada poput rutera za filtriranje i brane za nivoe sesije i primenjene nivoe. Njihov zajednički nedostatak jeste da ne mogu da spreče mnoge vrste napada (neovlašćene pristupe informaciji kroz lažni server, analizu mrežnog saobraćaja i odbijanje usluge).

Za održavanje tajnosti na određenom nivou u kompjuterskim sistemima koriste se sheme poput Pretty Good Privacy Secure-Multipurpose and Internet Mail Extension (s transportnim i tunelskim režimima protokola). Za održavanje autentičnosti podataka u protokolima primenjuju se algoritmi simetričnog i asimetričnog šifrovanja, heš funkcije i MAC-CODES. Optimizacija sredstva zaštite zavisi od zahteva za svaki pojedinačni slučaj i neophodna je za svaki kompjuterski sistem posebno.

Integritet bi trebao da obezbedi da samo ovlašćeni korisnik obavlja ažuriranje uskladištenih i poslatih informacija. Pod ažuriranjem se podrazumeva menjanje, uklanjanje, kreiranje, kašnjenje ili ponavljanje reprodukcije transferovanih podataka. Za održavanje integriteta algoritama za šifrovanje moraju se koristiti mrežni i transportni nivoi. Integritet poruka znači da će primljene poruke biti identične poslatim, bez gubljenja, dodavanja, promena ili ponavljanja, redom kojim su i poslate. Međutim, protokoli za zaštitu integriteta poruke obično obezbeđuju samo detekciju ugrožavanja integriteta toka podataka, a ne obezbeđuju rekonstrukciju oštećene ili izgubljene informacije.

Tajnost obezbeđuje zaštitu poslatih podataka od pasivnih napada. Njena svrha je da garantuje zaštitu podataka prilikom prenosa između korisnika tokom vremenskog perioda koji se poklapa s protokom podataka celokupne poruke kao i njenih pojedinačnih delova.

Značajan aspect tajnosti je zaštita podataka od analitičkog istraživanja. Šifrovanje kriptografskim metodama je neophodno u ovu svrhu. Data je osnovna klasifikacija ovih metoda i ukratko opisane njihove karakteristike. Detaljnije su razmatrane metode simetrične kriptografije (zasnovane na supstituciji i preuređivanju blokova) kao I metode s upotrebom javnog ključa.

Zaključci

U današnje vreme postojeći alati za zaštitu podataka u kompjuterskim mrežama ne obezbeđuju tajnost, autentifikaciju i verodostojnost podataka. Pravci u zaštiti podataka usmereni ka integrisanom rešenju za opisane probleme zasnivaju se na teoretskim šemama šifrovanja i algebarskim blok šiframa.

Ključne reči: zaštita informacija, kriptografske transformacije, tajnost, autentifikacija, integritet podataka, algoritmi za šifrovanje

MECHANISMS OF PROTECTION OF INFORMATION IN COMPUTER NETWORKS AND SYSTEMS

Evseev Sergey Petrovich, Dorokhov Oleksandr Vasilievich, Korol Olga Grigorievna

Kharkov National University of Economics, Faculty of Economics Informatics, Chair of Information Systems, Ukraine

FIELD: Computer Sciences, Cryptography

Summary:

Protocols of information protection in computer networks and systems are investigated. The basic types of threats of infringement of the protection arising from the use of computer networks are classified. The basic mechanisms, services and variants of realization of cryptosystems for maintaining authentication, integrity and confidentiality of transmitted information are examined. Their advantages and drawbacks are described. Perspective directions of development of cryptographic transformations for the maintenance of information protection in computer networks and systems are defined and analyzed.

Introduction

Creation of modern military computer systems and existence of global telecommunication networks have considerably changed the character and a range of problems of information protection. Information

protection methods become complicated and represent an important part of information technologies. Various cryptographic means are applied for information protection.

The paper deals with the protocols and mechanisms of information protection in computer systems and networks, the analysis of perspective directions of development of cryptographic transformations for the maintenance of information confidentiality, authentication and integrity.

Problems and mechanisms of computer network protection from threats and consequences of non authorized access

Problems of the protection of computer systems and communication networks from non-authorized access have recently become highly topical. Development of computer technologies allows building networks of allocated architectures consisting of plenty of segments, located at a significant distance from each other. All this results in increasing the number of network units and amounts of various communication lines between them, which, in turn, increases risks of non-authorized connections to networks and access to important information.

In this paper the basic types of threats of infringement of the protection arising from the use of computer networks have been discussed. The basic mechanisms and the services providing authentication, integrity and confidentiality of the transmitted information in computer systems and networks are considered. The comparative analysis is carried out and block diagrams of various algorithms of symmetric and asymmetric enciphering are obtained. Their opportunities from the point of view of maintenance of confidentiality and a demanded level of authentication for transmitted messages are examined.

One of the most effective variants for the use of message code authenticity is the unilateral hashing function which can provide authentication, a digital signature and confidentiality. The methods of message protection with the use of hash-codes are described. The basic characteristics of various most widespread hash-algorithms and hash-functions have been presented.

In addition, the application of the Kerberos system for maintaining authentication applying symmetric enciphering is considered and analyzed in detail.

Program and hardware instruments for maintaining the authenticity of allocated computer networks

Gateway screens, tools for the analysis of security and detection of attacks such as filtering routers, sluices of a session level and an applied level are considered. Their common drawback is that they cannot prevent many types of attacks (non-authorized access to information through a false server of service of Internet network domain names, analysis of the network traffic, service refusal).

For maintaining confidentiality at an applied level in computer systems the schemes such as Pretty Good Privacy Secure-Multipurpose and Internet Mail Extension are used (with transport and tunnel modes of protocols). Algorithms of symmetric and asymmetric enciphering, hash-functions and MAC-CODES are applied to maintain data authenticity in protocols. Optimizing the means of protection depends on the requirements for each particular case and it is necessary for each separate computer system.

Integrity should provide updating information stored and transmitted in a network only by authorized users. Updating is understood as a change, removal, creation, delay or repeated reproduction of transferred data. For the maintenance of the integrity of enciphering algorithms, network and transport levels must be used. The integrity of messages means that the received messages will be as accurate as the sent ones, without withdrawals, additions, changes or recurrences and in the initial order. However, protocols of the protection of message integrity usually provide only the detection of infringement of dataflow integrity, and do not provide reconstruction of the damaged or lost information.

Confidentiality provides the protection of transmitted data against passive attacks. It should guarantee protection of the data transferred between users during certain time occurring simultaneously with the outflow of data during messages and their separate parts transfer process.

A significant aspect of confidentiality is data protection against analytical research. For this purpose, enciphering by cryptographic methods is necessary. Their general classification and brief descriptions are presented. The methods of symmetric cryptography (based on blocks of substitutions and rearrangements), and the methods of public-key cryptography have been considered in particular.

Conclusions

Nowadays, in data protection in computer networks, existing protection tools do not provide confidentiality, authenticity and integrity of transmitted data and information. The perspective directions of the integrated solution of the described problems in protection mechanisms are to use corresponding tools based on theoretical-code schemes and algebraic blocks codes.

Key words: *information protection, cryptographic transformations, confidentiality, authentication, data integrity, encrypting algorithms*

Datum prijema članka: 29. 06. 2011.

Datum dostavljanja ispravki rukopisa: 10. 07. 2011.

Datum konačnog prihvatanja članka za objavljivanje: 12. 07. 2011.