# ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

**А.И. Галабурда**

*(БГТУ, г. Минск)*

Развитие средств шифрования стимулируется распространением электронной коммерции, виртуальных частных сетей и растущим числом мобильных сотрудников.

Особую роль в вопросе унификации и стандартизации играют различные стандарты и протоколы, а также продукты на их основе.

Универсальный протокол, основанный на использование цифровых сертификатов, являющийся в настоящее время стандартом де-факто для решения проблемы безопасности для Web технологий был разработан компанией Netscape Communications, Inc. Этот протокол получил название SSL (Secure Sockets Layer). В настоящее время SSL используется наиболее распространенными программными продуктами для World-Wide-Web (в том числе браузерами Netscape и Microsoft Explorer) для работы в защищенном режиме HTTPS (HTTP Secure).

Он позволяет решить следующие задачи:

– Обеспечить сокрытие передаваемой информации

– Обеспечить целостность этой информации, т.е. защиту от модификации

– Обеспечить аутентификацию сервера и клиентов

Протокол SSL обеспечивает безопасную передачу данных:

– Закрытое соединение. Для шифрования данных используются симметричные алгоритмы( DES[DES], RC4[RC4])

– Аутентификация узлов производится с использованием асимметричных алгоритмов(RSA[RSA], DSS[DSS]).

– Используется надежное соединение. При передаче используется проверка целостности данных с использованием ключевого MAC. Для вычисления MAC используются надежные хеш функции (SHA, MD5).

Защита подразумевает систему распределения сертификатов. Сертификационный центр обеспечивает персональными сертификатами администраторов виртуальных компьютеров и сайт сертификатами - сервера ресурсов. При создании специальных защищенных ресурсов внутри виртуальных компьютеров возможно предоставление персональных сертификатов и пользователям. Все управление подсистемами осуществляется администраторами по защищенному протоколу SSL/TLS. Использование СУБД во многом упроща-

ет схему взаимодействия подсистем и обеспечивает гибкость. В качестве системы защиты от несанкционированного доступа возможно использование FireWall, Ip filter или специализированных, типа Kweb. Пополнение перечня используемых в портале подсистем осуществляется созданием нового программного обеспечения, реализующего новые функции, единого на все виртуальные компьютеры с общей системой пополнения и выбора информации.

Для унификации средств защиты, а также для обеспечения поддержки разработчикам фирма "Микрософт" заложила в свою операционную систему Windows Crypto Api- интерфейс для обеспечения приватности данных.

Программный интерфейс CryptoAPI фирмы Microsoft предоставляет возможности для добавления в приложение, основанное на базе Win32, функций аутентификации, шифрования, расшифрования и электронной подписи. Для написания программы использующей CryptoAPI не надо знать конкретных реализаций алгоритмов шифрования, как не надо знать, например, процедур управления графической картой при использовании графической библиотеки.

Задачами CryptoAPI являются:

- Аутентификация сетевых пользователей
- Шифрование и дешифрование сетевых сообщений
- Шифрование и дешифрование данных
- Создание цифровой подписи и ее подтверждение

CryptoAPI состоит из пяти различных функциональных областей, взаимодействующих с приложением.

В корне иерархии находится криптопровайдер. Напрямую к провайдеру (CSP) приложение обратиться не может.

Функции кодирования сертификатов – эти функции управляют сертификатами и сопутствующими данными через сеть OSI (соединение открытых систем, семиуровневая модель) как описано в CCIT X.200. Методы OSI, описывающие абстрактные объекты, используют абстрактную синтаксическую нотацию один (ASN.1), как описано в CCITT X.209.

Функции базы сертификатов – используются для хранения сертификатов и управления ими. Пользователь со временем может собрать весьма много сертификатов. Обычно это сертификаты описывающие самого пользователя и сертификаты сущностей с которыми он взаимодействует. Обычно для каждой сущности есть несколько сертификатов - связок, используемых для проверки отслеживания существующих сертификатов у авторитета сертифи-

катов (обычно это сайт с сертификатами, отвечающий своим авторитетом за их верность).

Базовые криптографические функции – используются для наиболее полного использования криптографических возможностей в приложении. Это функции взаимодействующие с провайдером. Все криптографические операции выполняются независимыми модулями называемыми Cryptographic Service Providers (CSP). Каждый CSP предлагает различные реализации криптографической поддержки используемой через CryptoAPI. Некоторые провайдеры несут более сильные алгоритмы, некоторые содержат физические компоненты (смарткарты, криптоускорители). В дополнение, некоторые CSP могут напрямую работать с пользователем при использовании личного ключа или подписи.

Однако, версии операционной системы Windows отличаются по функциональным возможностям. Наиболее полно Crypto Api реализован в Windows 2000.

Такие инструментальные средства, как CryptoAPI, и новые, получившие поддержку в отрасли API-интерфейсы, разработанные компаниями RSA Data Security, IBM, JavaSoft, Netscape Communications и др., способны дать толчок широкому применению шифрования, поскольку превращают подобные алгоритмы в стандартные средства операционных систем. Шифрование может быть реализовано на разных уровнях. Самый нижний – это микросхемы и адаптеры, кодирующие, к примеру, данные, передаваемые по сетевому кабелю или отправляемые с рабочей станции. В то же время одной из наиболее привлекательных новых технологий является разработанный Рабочей группой инженеров Internet (IETF) протокол IPsec, предусматривающий стандартный способ шифрования трафика на уровне IP. Он может заменить патентованные решения, предлагаемые производителями брандмауэров и маршрутизаторов. Протокол IPsec включен в некоторые инструментальные средства шифрования и ПО маршрутизаторов.

Вот одно из применений CryptoApi. Одним из нововведений Windows 2000 и NTFS 5.0 является Encrypted File System (EFS), которая используется для шифрования файлов. NTFS по сути является защищенной файловой системой, однако в связи со все более широким распространением таких утилит, как NTFSDos, позволяющих обойти систему защиты NTFS, требуется дополнительный уровень защиты файловой системы. Система EFS использует

шифрование с открытым и закрытым ключом и архитектуру CryptoAPI. EFS может использовать любой симметричный алгоритм шифрования файлов, однако первоначальная версия использует только DES. В Северной Америке используются 128-битные ключи, а за ее пределами - 40-битные ключи.

В настоящее время закладываются предпосылки для унификации и стандартизации средств шифрования, что в свою очередь позволяет встраивать криптографическую защиту в программы и операционные системы на более высоком уровне.

**Литература:**

1. Schneier, Bruce. Applied Cryptography. John Wiley & Sons, 1996.
2. http://www.bdv.newmail.ru/
3. RSA Laboratories, a division of RSA Data Security, Inc., RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS), Copyrightc 1991-1993.

## СИСТЕМА АУТЕНТИФИКАЦИИ KERBEROS.

**А.И. Галабурда**
*(БГТУ, г. Минск)*

Используемые некогда лишь в правительственных учреждениях, таких как Агентство национальной безопасности и военные организации, алгоритмы шифрования сегодня нашли применение в коммерческом ПО брандмауэров. Этот процесс в значительной степени стимулируется распространением электронной коммерции, виртуальных частных сетей и растущим числом мобильных сотрудников. Сейчас улучшению защиты данных, передаваемых между узлами Internet, уделяется самое пристальное внимание.

Особую роль в вопросе унификации и стандартизации играют различные стандарты и протоколы, а также продукты на их основе.

Одним из нововведений Windows 2000 является система распределения ключей Kerberos 5.0. Kerberos – протокол аутентификации, основанный на распределении секретной информации, т.е. пользователь и ЦРК знают пароль пользователя. Кроме клиента и сервера применяется третий участник системы обмена ключевой информацией – ЦРК, которому «доверяют» и клиент и сервер. Протокол предполагает серию передач информации между клиентами, ЦРК, и серверами для получения и использования «билетов» kerberos.