УСТРОЙСТВА И СИСТЕМЫ АППАРАТНОГО ШИФРОВАНИЯ

ВЫПОЛНИЛА СТУДЕНТКА
ГРУППЫ ТКИ – **311**
СЕМЕНЧУК М.В.

Шифрование – это метод, используемый для преобразования данных в шифрованный текст для того, чтобы они были прочитаны только пользователем, обладающим соответствующим ключом шифрования для расшифровки содержимого. Шифрование используется тогда, когда требуется повышенный уровень защиты данных - при хранении данных в ненадежных источниках или передачи данных по незащищенным каналам связи.

С помощью шифрования обеспечиваются три состояния безопасности информации:

- Конфиденциальность.

Шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении.

- Целостность.

Шифрование используется для предотвращения изменения информации при передаче или хранении.

- Идентифицируемость.

Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Сегодня для шифрования данных наиболее широко применяют три вида шифраторов: аппаратные, программно-аппаратные и программные. Их основное различие заключается не только в способе реализации шифрования и степени надёжности защиты данных, но и в цене, что часто становится для пользователей определяющим фактором.

Аппаратное шифрование

Аппаратное шифрование – процесс шифрования, производимый при помощи специализированных вычислительных устройств. Современные средства криптографической защиты информации нельзя строго отнести к аппаратным, их было бы правильнее называть аппаратно-программными, однако, поскольку их программная часть неподконтрольна ОС, в литературе их часто называют аппаратными. Основной особенностью аппаратных СКЗИ является аппаратная реализация (за счет создания и применения специализированных процессоров) основных криптографических функций – криптографических преобразований, управления ключами, криптографических протоколов и т. д.

Перечень достоинств аппаратных шифраторов:

- аппаратный датчик случайных чисел создаёт действительно случайные числа для формирования надёжных ключей шифрования и электронной цифровой подписи;
- аппаратная реализация криптоалгоритма гарантирует его целостность;
- шифрование и хранение ключей осуществляются в самой плате шифратора, а не в оперативной памяти компьютера;
- загрузка ключей в шифрующее устройство с электронных ключей Touch Memory (i-Button) и смарт-карт производится напрямую, а не через системную шину компьютера и ОЗУ, что исключает возможность перехвата ключей;
- с помощью аппаратных шифраторов можно реализовать системы разграничения доступа к компьютеру и защиты информации от несанкционированного доступа;
- применение специализированного процессора для выполнения всех вычислений разгружает центральный процессор компьютера; также можно установить нескольких аппаратных шифраторов на одном компьютере, что ещё более повышает скорость обработки информации (это преимущество присуще шифраторам для шины PCI);
- применение парафазных шин при создании шифрпроцессора исключает угрозу чтения ключевой информации по колебаниям электромагнитного излучения, возникающим при шифровании данных, в цепях «земля — питание» устройства.

Современный рынок предлагает 3 разновидности аппаратных средств шифрования информации потенциальным покупателям

- блоки шифрования в каналах связи
- самодостаточные шифровальные модули (они самостоятельно выполняют всю работу с ключами)
- шифровальные платы расширения для установки в персональные компьютеры

Примеры аппаратного шифрования

- USB-шифратор ruToken

ruToken — российское средство аутентификации и защиты информации, использующее сертифицированные алгоритмы шифрования и аутентификации и объединяющее в себе российские и международные стандарты безопасности.

ruToken представляет собой небольшое электронное устройство, подключаемое к USB-порту компьютера (USB-брелок). Он является аналогом смарт-карты, но для работы с ним не требуется дополнительное оборудование (считыватель)

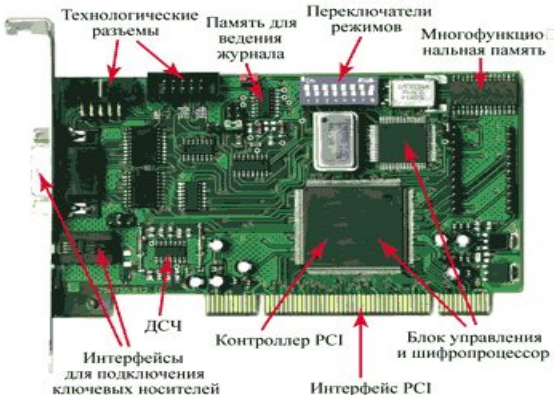
Аутентификация

- Замена парольной защиты при доступе к БД, Web-серверам, VPN-сетям и security-ориентированным приложениям на программно-аппаратную аутентификацию;
- Защищённые соединения при доступе к почтовым серверам, серверам баз данных, Web-серверам, файл-серверам, аутентификации при удалённом доступе.

- УКЗД КРИПТОН

Устройства криптографической защиты данных (УКЗД) серии КРИПТОН — это аппаратные шифраторы для IBM PC-совместимых компьютеров. Устройства применяются в составе средств и систем криптографической защиты данных для обеспечения информационной безопасности (в том числе защиты с высоким уровнем секретности) в государственных и коммерческих структурах.

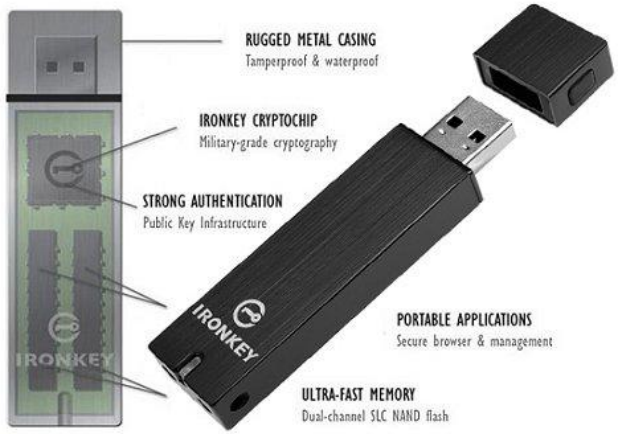
КРИПТОН — серия аппаратных шифраторов для IBM PC-совместимых компьютеров, выполнены в виде плат расширения ISA и PCI персонального компьютера с процессором i386 и выше.



- IronKey

IronKey флеш-диск с прозрачным аппаратным шифрованием данных. Предназначен для безопасного хранения секретных данных.

- Защищённая память объёмом 1-32Гб, в зависимости от модели.
- Самоуничтожение ключей шифрования и собственно данных после 10 неправильных попыток ввода пароля (устройство более не работоспособно).
- Дополнительные функции, обеспечивающие безопасность работы пользователя (менеджер паролей, анонимный шифрованный доступ в интернет, виртуальная клавиатура, утилита создания и восстановления зашифрованных резервных копий и т.д.)



СПАСИБО ЗА ВНИМАНИЕ!