**Аппаратные шифраторы**

Аннотация: Материал, полученный в этом исследовании, предназначен для ознакомления читателей с аппаратными шифраторами в современном мире, а также с их преимуществами и недостатками.

Ключевые слова: криптография; криптосистема; аппаратные шифраторы

Вчера, сегодня и, возможно, завтра, очень часто для шифрования данных, по крайней мере такие шифраторы, как аппаратные шифраторы используются в качестве крайних аппаратных шифров, программных и аппаратных кодеров и, наконец, программного обеспечения. Все они отличаются не только способом шифрования, но и ценовой категорией. Самые дорогостоящие шифраторы - это аппаратные, а затем программно-аппаратные, а затем большинство низкостоющие - программные. По сути, все эти шифраторы имеют определенные неотъемлемые функции - шифровать, но поскольку в денежном выражении все они совершенно разные, нет смысла выбирать самые дешевые или самые дорогие, так как можно сказать, что они одинаковые.

Цель этой статьи - проанализировать аппаратное шифрование.

В рамках этой работы был проведен анализ литературы, посвященной криптографии, а также выявление плюсов и минусов аппаратного шифрования.

Чтобы узнать больше об аппаратном шифровании, вам нужно понять, что такое криптография, что такое аппаратное шифрование и определить компоненты в нем.[[1]](#footnote-2)

Криптография - это наука о методах обеспечения, целостности данных и аутентификации, а также о невозможности отказа от авторства.

Криптография первоначально изучала методы (возможности) шифрования информации - обратимое преобразование открытого (исходного) текста на основе секретного алгоритма или ключа в самом зашифрованном тексте (зашифрованном тексте). Традиционная криптография формирует разделение симметричных криптосистем, в которых шифрование и дешифрование выполняются с использованием того же секретного ключа. Само слово криптография формируется из древнегреческих Kriptos-скрытый и graphy - пишу, что ясно, криптография - это шифропись (скрытопись).

Преимущества и недостатки аппаратного шифратора.

Программные шифраторы ниже в ценовой категории, чем аппаратные, и в некоторых случаях способны обеспечить быструю скорость обработки данных, но список их преимуществ исчерпан. Но все же преимущества аппаратного шифратора намного выше, среди них:

Аппаратный генератор случайных чисел использует действительно случайные числа, что, в свою очередь, дает огромное преимущество в защите информации;

аппаратная реализация дает стопроцентную гарантию целостности алгоритма криптографии;

шифрование и хранение ключей происходит в шифре, а не в;

с электронных ключей или с электронных носителей, загрузка ключей происходит напрямую, а не через компьютер, который никогда не позволит вам перехватить ключ;

благодаря аппаратным шифрам вы можете сделать дифференциацию доступа к компьютеру, избегая при этом несанкционированного доступа;

При использовании нескольких аппаратных кодеров можно увеличить скорость обработки информации

Если вы добавите на свой компьютер специальное оборудование для шифрования, то проблем будет меньше, чем при добавлении функций подобного криптографического оборудования в программное обеспечение. Само шифрование должно быть прозрачным даже для пользователя. Если вы делаете то же самое с помощью программного обеспечения, вам нужно скрыть его достаточно глубоко в операционной системе. Это непросто сделать с хорошо функционирующей операцией. Даже любой непрофессионал сможет подключиться к компьютеру или модему с помощью устройства шифрования

Типы аппаратных устройств шифрования.

На рынке существует три типа аппаратных средств шифрования

блоки шифрования в каналах связи

автономные модули шифрования

криптографические карты расширения для установки на персональных компьютерах

В дополнение ко всем основным функциям шифрования изобретатели пытаются добавить на свои устройства различные функции, например:

Генератор случайных чисел - необходимо создать криптографические ключи. При создании подписи каждый раз используется новое число, генерируемое генератором.

Надежная загрузка. Он управляет входом на компьютер. При каждом включении компьютера пользователю запрашиваются его данные, которые уже забиты в устройстве шифрования. Если ключи кодера считаются их собственными, компьютер продолжит свою работу. Если все происходит наоборот, пользователю придется разобрать компьютер и вытащить шифр оттуда, чтобы выключить компьютер.

Контролируйте целостность файлов операционной системы. В ваше отсутствие злоумышленник ничего не может изменить. Шифрование сохраняет весь список всех важных файлов, если есть взлом, злоумышленник не может ничего сделать, если при следующей загрузке, если есть несоответствие хотя бы одного из файлов, произойдет блокировка.[[2]](#footnote-3)

Устройство для защиты криптографических данных - другими словами, UKKD, называется материнской платой со всеми вышеперечисленными функциями. Аппаратное устройство шифрования, которое контролирует ввод персонального компьютера и проверяет целостность всех файлов операционной системы, также называется «электронным замком». Конечно, аналогия не совсем то же самое - обычные замки намного уступают этим устройствам. Доступ ко всем файлам осуществляется только от администратора или от лица, которому доверяет администратор.

Как работает шифр процессор?

Для этого рассмотрим схему, на которой будет представлен сам процесс

1) В общем, калькулятор представляет собой набор регистров, которые обмениваются данными между шинами данных. Это калькулятор, который создает определенные криптографические методы с достаточной скоростью выполнения. Вначале калькулятор получает определенный текст или информацию, которые необходимо зашифровать, а также ключ шифрования, который является произвольно сгенерированным числом. Само шифрование - довольно сложное математическое преобразование, поэтому оно похоже на набор сгенерированных чисел (величин).

2) Блок управления, так сказать, программа, которая управляет калькулятором. Если вы по какой-либо причине измените программу, работа завершится неудачно. Исходя из этого, мы можем сказать, что программа для хорошей производительности должна не только быть достаточно стабильной и функциональной, но и всегда выполнять проверку. В общем, калькулятор также отправляет задания в блок управления, которые контролируют его работу. В общем, в жизни есть два или более шифров процессора. Это необходимо для сравнения производительности каждого устройства.

3) Буфер ввода и вывода необходим для повышения производительности самого устройства. Это происходит так: когда первый блок зашифрован, второй блок сразу загружается и так далее, пока информация не будет завершена. То же самое происходит на выходе. Этот способ работы значительно увеличивает скорость шифрования.

Исходя из всего вышеизложенного, мы можем заключить, что криптографический метод - аппаратное шифрование остается надежным способом скрыть информацию на сегодняшний день, хотя в нем есть относительно много плюсов и минусов. Но, несмотря на это, криптографические методы (аппаратное шифрование) популярны в определенных областях, связанных с защитой информации и защитой личной информации.

**Список используемой литературы**

1. Лукашов Игорь Владиславович «Криптография? Железно! »[Электронный ресурс] // Электронная статья. URL: http: //www.osp.ru/pcworld/2003/03/165312/ (дата обращения 25.12.2015г.)

2. Панасенко С.П., Ракитин В.В. Аппаратные шифраторы. [электронный ресурс] // Электронная статья. URL: http: //www.osp.ru/pcworld/2002/08/163808/ (дата обращения 25.12.2015г.)

1. Лукашов Игорь Владиславович «Криптография? Железно! // Электронная статья. (дата обращения 25.12.2015г.) [↑](#footnote-ref-2)
2. Панасенко С.П., Ракитин В.В. Аппаратные шифраторы. [электронный ресурс] // Электронная статья. URL: http: //www.osp.ru/pcworld/2002/08/163808/ (дата обращения 25.12.2015г.) [↑](#footnote-ref-3)