

КОМПЛЕКСНАЯ ЗАЩИТА КОМПЬЮТЕРА НА БАЗЕ УСТРОЙСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ



Алгоритмы защиты информации, в частности, алгоритмы шифрования, могут быть реализованы как программным, так и аппаратным способом. Оба варианта имеют ярко выраженные достоинства и недостатки. Основным недостатком устройств криптографической защиты данных (УКЗД), реализующих аппаратное шифрование информации, - это их относительно высокая стоимость. К достоинствам же относится тот факт, что на базе УКЗД можно обеспечить всестороннюю защиту компьютера, чего нельзя сделать при использовании только программно реализованного шифрования.

Панасенко С.П., начальник отдела разработки программного обеспечения фирмы "АНКАД"

Принципы работы УКЗД

Основное назначение УКЗД - шифрование данных. Эта операция выполняется шифропроцессором, представляющим собой специализированную микросхему, которая выполняет криптографические операции, или микросхему программируемой логики (PLD - Programmable Logic Device). Шифропроцессоров может быть несколько для повышения скорости и/или надежности шифрования. Для повышения скорости информацию распараллеливают между ними. Для обеспечения надежности производят обработку одних и тех же данных двумя шифропроцессорами с последующим сравнением результатов перед их выдачей.

Шифропроцессорами и другими модулями УКЗД управляет основной модуль - блок управления, реализуемый обычно на базе микроконтроллера с достаточным количеством внутренних ресурсов и хорошим быстродействием.

Помимо собственно шифрования, УКЗД может выполнять ряд дополнительных функций, из которых, прежде всего, стоит отметить следующие:

- наличие аппаратного датчика случайных чисел (ДСЧ), которые необходимы для генерации криптографических ключей, а также используются в алгоритмах электронной цифровой подписи (ЭЦП);
- наличие функциональности электронного замка: контроль

входа пользователя на компьютер и контроль целостности файлов операционной системы.

Последняя из данных функций позволяет обеспечить на базе УКЗД полноценную защиту компьютера от несанкционированного доступа. Рассмотрим более подробно принципы работы электронного замка.

Защита компьютера от несанкционированного доступа

УКЗД, работающее в режиме электронного замка, при загрузке компьютера перехватывает управление (в тот момент, когда BIOS компьютера опрашивает вставленные в него аппаратные модули) и выполняет следующий набор действий:

- 1) Предлагает пользователю вставить специальный ключевой носитель (в простейшем случае - дискету с файлами криптографических ключей), с которого считывает необходимую информацию. Производится анализ предъявленных ключей и аутентификация пользователя. Если пользователь не входит в число тех, кому разрешен доступ на данный компьютер (список хранится в памяти УКЗД), в загрузке компьютера будет отказано.
- 2) Производится контроль целостности важных файлов компьютера согласно списку, хранящемуся в памяти УКЗД. Список контролируемых файлов хранится вместе с контрольными суммами или хэш-значениями, рассчитанными по алгоритму ГОСТ Р 34.11-94 для каждого файла, входящего в список. Если хэш хотя бы одного из файлов списка не совпадает с эталоном для данного файла, УКЗД расценивает это как нарушение

целостности операционной системы и блокирует загрузку компьютера.

- 3) Если описанные выше условия выполнены, УКЗД возвращает компьютеру управление, разрешая загрузить операционную систему. Удачная или неудавшаяся попытка входа на компьютер фиксируется в аппаратном журнале УКЗД.

Подразумевается, что за каждое рабочее место, оснащенное УКЗД, отвечает администратор по безопасности (один на организацию или структурное подразделение). В данном случае его функциями является настройка и обслуживание электронного замка, а именно:

- 1) создание списка пользователей, которым разрешен доступ на компьютер, и генерация ключевых комплектов для каждого из них;
- 2) создание списка контролируемых файлов. Набор файлов различается в зависимости от используемой операционной системы и выполняемых пользователем задач. Набор файлов может выглядеть следующим образом: `io.sys`, `msdos.sys`, `autoexec.bat`, `gdi32.dll`, `kernel32.dll`, `user32.dll`, `normal.dot`, `winword.exe` и т.д. Нарушение целостности этих файлов (которые находятся в постоянном использовании) может быть следствием попытки внедрения злоумышленником программной закладки с целью, например, последующего перехвата и/или модификации обрабатываемой

информации;

- 3) анализ журнала УКЗД для расследования попыток несанкционированного входа на компьютер.

Электронный замок отличает администратора от непривилегированных пользователей по специальному ключевому носителю администратора, по предъявлении которого перечисленные выше возможности по настройке становятся доступными.

Для обеспечения полной надежности защиты от НСД, память УКЗД содержит программную среду, гарантированно свободную от внедренного злоумышленником программного обеспечения ("закладок"). Именно в этой среде, загружаемой в компьютер непосредственно из памяти УКЗД, и производятся все описанные выше проверки. Гарантированная программная среда не позволит также злоумышленнику осуществить перехват ключевой информации на этапе ее ввода в УКЗД.

Принципы взаимодействия с прикладными процессами

Все же основное значение УКЗД - аппаратное шифрование

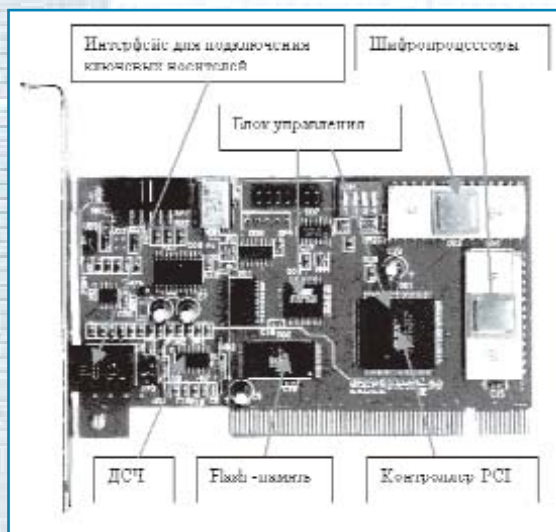


Рис. 1. УКЗД и его модули на примере КРИПТОН-4/РС1.

данных, выполняемое согласно получаемым устройством командам. Команды может отдавать, например, программа шифрования файлов. Рассмотрим принципы взаимодействия прикладных программ с УКЗД на примере операционных систем семейства Microsoft Windows.

УКЗД может одновременно использоваться несколькими программами, например:

- программой прозрачного шифрования логических дисков компьютера;
- модулем шифрования сообщений электронной почты;
- программой ЭЦП (запросы к ДСЧ);
- программой генерации ключей шифрования (запросы к ДСЧ).

Обычно прикладные программы не получают прямого интерфейса к УКЗД (что было принято в MS-DOS). В Windows такой подход неприменим по ряду причин, в качестве основной из которых следует назвать возможность возникновения коллизий при одновременном обращении различных программ к УКЗД. Поэтому на промежуточном уровне между Windows-приложениями и УКЗД располагается программный интерфейс, управляющий УКЗД и решающий нижеперечисленные задачи.

1) Управление очередностью обращений к УКЗД различных прикладных программ и модулей. Интерфейс управления УКЗД для каждой программы, которая обращается к УКЗД, создает отдельную сессию, а затем следит за корректным очередным предоставлением ресурсов УКЗД разным сессиям. Это несколько похоже на распределение ресурсов центрального процессора компьютера между несколькими программами в многозадачной среде. Таким образом, УКЗД виртуализуется для каждого прикладного процесса - каждая сессия имеет как бы собственный шифратор со своими ключами шифрования, которые корректно перезагружаются при переключении между сессиями.

2) Предоставление корректного интерфейса к УКЗД прикладным программам, работающим в DOS-сессии Microsoft Windows. Эта особенность позволяет использовать УКЗД в многозадачной среде DOS-программам, не рассчитанным на многозадачность и требующим монопольного использования ресурсов УКЗД. Механизм виртуализации

позволяет выполнять такие DOS-программы параллельно с шифрующими Windows-приложениями.

3) Предоставление стандартного интерфейса функций УКЗД Windows-приложениям.

4) Возможность подключения различных типов УКЗД через драйверы, предоставляющие стандартный набор

функций, требуемый интерфейсу управления УКЗД. Это позволяет прикладным программам не зависеть от конкретного типа УКЗД. В данном случае вместо УКЗД можно подключить и программный шифратор, работающий на уровне ядра операционной системы.

Таким образом, при обращении программы к УКЗД любой запрос проходит несколько уровней:

- 1) уровень приложений;
- 2) уровень, обеспечивающий интерфейс между приложением и драйвером УКЗД;
- 3) уровень ядра операционной системы - драйвер УКЗД;
- 4) аппаратный уровень - собственно УКЗД.

Тем не менее, несмотря на сложность реализации такой схемы, по принципу унификации интерфейсов и разделения аппаратных ресурсов в системах семейства Microsoft Windows работают многие подсистемы, например сетевая.

Комплексная защита компьютера

Рассмотрим комплекс задач по обеспечению защиты информации на персональном компьютере. Для большинства случаев приведенный список является избыточным - набор задач на конкретных автоматизированных рабочих местах (АРМ) представляет собой подмножество приведенных здесь.

- 1) Обеспечение защиты компьютера от НСД и контроль целостности операционной системы - во избежание внедрения злоумышленником программных закладок, имеющих целью перехват криптографических ключей, прочтение и модификацию хранимой и обрабатываемой информации,

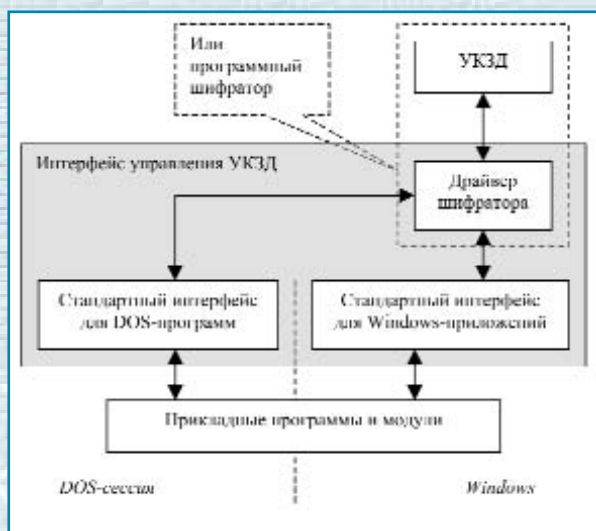


Рис.2. Интерфейс управления УКЗД.

- удаленное управление компьютером и т.д.
- 2) Обеспечение конфиденциальности и целостности хранящейся и обрабатываемой информации.
 - 3) Обеспечение конфиденциальности и целостности, а также подтверждение авторства информации, передаваемой по локальным и/или глобальным вычислительным сетям.
 - 4) Обеспечение защиты компьютера от НСД по сети.

Решение первой из приведенных задач - применение УКЗД в режиме электронного замка, который подробно описан выше. Данный режим имеет один серьез-

производит автоматическое зашифрование данных при их записи на HDD компьютера и их расшифрование при чтении. Ясно, что в данном случае удаление УКЗД или хищение HDD не позволит злоумышленнику получить доступ к информации.

Помимо средств прозрачного шифрования, существуют и программы, в которых можно вручную выбирать шифруемые объекты (файлы или каталоги). Применение таких программ совместно с программами ЭЦП решает задачи обеспечения конфиденциальности и целостности хранящейся и передаваемой информации. Программные модули, реализующие алгоритмы шифрова-

Защита от НСД по сети обеспечивается применением прозрачного шифрования сетевого обмена данными в сочетании с механизмом фильтрации входящих и исходящих информационных пакетов. Здесь соблюдается аналогия с программами прозрачного шифрования логических дисков в том смысле, что достаточно один раз настроить критерии фильтрации сетевых пакетов и критерии выбора криптографических ключей, после чего все действия будут выполняться автоматически.

Следует также отметить, что существуют специализированные АРМ, например АРМ администратора по безопасности, где, помимо перечисленных задач, УКЗД используется для генерации комплектов криптографических ключей для всех пользователей организации или структурного подразделения.

Иллюстрирующая описанное выше схема (рис. 3) в большинстве случаев является избыточной. Однако она наглядно показывает возможность построения хорошего защищенного АРМ на базе УКЗД.

Литература:

1. Онучин С. Устройства защиты информации: критерии выбора. // Connect! Мир связи. 1998, № 11, с. 104-107.
2. Панасенко С. Комплексная защита информации. // Информационные технологии. 2001, № 3, с. 14-16.
3. Панасенко С. Защита от несанкционированного доступа. // Банки и технологии. 2001, № 5, с. 82-85.

**С автором
можно связаться
по E-mail:
develop@ancud.ru**

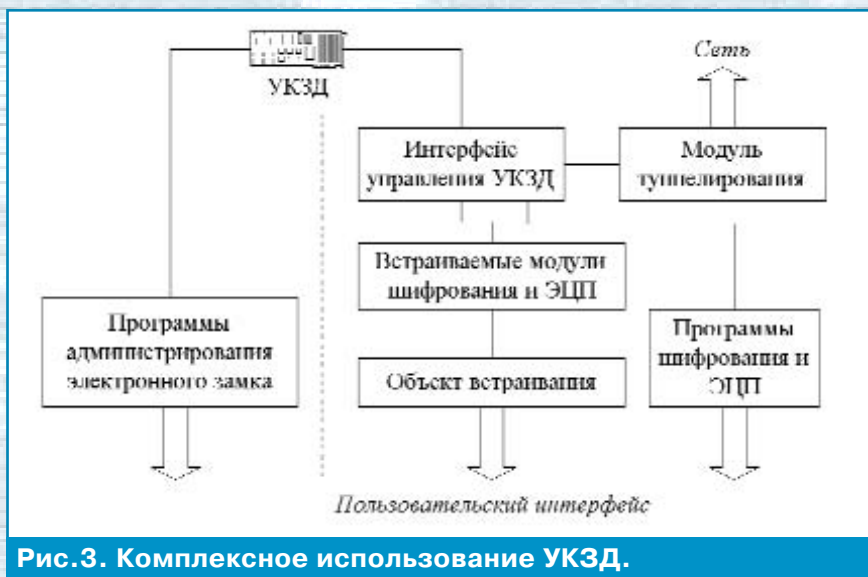


Рис. 3. Комплексное использование УКЗД.

ный недостаток - злоумышленник может вынуть УКЗД из компьютера, что позволит ему получить желаемый доступ к компьютеру. Эта проблема решается административными мерами и/или применением средств прозрачного шифрования информации.

Термин "прозрачное" означает незаметность шифрования для пользователя. Средство прозрачного шифрования обычно один раз настраивается на шифрование определенных логических дисков компьютера, после чего

и ЭЦП, в зависимости от конкретных задач выполняются как в виде отдельных программ с графическим интерфейсом или интерфейсом командной строки, так и в виде дополнительных модулей, встраиваемых в наиболее часто используемые приложения, например Windows Explorer, Microsoft Office и т.д. В любом из этих случаев для шифрования и генерации случайных чисел программными модулями используются ресурсы УКЗД через интерфейс управления УКЗД.