**Задание на 07.02.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу №15 Идентификация и аутентификация пользователей операционных систем.**
3. **Сделать практическую работу №16 Аудит в операционных системах**
4. **Отчет отправить на почту svebalch@mail.ru**

**Лекция 15**

**Устройства криптографической защиты данных серии КРИПТОН**

Фирма АНКАД известна на отечественном рынке как разработчик, производитель и поставщик аппаратно-программных криптографических средств защиты информации серии КРИПТОН . Традиционно они выпускались в виде устройств с минимальным программным обеспечением. Встраивание их в конечные системы осуществлялось пользователем. В настоящий момент наряду с производством и поставкой устройств фирма предлагает готовые решения: от программ абонентского шифрования и электронной подписи до защиты отдельных рабочих мест и систем в целом.

В состав средств криптографической защиты информации (СКЗИ) фирмы АНКАД включены (рис. 7.1):

wpgD8

Рисунок 7.1 – Структура средств криптографической защиты информации

1. устройства криптографической защиты данных (УКЗД) и их программные эмуляторы;
2. контроллеры смарт-карт;
3. системы защиты информации от несанкционированного доступа

(СЗИ НСД);

1. программы абонентского шифрования, электронной подписи и защиты электронной почты;
2. коммуникационные программы прозрачного шифрования IP-пакетов и ограничения доступа к компьютеру по сети;
3. криптомаршрутизаторы;
4. библиотеки поддержки различных типов смарт-карт;
5. библиотеки функций шифрования и электронной цифровой подписи для различных операционных систем.

Отдельным рядом (семейством) устройств с использованием криптографических методов защиты являются специализированные модули безопасности для терминального оборудования, контрольно-кассовых машин, банкоматов и другого оборудования, используемого в палтежных и расчетных системах.

Отличительной особенностью и в этом смысле уникальностью семейства УКЗД фирмы АНКАД является разработанная ею в рамках научно-технического сотрудничества с ФАПСИ отечественная специализированная

микропроцессорная элементная база для наиболее полной и достоверной аппаратной реализации российского стандарта шифрования (см. табл. 7.1). В настоящее время серийно выпускаются УКЗД КРИПТОН -4, 4К/8 и 4К/16, предназначенные для шифрования по ГОСТ28147-89 и генерации случайных чисел при формировании ключей. Началось производство устройств серии КРИПТОН с интерфейсом шины PCI.

В качестве ключевых носителей применяются дискеты, смарт-карты и Touch-Memory. Все ключи, используемые в системе, могут шифроваться на мастер-ключе и храниться на внешнем носителе в зашифрованном виде. Они расшифровываются только внутри платы. Устройство может выполнять проверку целостности программного обеспечения до загрузки операционной системы, а также играть роль электронного замка персонального компьютера, обеспечивая контроль и разграничение доступа к нему.

УКЗД семейства КРИПТОН аттестованы в ФАПСИ, широко применяются в разнообразных защищенных системах и сетях передачи данных и имеют сертификаты соответствия ФАПСИ в составе ряда АРМ абонентских пунктов при организации шифровальной связи I класса для защиты информации, содержащей сведения, составляющие государственную тайну.

Для систем защиты информации от несанкционированного доступа разработана специальная плата КРИПТОН -НСД, выполняющая программное шифрование по ГОСТ28147-89, аппаратную генерацию случайных чисел, загрузку ключей с дискет, смарт-карт или Touch Memory.

Для встраивания в конечные системы пользователя УКЗД имеют два уровня интерфейса в виде набора команд устройства и библиотеки функций. Команды выполняются драйверами устройств для операционных систем DOS, Windows 95/98 и NT4.0, UNIX. Функции реализованы на основе команд.

Наиболее важными особенностями рассматриваемых плат являются:

1. наличие загружаемого до загрузки операционной системы мастер

ключа, что исключает его перехват;

1. выполнение криптографических функций внутри платы, что исключает их подмену или искажение;
2. наличие аппаратного датчика случайных чисел;
3. реализация функций проверки целостности файлов операционной системы и разграничения доступа к компьютеру;
4. высокая скорость шифрования: от 350 Кбайт/с (КРИПТОН -4) до

8800 Кбайт/с (КРИПТОН 8/PCI).

Допустимо параллельное подключение нескольких устройств одновременно в одном персональном компьютере, что может значительно повысить интегральную скорость шифрования и расширить другие возможности при обработке информации.

Средства серии КРИПТОН независимо от операционной среды обеспечивают:

1. защиту ключей шифрования и электронной цифровой подписи

(ЭЦП );

1. неизменность алгоритма шифрования и ЭЦП .

Все ключи, используемые в системе, могут шифроваться на мастер-ключе и храниться на внешнем носителе в зашифрованном виде. Они расшифровываются только внутри платы. В качестве ключевых носителей используются дискеты, микропроцессорные электронные карточки (смарткарты) и "таблетки" Touch-Memory.

**Устройства для работы со смарт-картами.**

Для ввода ключей, записанных на смарт-карты, предлагаются разработанные фирмой АНКАД устройства для работы со смарт-картами, функции которых приведены в табл. 7.2.

**Адаптер смарт-карт SA-101i** предназначен для чтения и записи информации на смарт-картах. Адаптер подключается к УКЗД КРИПТОНи позволяет вводить в него ключи шифрования, хранящиеся на смарт-карте пользователя.

На одной смарт-карте могут быть размещены:

1. таблица заполнения блока подстановок УЗ (ГОСТ28147-89);
2. главный ключ шифрования;
3. секретный и открытый ключи электронной цифровой подписи

(ЭЦП ) пользователя;

1. открытый ключ ЭЦП сертификационного центра;
2. идентификатор пользователя системы защиты от несанкционированного доступа КРИПТОН -ВЕТО.

Адаптер SA-101i выпускается во внутреннем исполнении и легко встраивается в персональный компьютер на свободное место, предназначенное для дисковода.

Таблица 7.2 Устройства для работы со смарт-картами

|  |  |  |
| --- | --- | --- |
| Наименование | Описание |  |
| SA-101i  (Адаптер смарт-карт) | Запись/чтение информации на/с смарт-карты  EEPROM (протокол I2C). Интерфейс с УКЗД серии КРИПТОН, обеспечивающий прямую загрузку ключей в устройство |  |
| SCAT-200  (Контроллер  смарт-карт) | Шифрование по ГОСТ 28147-89, DES.  Память для хранения одного мастер-ключа.  Генерация случайных чисел.  Запись/чтение информации на/с смарт-карты.  Протоколы карт: I2C, GPM, ISO 781C Т= 0.  Интерфейс RS-232 с компьютером и  специализированный интерфейс с УКЗД серии КРИПТОН |  |
| SR-210  (Контроллер  смарт-карт) | Запись/чтение информации на/с смарт-карты.  Протоколы карт: I2C, GPM, ISO 7816 Т= 0, Т= 1.  Интерфейс RS-232 с компьютером и  специализированный интерфейс с УКЗД серии КРИПТОН |  |

**Универсальный контроллер смарт-карт SCAT-200** предназначен для работы со смарт-картами. Контроллер SCAT-200 может подключаться как к УКЗД, так и к интерфейсу RS-232. Наиболее важными представляются следующие функции контроллера:

1. запись информации на смарт-карту;
2. чтение информации со смарт-карты;
3. шифрование по ГОСТ28147-89 и DES;
4. хранение секретных ключей (так же, как в плате КРИПТОН -4);
5. генерация случайной последовательности;
6. набор на клавиатуре PIN-кода.

В контроллере могут применяться электронные карточки:

1. открытая память (протокол I2C);
2. защищенная память (серия GPM);
3. микропроцессорные карты (PCOS).

Универсальный контроллер SCAT-200 позволяет строить информационные системы на базе смарт-карт, что делает его полезным для систем:

1. безналичных расчетов (дебетно/кредитные карты);
2. контроля доступа (хранения прав доступа);
3. хранения конфиденциальной информации (медицина, страхование,

финансы);

1. защиты информации (хранения идентификаторов, паролей и ключей шифрования).

Контроллер может использоваться в компьютерах, электронных кассовых аппаратах, электронных замках, торговых автоматах, бензоколонках, платежных терминалах на базе IBM-совместимых компьютеров. Контроллер SCAT-200-совместный продукт фирмы АНКАД и АО "Скантек".

**Универсальный контроллер смарт-карт SR-210** имеет те же возможности, что и SCAT-200, за исключением функций шифрования и генерации случайных последовательностей. Контроллер совместим с российскими интеллектуальными микропроцессорными карточками.

**Лекция 16**

**Программные эмуляторы функций шифрования устройств КРИПТОН**

Для программной эмуляции функций шифрования УКЗД серии КРИПТОН разработаны и применяются:

1. программа шифрования Crypton LITE для работы в среде MS-DOS;
2. эмулятор Crypton Emulator для ОС Windows 95/98/NT.

**Программа шифрования Crypton LITE** предназначена для криптографической защиты (шифрования) информации, обрабатываемой ПЭВМ типа IBM PC/XT/AT 286, 384,486, Pentium в среде MS-DOS 3.0 и выше по алгоритму ГОСТ 28147-89.

Программа Crypton LITE полностью совместима с устройствами серии КРИПТОН , обеспечивающими гарантированную защиту информации. Crypton LITE и устройства серии КРИПТОН используют общее программное обеспечение.

Программа Crypton LITE рекомендуется для применений в компьютерах, где использование устройств КРИПТОН затруднено из-за конструктивных особенностей (например, в notebook). Crypton LITE применяется не только для защиты информации в компьютерах различного конструктивного исполнения, но и как средство поддержки при написании и отладке специализированного программного обеспечения к устройствам серии КРИПТОН .

Основные характеристики программы Crypton LITE:

Алгоритм шифрования ГОСТ 28147-89

Скорость шифрования “память-память” до 3 Мбайт/ с (для Pentium-2)

Необходимая оперативная память 2,5…8 Кбайт

Длина ключа 256 бит

Ключевая система 3-уровневая

Программа Crypton LITE реализует все режимы алгоритма ГОСТ 2814789:

1. режим простой замены;
2. режим гаммирования;
3. режим гаммирования с обратной связью;
4. режим вычисления имитовставки (имитоприставки).

Crypton LITE имеет встроенный датчик случайных чисел, используемый для генерации ключей. В программе Crypton LITE используются следующие ключевые элементы: К1 - первичный или файловый ключ (ключ данных), применяемый непосредственно для шифрования данных; К2 - вторичный ключ, применяемый для шифрования первичного ключа (в зависимости от используемой ключевой системы в качестве К2 выступают пользовательский ключ или сетевой ключ); ГК (или КЗ)-главный ключ (мастер-ключ), применяемый для шифрования других ключей; УЗ-узел замены, представляющий собой несекретный элемент, определяющий заполнение блока подстановки в алгоритме шифрования ГОСТ 28147-89.

Главный ключ и узел замены называют базовыми ключами. Базовые ключи загружаются при запуске программы Crypton LITE.

Дискета пользователя, на которой записаны базовые ключи ГК и УЗ, является ключом ко всей шифруемой информации. Для ключевой дискеты должен быть обеспечен специальный режим хранения и доступа. Следует отметить, что ГК может быть защищен от злоумышленников паролем (на случай потери ключевой дискеты).

Ключи К1 и К2 могут вводиться в программу Crypton LITE в любое время. В зашифрованном виде ключи К1 и К2 могут свободно храниться на внешних носителях и передаваться по каналам связи.

Открытый программный интерфейс программы Crypton LITE позволяет внедрять ее в любые системы без затруднений, а также разрабатывать дополнительное программное обеспечение специального назначения для защиты информационных и финансовых, биржевых и банковских коммуникаций, баз данных и других массивов компьютерной информации.

Программные продукты фирмы АНКАД, совместимые с Crypton LITE, позволяют:

1. прозрачно шифровать логические диски;
2. разграничить доступ к компьютеру;
3. осуществлять цифровую подпись электронных документов;
4. передавать зашифрованную информацию по открытым каналам связи.

**Программный эмулятор Crypton Emulator** обеспечивает криптографическое преобразование данных по алгоритму шифрования ГОСТ 28147-89 в компьютере, работающем под управлением ОС Windows 95/98/NT. Основная задача данной программы заключается в эмуляции шифровальных функций устройств криптографической защиты данных серии КРИПТОН .

Для работы программы необходима операционная система Windows 95/98/NT 4.0. Перед установкой драйвера-эмулятора на компьютер необходимо установить программный интерфейс Crypton API версии 2.1 и выше. Никаких особых требований к компьютеру не предъявляется-драйвер-эмулятор будет работать на любом компьютере, где установлены вышеназванные ОС.

Win32-nporpaммыi могут обращаться к функциям драйвера-эмулятора с помощью программного интерфейса Crypton API. Драйвер-эмулятор обеспечивает также возможность использования прерывания Ох4С в DOSсессии Windows 95/98 или Windows NT 4.0. Драйвер-эмулятор находится на уровне ядра операционной системы, и все запросы на шифрование или расшифрование проходят через него при отсутствии в компьютере платы шифрования.

Входными данными для драйвера-эмулятора являются главный ключ (мастер-ключ) и узел замены (секретный элемент, определяющий заполнение блока подстановки в алгоритме ГОСТ 28147-89). Для инициализации драйвераэмулятора необходимо загрузить базовые ключи ГК и УЗ с защищенной ключевой дискеты. Эта загрузка выполняется с помощью специальной утилиты, поставляемой вместе с драйвером-эмулятором. В зависимости от применяемой операционной системы обмен данными между приложением Win32 или DOS и драйвером-эмулятором ведется двумя разными способами.

Рассмотрим, в частности, особенности обмена данными в Windows NT. При обращении приложения Win32 к драйверу-эмулятору запрос от приложения Win32 проходит три уровня:

1. уровень приложений;
2. уровень, обеспечивающий интерфейс приложений с драйвером;
3. уровень ядра ОС.

Драйвер эмулирует работу платы шифрования, т.е. каждое Win32пpилoжeниe имеет собственную виртуальную плату шифрования со своими ключами К1 и К2, однако ГК и УЗ являются общими для всех приложений.

Программные продукты фирмы АНКАД, совместимые с Crypton Emulator, позволяют эффективно решать разнообразные задачи защиты информации в компьютерных системах и сетях.

**Системы защиты информации от несанкционированного доступа Система криптографической защиты информации от НСД КРИПТОН –ВЕТО**

Система предназначена для защиты ПК с процессором не ниже 386, работающего под управлением MS DOS 5.0 и выше, Windows 3.1. Персональный компьютер при этом может использоваться в качестве:

* + 1. абонентского пункта;
    2. центра коммутации пакетов;
    3. центра выработки ключей.

Система ограничивает круг лиц и их права доступа к информации на персональном компьютере. Ее реализация основана на технологиях "прозрачного" шифрования логических дисков по алгоритму ГОСТ 28147-89 и электронной цифровой подписи по ГОСТ 34.10/11-94. Согласно требованиям ГТК России ее можно отнести к СЗ НСД класса 1В-1Б. (Сертификат №178 от 29 апреля 1998 г. на соответствие классу 1В, выдан ГТК при президенте Российской Федерации. Система также передана на сертификацию в ФАПСИ .)

В состав основных функций системы КРИПТОН -ВЕТО включены следующие (рис. 7.2):

* обеспечение секретности информации в случае кражи "винчестера" или ПК ;
* обеспечение защиты от несанкционированного включения компьютера;
* разграничение полномочий пользователей по доступу к ресурсам компьютера;
* проверка целостности используемых программных средств системы в момент включения системы;
* проверка целостности программы в момент ее запуска на выполнение;
* запрещение запуска на выполнение посторонних программ;
* ведение системного журнала, регистрирующего события, возникающие в системе;
* обеспечение "прозрачного" шифрования информации при обращении к защищенному диску;
* обнаружение искажений, вызванных вирусами, ошибками пользователей, техническими сбоями или действиями злоумышленника.

Основным аппаратным элементом системы являются серийно выпускаемые аттестованные ФАПСИ платы серии КРИПТОН , с помощью которых проверяется целостность системы и выполняется шифрование по ГОСТ 28147-89. Система предполагает наличие администратора безопасности, который определяет взаимодействие между управляемыми ресурсами:

1. пользователями;
2. программами;
3. логическими дисками;
4. файлами (дискреционный и мандатный доступ);
5. wpgD9принтером;
6. дисководами.

Рисунок 7.2 – Структура системы КРИПТОН -ВЕТО

Система обеспечивает защиту следующим образом. Жесткий диск разбивается на логические диски. Первый логический диск (С:) отводится для размещения системных программ и данных; последний логический диск-для размещения СЗИ НСД и доступен только администратору. Остальные логические диски предназначены для хранения информации и программ пользователей. Эти диски можно разделить по пользователям и/или по уровню секретности размещаемой на них информации. Можно выделить отдельные диски с информацией различного уровня секретности (доступ к таким дискам осуществляется с помощью специальной программы, проверяющей допуск пользователя к документам-файлам). Сначала администратор устанавливает уровень секретности диска, а затем определяет круг лиц, имеющих доступ к этому диску. По форме хранения информации диски подразделяются на открытые и шифруемые; по уровню доступа - на доступные для чтения и записи, доступные только для чтения, недоступные (заблокированные).

Недоступный диск делается невидимым в DOS и, следовательно, не провоцирует пользователя на несанкционированный доступ к нему. Доступный только для чтения диск можно использовать для защиты не только от целенаправленного, но также от непреднамеренного (случайного) искажения (удаления) информации. Открытый диск ничем не отличается от обычного логического диска DOS. Очевидно, что системный диск должен быть открыт. Для шифруемых дисков используется шифрование информации в прозрачном режиме. При записи информации на диск она автоматически шифруется, при чтении с диска автоматически расшифровывается. Каждый шифруемый диск имеет для этого соответствующий ключ. Последнее делает бесполезными попытки улучшения своих полномочий пользователями, допущенными на ПК , поскольку они не имеют ключей доступа к закрытым для них дискам. Наличие шифрования обеспечивает секретность информации даже в случае кражи жесткого диска.

Для допуска к работе на ПК администратором формируется список пользователей, в котором:

1. указывается идентификатор и пароль пользователя;
2. определяется уровень допуска к секретной информации;
3. определяются права доступа к логическим дискам.

В дальнейшем только администратор может изменить список пользователей и их полномочия.

Для исключения возможности установки на ПК посторонних программ с целью взлома защиты администратор определяет перечень программ, разрешенных к запуску на данном компьютере. Разрешенные программы подписываются администратором электронно-цифровой подписью (ЭЦП ). Только эти программы могут быть запущены в системе. Использование ЭЦП одновременно с наличием разрешения позволяет отслеживать целостность запускаемых программ. Последнее исключает возможность запуска измененной программы, в том числе и произошедшего в результате непредвиденного воздействия "вируса".

Для входа в компьютер используются ключи, записанные на ключевой дискете, смарт-карте или на устройстве Touch-Memory. Ключи изготавливаются администратором системы и раздаются пользователям под расписку.

Для исключения загрузки компьютера в обход СЗ НСД загрузка осуществляется только с жесткого диска. При включении ПК (до загрузки операционной системы) с "винчестера" аппаратно проверяется целостность ядра системы безопасности КРИПТОН -ВЕТО, системных областей "винчестера", таблицы полномочий пользователей. Затем управление передается проверенному ядру системы безопасности, которая проверяет целостность операционной системы. Расшифрование полномочий пользователя, ключей зашифрованных дисков и дальнейшая загрузка операционной системы производятся лишь после заключения о ее целостности. В процессе работы в ПК загружены ключи только тех дисков, к которым пользователю разрешен доступ.

Для протоколирования процесса работы ведется журнал. В нем регистрируются следующие события:

1. установка системы КРИПТОН -ВЕТО;
2. вход пользователя в систему (имя, дата, время);
3. попытка доступа к запрещенному диску (дата, время, диск);
4. зашифрование диска;
5. расшифрование диска;
6. перешифрование диска;
7. добавление нового пользователя;
8. смена полномочий пользователя;
9. удаление пользователя из списка;
10. сброс причины останова системы;
11. попытка запуска запрещенной задачи;
12. нарушение целостности разрешенной задачи и т.д.

Журнал может просматриваться только администратором. Для проверки работоспособности системы используются программы тестирования. При необходимости пользователь может закрыть информацию на своем диске и от администратора, зашифровав последнюю средствами абонентского шифрования.