ЛЕКЦИЯ 18

Особенности программно-аппаратной реализации криптографической защиты компьютерных сетей и сетей связи

18.1. Проходные шифраторы: структура и программное обеспечение

18.1.1.Функциональные возможности и структура проходного шифратора

18.1.2. Загрузка ключей шифрования

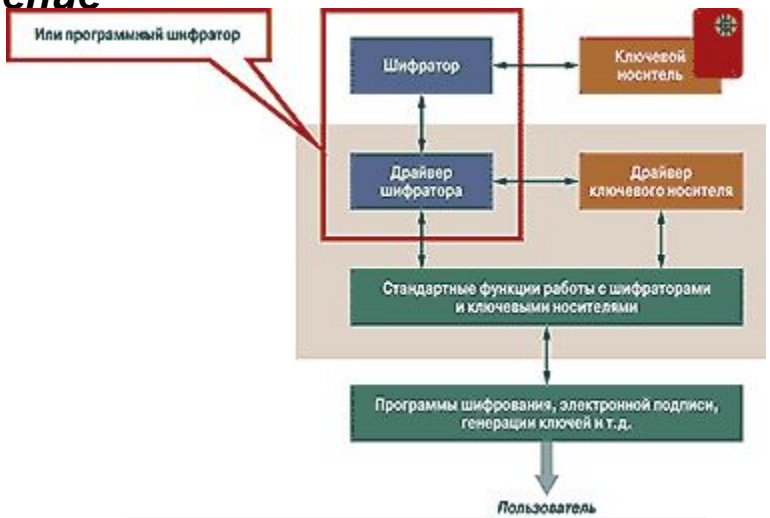
18.1.3. Взаимодействие шифратора с программами компьютера

18.1.4. Прикладное программное обеспечение

18.2. Организация криптозащиты информации при ее передаче по каналам телефонной, мобильной и специальной связи

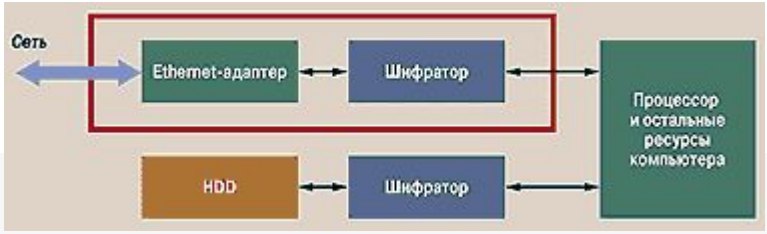
18.3. Специализированные шифраторы.

Проходные шифраторы: структура и программное обеспечение



Структура проходных шифраторов

Взаимодействие шифратора с программами компьютера



Программный интерфейс для шифратора

УКЗД выполняет *два* принципиально разных вида команд:

- перед загрузкой операционной системы - команды, ***зашитые в память шифратора***.

Они осуществляют все необходимые проверки и устанавливают требуемый уровень безопасности - допустим, отключают внешние устройства.

- после загрузки, например, *Windows* - команды, ***поступающие через модуль управления шифраторами***: шифровать данные, перезагружать ключи, вычислять случайные числа и т. д.

Прикладное программное обеспечение

Любая программа защиты информации должна соответствовать, **как минимум,** одной из следующих характеристик:

- Автоматическое и незаметное для пользователя выполнение – для программ *прозрачного шифрования* и средств построения ***VPN***.

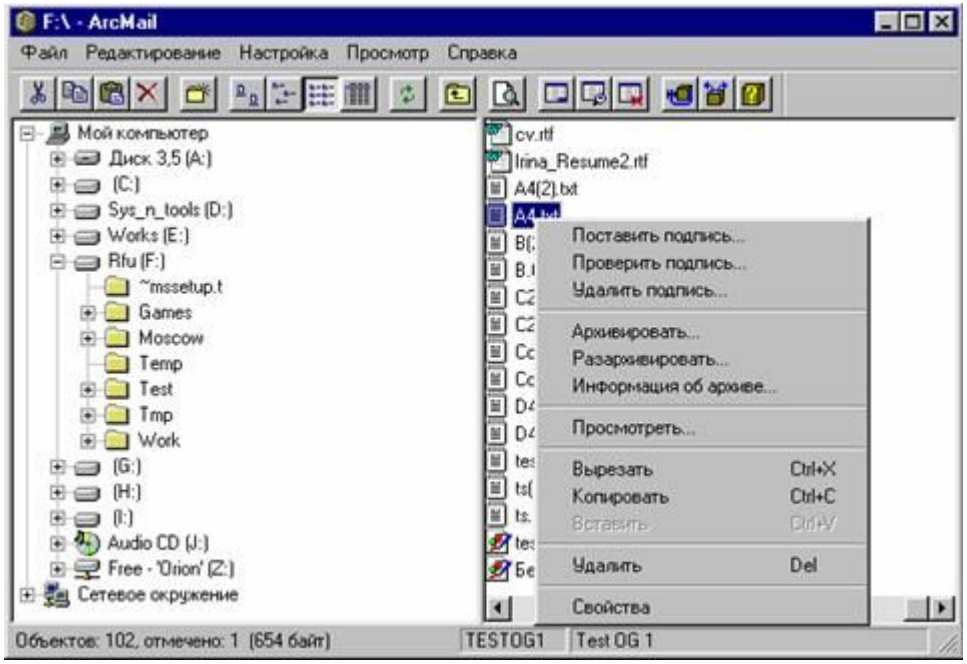
- Дублирование возможностей стандартных программ типа *Windows Explorer* («*Проводник*») – позволяет выполнять все действия с файлами и папками на диске, *не выходя* из программы защиты информации.

Встраивание функций защиты в известные и широко применяемые продукты: расширения меню (***Shell Extensions***) ***Windows Explorer***, дополнительные панели инструментов в ***Microsoft Word*** и ***Microsoft Excel***, автоматический перехват событий в ***Microsoft Outlook*** и т.д.

Пример средства защиты, дублирующего основные функции ***Windows Explorer***,

- специализированный архиватор (программа, выполняющая ***специализированное архивирование***: вычисление ***ЭЦП*** информации, ее ***сжатие*** и **зашифрование**)

Crypton ArcMail.



Главное окно специализированного архиватора ***Crypton ArcMail***.

Программные продукты *Crypton* обладают следующими характеристиками:

- Они имеют ***сертификаты ФАПСИ*** или используют в своем составе сертифицированное ФАПСИ *криптоядро*.

- Практически все продукты выпускаются в ***двух вариантах***: полнофункциональная версия **администратора** и версия *пользователя*, позволяющая выполнять ограниченный набор функций.

- Выполняют ***автоматическое протоколирование*** операций.

- Существуют также в виде ***библиотек функций для встраивания***.

- Имеют ***различные ключевые системы***, позволяющие клиенту выбрать наиболее оптимальную для конкретных задач.

- Поддерживают ***совместимость по форматам*** с предыдущими версиями, что позволяет осуществлять **постепенное обновление** программного обеспечения – *это особенно актуально для крупных организаций, имеющих территориально-распределенную структуру.*

- Продукты являются ***взаимозаменяемыми*** и ***совместимыми*** между собой по **основным** форматам, например, ***Crypton Word, Crypton Excel*** и ***Crypton Outlook*** полностью совместимы как между собой, так и со всеми продуктами серии ***Crypton ArcMail.***

Организация криптозащиты информации при ее передаче по каналам телефонной, мобильной и специальной связи

Основные характеристики *КриптоСмартТелефона*

Категория	Параметры и состав	Особенности и возможности
Общие характеристики	***Принцип передачи***	Радиомодем стандарта 900/1800 МГЦ
	Режимы работы	шифрование голоса в полнодуплексном режиме, стандартный режим GSM, шифрование SMS, шифрование данных в телефоне, шифрование и передача электронной почты
	Процессоры: ***- основной,*** ***- шифрующий***	Моторола MX21 266 M, TMS 320 VC 5416
Криптографические характеристики	***Криптоалгоритм***	Симметричный, 256 бит
	Метод распределения ключей	Открытый ключ + Общий ключ (формируется для каждого сеанса)
	Ключевая мощность	10^{77}

Сравнительные характеристики **персональных шифраторов**

Персональный шифратор	**Разработчик**	**Алгоритм шифрования**	**Назначение**	**Носитель ключевой информации**	**Примечание**
Шифратор, встроенный в специальный сотовый телефон ***SMP-Атлас***	ФГУП **“НТЦ “Атлас”** + концерн **“Гудвин”**	ГОСТ **28147-89**	***гарантированная*** защита информации, передаваемой по сетям ***GSM***	российская **интеллектуальная карта РИК** (микросхема **КБ5004ВЕ1**)	персональный **шифратор**, встроенный в мобильный радиотелефон
Шифратор, встроенный в ***Крипто Смарт Телефон***	ЗАО **“АНКОРТ”**	симметричный, **256 бит**	***гарантированная*** защита информации, передаваемой по сетям ***GSM***	**Шифропроцессор** на основе **TMS VC 5416**	персональный **шифратор**, встроенный в мобильный радиотелефон
Шифратор, встроенный в специальный сотовый телефон ***Талисман-GSM***	НИИ **“КВАНТ”**	ГОСТ **28147-89**	криптозащита речевой информации в каналах ***GSM 900/1800***	микропроцессор	аппаратный **шифратор** - гарнитура к телефону с поддержкой ***Bluetooth***
Устройство защиты информации ***Шипка-1.5***	ОКБ “**САПР**”	ГОСТ **28147-89**, ГОСТ **Р 34.10-94,** ГОСТ **Р 34.10-2001**, ГОСТ **Р 34.11-94**	***гарантированная*** защита информации и информационных технологий	микропроцессор	защищенная ***энерго-независимая*** память до **2 Мб**
Персональный идентификатор ***ruToken RF***	ЗАО “**Актив**”	ГОСТ **28147-89**	хранение ключевой информации, контроль доступа к ресурсам ПК и в помещения	***USB***-брелок	полнофункциональный аналог **смарт-карты** + ***радиочастотная метка***

Телефонный скремблер "Грот"

предназначен для защиты **конфиденциальной** информации и обеспечивает шифрование *речевого сигнала* и защиту ***факсимильных сообщений***, передаваемых по телефонной сети общего применения.

Характеристики работы в канале связи и пользовательские свойства:

• напряжение постоянного тока в абонентской линии: 30…60 В;
• ***высокая*** помехоустойчивость;
• ***автоматическая адаптация*** к телефонному аппарату абонента, абонентской линии, нелинейности трактов АТС;
• ***устойчивость работы*** в реальных телефонных каналах России и стран СНГ, включая междугородные и международные каналы с радиорелейными вставками и *любыми* видами уплотнения;
• ***совместимость с любым типом*** телефонного и факсимильного аппарата, с мини-АТС любого типа, имеющей аналоговый выход;
• работа в линиях, оборудованных системами уплотнения и используемых для охранной сигнализации;
• высокая степень ***эхокомпенсации***;
• ***низкий уровень шумов*** в телефонной трубке;
• ***высокое качество*** восстановленной речи;
• ***энергонезависимая память*** индивидуальных ключей-идентификаторов;
• упрощенный алгоритм ввода индивидуальных ключей-идентификаторов за счет использования ***электронного блокнота индивидуальных ключей.***

Шифрование:

• метод шифрования – **мозаичный**: ***частотные*** и *временные* перестановки;
• метод **открытого распределения** ключей, позволяющий работать без ручного набора ключей;
• общее количество ключевых комбинаций - **2 × 1018**;
• возможность введения ***дополнительного семизначного ключа*** для идентификации абонента;
• высокая степень криптографической защиты за счет наличия дополнительных **мастер-ключей,** которые устанавливаются по желанию Заказчика.

***Аппаратура криптографической защиты речевой и документальнойинформации с гарантированной стойкостью* E-20** обеспечивает:

• режим ***телефонного аппарата общего пользования***;
• режим ***криптографической защиты речи***;
• режим ***передачи и криптографической защиты данных со встроенным устройством имитозащиты.***

Работа в закрытом режиме осуществляется при установленном ключевом носителе **Data Key.**

Аппаратура M459-1C предназначена для криптографической защиты**конфиденциальной** и секретной ***телефонной*** и ***документальной*** информации и обеспечивает:

• работу по ***выделенным*** и ***предварительно коммутированным*** каналам связи совместно с модемом ***УПС-ТФ*** в *дуплексном* режиме на скоростях ***2400, 4800, 9600 бит/с;***
• работу по ***предварительно коммутированным*** телефонным каналам общего пользования для *встречной* работы с аппаратурой ***E-20***;
• передачу/прием ***документальной*** информации от **ПЭВМ** через аппаратуру ***Адаптер-ДС.***

Шифратор **КРИПТОН AncNet**, совмещенный с сетевой картой ***Ethernet.***

Шифратор **КРИПТОН-IDE** для прозрачного шифрования жестких дисков интерфейса ***IDE.***

Шифрует по алгоритму ГОСТ **28147-89** со скоростью до ***70 Мбит в секунду***.

Для *управления работой* данных шифраторов предназначен
аппаратно-программный модуль доверенной загрузки (АПМДЗ) **КРИПТОН-ЗАМОК.**
Выполняет следующие функции:

- **Контроль целостности модулей** операционной системы компьютера перед его загрузкой.
- **Аутентификация** пользователей.
- **Контроль** и **блокировка доступа** к жестким дискам и дисководам компьютера, а также к устройствам чтения компакт-дисков.
- **Контроль доступа** к портам компьютера, а также к сетевым адаптерам.

Аппаратный шифратор «М-506» -
СКЗИ (*Система криптографической защиты информации*) **М-506**

состоит из компонентов:
· **сервер безопасности -** устанавливается на *выделенном* компьютере или *контроллере домена;* собирает и обрабатывает информацию о состоянии всех защищаемых рабочих станций и хранит данные о настройках всей системы защиты;

· **средство защиты информации от несанкционированного доступа (СЗИ)** ***Secret Net NT 4.0.***

· **подсистема управления -** устанавливается на рабочем месте администратора системы и позволяет *конфигурировать* **СЗИ *Secret Net***, *контролировать* все события, влияющие на защищенность системы, и реагировать на них в режиме ***реального времени*** и в терминах реальной предметной области *(сотрудник, задача, подразделение, помещение);*

· **криптоменеджер -** устанавливается на ***автономном компьютере*** и выполняет функции:
создание ключей шифрования,
изготовление ключевых дискет,
ведение базы созданных ключей на жестком диске компьютера.

Все компоненты ***СКЗИ М-506*** функционируют в замкнутой программной среде, *недоступной* воздействию вирусов.

Средства криптографической защиты информации "Верба-О","Верба-ОW"
решают задачи:

• **шифрование/расшифрование** информации на уровне ***файлов***;
• генерация **электронной цифровой подписи** ;
• **проверка ЭЦП**; обнаружение ***искажений***, вносимых злоумышленниками или вирусами в защищаемую информацию.

Программные продукты и *аппаратно-программные средства* "***Верба***" классифицируются следующим образом:

• **библиотечные модули**, предназначенные для вызова криптографических функций непосредственно из ***приложения***, осуществляющего обработку конфиденциальной информации. Обеспечивают **шифрование** и **ЭЦП** (программный модуль "***VCrypt***");
• средства **криптографической защиты данных** пользователя, предназначенные для **электронной подписи** и **шифрования** данных пользователей на рабочих местах с возможностью последующего хранения и передачи по каналам связи ***("Файловый криптоменеджер");***
• средства **криптографической защиты клиент-серверных технологий**, предназначенные для использования в системах типа "***клиент-сервер***" и имеющие в своей основе ***принцип раздельного функционирования*** *систем обработки запросов* и систем криптографической защиты информации ("***Криптографический сервер***");
• средства **криптографической защиты каналов связи**, предназначенные для защиты информации в каналах связи в режиме ***on-line*** по протоколам ***IP, X.25, Fray Relay*** и т.д.
• защищенные **почтовые технологии**, предназначенные как для организации собственных *защищенных почтовых систем* на базе **X.400**, так и для организации *защищенного документооборота* через ***Internet*** - приложения.