Министерство связи и массовых коммуникаций Российской Федерации

Государственное образовательное учреждение
высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара

Федеральное агентство связи

Государственное образовательное учреждение высшего профессионального образования

Поволжская государственная академия телекоммуникаций и информатики

Кафедра передачи дискретных сообщений

Методические указания к лабораторной работе

ИЗУЧЕНИЕ ПРОГРАММНОГО СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ СЕРИИ КРИПТОН

для студентов, обучающихся по специальностям 210403,210404,210406

Составители: к.т.н., доцент Крыжановский А.В.

к.т.н., доцент Киреева Н.В.

к.т.н., доцент Пугин В.В.

Редактор: д.т.н., профессор Лихтциндер Б.Я.

Рецензент: д.т.н., профессор Карташевский В.Г

Самара 2008

Создание защищенного документа

Цель работы: *Изучить принципы работы «Crypton Word», «Crypton Excel», понять процедуры шифрования/дешифрования электронных документов, постановки электронной цифровой подписи (ЭЦП).*

Методические указания к выполнению лабораторной работы:

1. Проверить наличие ключа Novex Stealth в порте LPT на задней панели системного блока. Выполнить настройку эмулятора Crypton
2. Открыть программу MS Word.
3. Создать новый электронный документ или открыть любой имеющийся. Создать защищённый документ и поставить ЭЦП.
4. Ознакомиться с работой ПО мастер ключей шифрования
5. Ознакомиться с программой тестирования функций приложения Crypton API
6. Получить навыки работы с Crypton Disk

Настройка эмулятора производится с помощью ярлыка «Конфигурация драйвера-эмулятора», доступного через главное меню Windows. С помощью данного ярлыка вызывается программа конфигурирования эмулятора “drvsetup.exe”, находящаяся в каталоге установки эмулятора.

Главное окно программы показано на рис. 1:

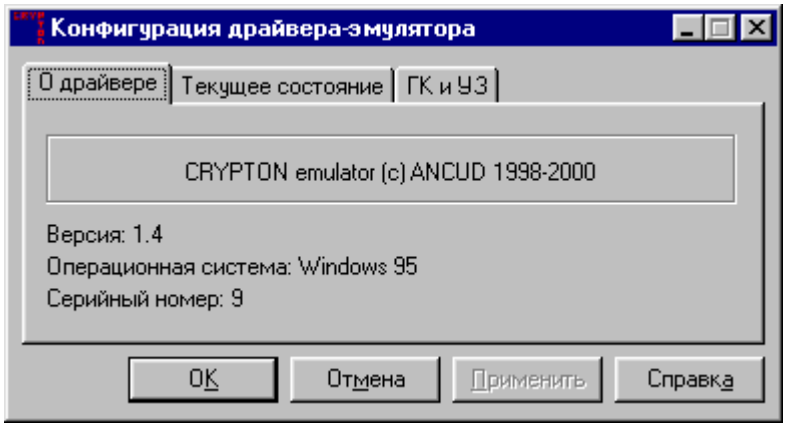


Рисунок 1 - Главное окно программы конфигурирования эмулятора

Данное окно имеет три вкладки:

1) «О драйвере» (см. рис. 1). На данной вкладке содержится информация об используемом экземпляре эмулятора:

- установленная версия эмулятора;
- используемая операционная система;
- серийный номер эмулятора.

2) «Текущее состояние». На данной вкладке содержится информация о количестве открытых сессий работы эмулятора, т. е., используется ли эмулятор в текущий момент и сколько приложений его использует. Кроме того, на данной вкладке содержится информация о состоянии защиты от копирования данного экземпляра эмулятора.

3) «ГК и УЗ» (см. рис. 2). Данная вкладка служит для указания местонахождения ключей инициализации эмулятора, а также для их загрузки и выгрузки. Назначение ключей инициализации и порядок работы с ними описаны ниже.

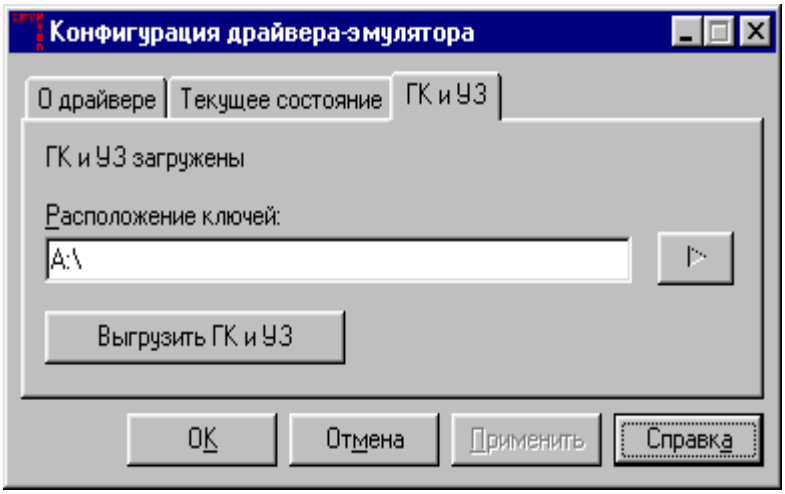
Главное окно программы конфигурации эмулятора имеет также следующие кнопки:

1) «ОК». Записывает измененную конфигурацию эмулятора (если были сделаны изменения) и завершает работу программы.

2) «Отмена». Завершает работу программы без записи изменений.

3) «Применить». Записывает изменения конфигурации и позволяет продолжить работу с программой конфигурации эмулятора.

4) «Справка». Вызывает справочную информацию об эмуляторе.



Единственный параметр конфигурации, который можно изменить с помощью программы конфигурации эмулятора, - это расположение Главного ключа (ГК) и узла замены (УЗ). Данные ключевые элементы используются эмулятором для выполнения криптографических функций и должны быть загружены в эмулятор до начала выполнения каких-либо криптографических функций.

Для изменения каталога расположения ГК и УЗ предназначена вкладка «ГК и УЗ» программы конфигурации эмулятора (см. рис. 2). Данная вкладка содержит следующие дополнительные элементы:

1) Поле для ввода каталога расположения ГК и УЗ.

2) Кнопка для выбора каталога расположения ГК и УЗ с помощью стандартных диалоговых окон (справа от поля ввода каталога).

3) Кнопка для загрузки и выгрузки ГК и УЗ. Название данной кнопки меняется в зависимости от того, инициализирован ли эмулятор, и может быть одним из следующих:

- «Загрузить ГК и УЗ» – если ГК и УЗ еще не загружены (эмулятор не инициализирован). При нажатии на данную кнопку происходит загрузка ГК и УЗ (процесс загрузки подробно описан ниже).
- «Выгрузить ГК и УЗ» – если эмулятор уже проинициализирован. В этом случае ключи ГК и УЗ выгружаются и для дальнейшей работы эмулятор необходимо проинициализировать снова.

Ключи ГК и УЗ хранятся на носителях информации в файлах “gk.db3” и “uz.db3” соответственно. Данная версия эмулятора разрешает использовать в качестве ключевых носителей только съемные носители информации, например, дискеты или смарт-карты.

Для создания защищенного документа следует нажать кнопку «Подписать и зашифровать» панели инструментов «Crypton Word». При этом в Microsoft Word должен быть открыт хотя бы один документ. Защищается ак-

тивный документ. В случае, если Microsoft Word не содержит активных документов, будет выдано сообщение об ошибке.

Кроме того, для создания защищённого документа программа потребует загрузить ключи ГК и УЗ. Для этого нужно вставить в дисковод дискету с хранимыми на ней ключами ГК и УЗ (у преподавателя). После этого появится диалоговое окно с предложением извлечь носитель.

Внимание: Категорически запрещается оставлять носитель с ГК и УЗ в дисководе!

В случае если текущий документ не сохранен, будет выдано сообщение с предложением сохранения документа. Нажатие кнопки «Отмена» в данном окне отменяет операцию создания защищенного документа. При выборе кнопки «Да» документ сохраняется, при выборе кнопки «Нет» сохранения документа не происходит; и в том, и в другом случае текущий документ закрывается, после чего на экран выводится окно создания защищенного документа (см. рис. 1)

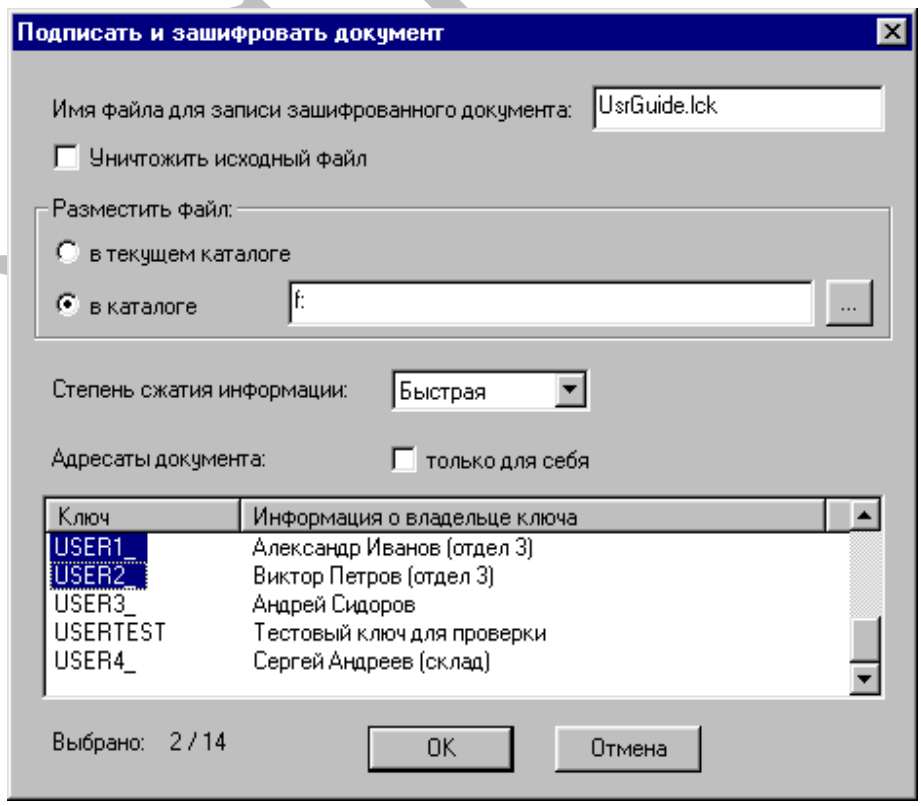


Рисунок 3 - Окно создания защищенного документа

Для создания защищенного документа необходимо выполнить следующие шаги:

1) Указать имя файла для его записи.
2) Выбрать каталог расположения создаваемого файла.
3) Выделить нужных абонентов с помощью мыши и клавиш «Ctrl» и «Shift». Выделение абонентов происходит таким же образом, как и выделение объектов в программе Windows Explorer.
4) Нажать «ОК».

Одновременно с зашифрованием на файлы будет устанавливаться электронная подпись для обеспечения последующего контроля целостности и авторства документа. Подписывается только копия исходного документа в оперативной памяти компьютера, исходный документ не изменяется.

После нажатия кнопки «ОК» начнется процесс создания защищенного документа. При этом на экран выводится окно, в котором показывается прогресс данного процесса. Окно прогресса содержит кнопку «Прервать», нажав на которую можно отменить процесс. При этом на экран выводится запрос подтверждения отмены операции.

В случае возникновения ошибки во время создания защищенного документа или отмены данной операции пользователю предлагается вернуться к редактированию защищаемого документа. При согласии пользователя документ будет открыт и станет активным документом Microsoft Word.

5) Открыть защищённый документ.

Для открытия защищенного документа следует нажать кнопку «Открыть защищенный документ» панели инструментов «Crypton Word». На экран будет выведено стандартное окно выбора файлов в Windows, в котором следует выбрать открываемый защищенный документ.

Результаты проверки подписи отображаются в окне, пример которого приведен на рис. 2.

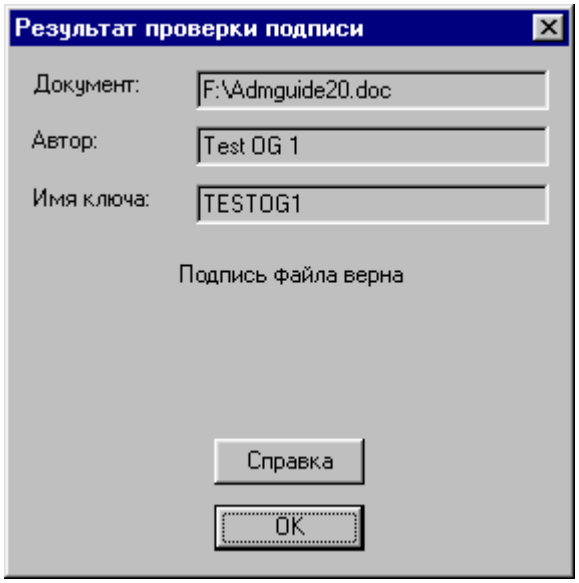


Рисунок 4 - Окно вывода результатов проверки подписи

В случае, если подпись документа является неверной, данное окно содержит также дополнительную информацию, почему подпись признана неверной. В этом случае в окне выводится следующее информационное сообщение:

«Внимание! Подпись документа неверна. Открывать все равно?»

В этом случае вместо кнопки «ОК» в окне присутствуют кнопки «Да» и «Нет». Документ будет открыт или нет в зависимости от нажатия одной из этих кнопок.

6) Открыть MS Excel.

7) Повторить п.3, п.4, п.5.

Приложение для CRYPTON WORD

Программный комплекс Crypton Word предназначен для встраивания в Microsoft Word шифрования и ЭЦП электронных документов по алгоритмам ГОСТ 28147-89 и ГОСТ Р 34.10/11-94 соответственно. Реализованный механизм шифрования и ЭЦП позволяет легко обеспечивать защиту электронных документов, как при их последующей передаче по сети, так и при их хранении на персональном компьютере.

Функции Crypton Word обеспечивают:

- сжатие документов;
- контроль целостности документов путем применения ЭЦП;

- конфиденциальность документов путем применения шифрования;
- установление авторства документа.

Комплекс не накладывает каких-либо ограничений на типы защищаемых документов. Возможно одновременное использование защиты с помощью Crypton Word и механизмов защиты, встроенных в Microsoft Word.

Комплекс Crypton Word предоставляет разнообразную справочную информацию, которая может быть получена как с помощью пунктов «Справка» или «Помощь» меню программ, так и с помощью кнопок «Справка» различных диалоговых окон. В последнем случае на экран выводится контекстная справочная информация, поясняющая работу именно в данном диалоговом окне, что наиболее удобно при работе с комплексом.

Комплекс Crypton Word предназначен для обеспечения защиты от несанкционированного доступа и контроля целостности документов при их хранении или передаче по открытым каналам связи.

Комплекс Crypton Word защищен от копирования путем привязки каждого экземпляра комплекса к конкретному серийному номеру УКЗД серии КРИПТОН или его программного эмулятора. При несовпадении номеров работа комплекса будет блокирована с выдачей соответствующего сообщения об ошибке.

Для работы с комплексом Crypton Word каждый пользователь должен иметь следующий комплект ключей:

Персональный секретный ключ	Уникальный ключ пользователя, с помощью которого пользователь ставит свою ЭЦП и шифрует документы. Хранится в файле с расширением sk.
Открытые ключи других пользователей	Необходимы для шифрования документов для конкретных пользователей (при шифровании используется пара ключей: свой секретный + чужой открытый) и для проверки их ЭЦП. Хранятся в файлах с расширением pk или в базе данных открытых ключей (БД ОК). БД ОК хранится в двух файлах с расширениями pkd и pkm.
Открытый ключ-сертификат	Необходим для проверки целостности открытых ключей других пользователей (во избежание их подмены). Хранится в файле с расширением pk.
Ключи инициализации УКЗД КРИПТОН или Crypton Emulator	Хранятся в файлах **uz.db3** и **gk.db3** (см. главу 3.4.1).

Секретный ключ необходимо хранить таким образом, чтобы он не был доступен кому-либо еще – иначе получивший ключ злоумышленник сможет ставить Вашу подпись и расшифровывать Вашу информацию. Открытый ключ-сертификат необходимо защитить от подмены. Каждому пользователю рекомендуется создать персональный ключевой носитель, на котором хранить следующую ключевую информацию:

- Секретный ключ пользователя.
- Открытый ключ-сертификат.
- Ключи инициализации **gk.db3** и **uz.db3**.

Персональным ключевым носителем может быть как дискета, так и любой другой носитель, поддерживаемый комплексом Crypton Word.

Секретный и открытый ключи пользователя генерируются фирмой АНКАД после оплаты экземпляра комплекса Crypton Word; в ключи записывается

персональная информация пользователя (выводится в окно проверки подписи в качестве информации об авторе документа – см. главу 3.2), если она была сообщена фирме АНКАД в процессе генерации ключа (в противном случае в качестве персональной информации записывается номер экземпляра комплекса).

Срок действия ключей пользователя – 3 месяца с момента их генерации. По истечении срока действия ключевой информации Вы можете заказать новый комплект ключей у фирмы АНКАД (сроком на 3, 6 или 12 месяцев с момента генерации) за дополнительную плату, сообщив свой номер и персональные данные. Новый комплект ключей может быть выслан Вам одним из следующих способов:

1) На дискете по почте или курьерской службой (оплачивается отдельно).
2) По e-mail, в зашифрованном виде. В качестве ключа шифрования используется Ваш текущий ключ (рекомендуется в этом случае заказывать ключи заблаговременно, до окончания срока действия Вашего ключа).

При активизации комплекса с помощью кнопок панели инструментов «Crypton Word» происходит считывание с ключевого носителя указанного в конфигурации секретного ключа. В случае отсутствия вставленного в устройство чтения ключевого носителя будет выдано сообщение с просьбой вставить ключевой носитель.

В том случае, если секретный ключ защищен паролем, будет запрошен его пароль; дальнейшая работа комплекса будет возможна только после корректного ввода пароля.

Окно создания защищённого документа содержит ряд элементов управления, позволяющих задать параметры создаваемого защищенного документа:

1) Поле "Имя файла для записи зашифрованного документа". В данном поле необходимо указать имя файла создаваемого защищенного документа. Crypton Word автоматически предлагает имя файла, пользователь может оставить это имя или отредактировать его вручную. Имя формируется по имени защищаемого документа (активного документа

Microsoft Word), расширение которого меняется на стандартное – «.lck» (рекомендуется). Если расширение файла не указано, добавляется стандартное расширение. В случае наличия в целевом каталоге файла с таким же именем будет выдан запрос на перезапись.

2) Переключатель «Уничтожить исходный файл». Если переключатель включен, то исходный документ уничтожается без возможности восстановления. ***Внимание!*** *При включении данного переключателя восстановить исходный файл будет невозможно. Включайте его только в том случае, если Вы уверены в необходимости уничтожения исходного документа.*
3) Группа элементов «Разместить файл». Управляет выбором местоположения будущего файла защищенного документа. Если выбран пункт «в текущем каталоге», то файл будет расположен в том же каталоге, где располагается защищаемый документ. Если выбран пункт «в каталоге», то следует также указать каталог расположения файла. По умолчанию в данное поле подставляется каталог, в котором был сохранен предыдущий защищенный документ. Каталог можно как указать вручную, так и выбрать с помощью кнопки обзора папок («…»), находящейся справа в данной группе элементов.
4) Поле «Степень сжатия информации». Управляет степенью сжатия защищаемых документов. Позволяет выбрать одну из трех степеней:
   - «нет сжатия»
   - «быстрая»
   - «сильная»
5) Группа элементов «Адресаты документа». Включает в себя список возможных адресатов документа. Выбранные из них смогут расшифровать данный защищенный документ (выбранные адресаты выделяются цветом). Допускается создание защищенного документа только для собственного использования. Для этого следует

включить переключатель «Только для себя»; в этом случае никто, кроме

Вас, не сможет расшифровать документ.

Список адресатов документа активен только в том случае, если переключатель «Только для себя» выключен. При включении переключателя «Только для себя» выбор адресатов в списке сбрасывается.

6) Поле «Выбрано». Динамически отображает количество выбранных адресатов и количество доступных адресатов.

Исходные значения переключателей «Уничтожить исходный файл», «Только для себя», полей «Разместить файл» и списка степеней сжатия информации устанавливаются аналогично их установке при формировании прошлого защищенного документа.

Для открытия защищенного документа следует нажать кнопку «Открыть защищенный документ» панели инструментов «Crypton Word».

После выбора файла Crypton Word выполняет следующие действия:

- Расшифрование документа.
- Разжатие документа, если при его создании производилось сжатие.
- Проверка подписи документа.

Окно вывода результата содержит следующую информацию:

- Имя файла открываемого документа.
- Информацию об авторе документа.
- Имя ключа, с помощью которого поставлена подпись.
- Результат проверки подписи.

Выполнение работы по Crypton Excel является аналогичным вышеизложенному материалу.

Теперь следует рассмотреть принцип работы ПО Crypton Шифрование Прежде всего выделим основные термины и понятия:

Зашифрование

Процесс преобразования открытых данных в закрытые (зашифрованные). В данном программном продукте используется алгоритм шифрования ГОСТ 28147-89. Это симметричный алгоритм, что означает, что для шифрования и расшифрования используется одинаковый ключ.

Расшифрование

Процесс преобразования закрытых данных в открытые (расшифрованные).

Ключ, ключевая система

Конкретное секретное значение криптографического преобразования, определяющее ход процесса преобразования данных. В данном пакете программ в качестве ключей шифрования могут использоваться:

* Ключ Пользователя;
* Сетевой ключ.

При работе с ключами всегда производится анализ имитоприставки.

Узел Замены (УЗ)

Долговременный элемент ключевой системы ГОСТ 28147-89. Обычно хранится в файле uz.db3 на ключевом носителе и является первым ключевым элементом, вводимым в устройство шифрования при инициализации. Все компьютеры, между которыми предполагается обмен зашифрованной информацией (например, локальная сеть), должны использовать один и тот же УЗ, т. к. несоответствие Узлов Замены приведет к невозможности расшифрования файлов с другой машины.

Главный Ключ (ГК)

Секретный ключ, используется для шифрования других ключей. Обычно хранится в файле gk.db3 на ключевом носителе. Может быть зашифрован на пароле. Создается администратором. При инициализации устройства шифрования загружается в него и находится там до выключения питания ЭВМ.

Пароль

Последовательность символов, вводимых с клавиатуры. Пароль защищает ключи от несанкционированного использования в случае их хищения или потери. Максимальная длина пароля для ключей шифрования - 37 символов. Минимальная длина - 4 символа. Длина пароля определяет стойкость системы. Поэтому рекомендуется использовать длинные пароли с неповторяющимися символами. Символы разных регистров (прописные и строчные буквы) разли-

чаются. Использовать символы с кодами меньше 32 и больше 127 (управляющие символы, псевдографику и русские буквы) не рекомендуется.

Ключ пользователя (ПК)

Секретный ключ, используется для шифрования файлов и других ключей. Хранится в файле с расширением ".KEY", обычно в зашифрованном виде.

Сетевой ключ

Секретный ключ, используется для шифрования файлов с целью передачи их между узлами криптографической сети. Все узлы сети нумеруются. Для каждого узла, с которым планируется обмен информацией, необходимо иметь свой сетевой ключ. Задача обеспечения сетевыми ключами возлагается на администратора сети. Сетевые ключи хранятся в Сетевом Наборе.

Имитовставка, имитоприставка

Применяется для обеспечения защиты системы шифрования от навязывания ложных данных. Имитовставка представляет собой отрезок информации фиксированной длины, полученный из открытых данных и ключа. Создается при зашифровании данных и добавляется к ним. При расшифровании данных также вычисляется имитовставка и сравнивается с хранимой. В случае несовпадения можно выделить следующие причины:

* изменен Узел Замены;
* изменен ключ, на котором были зашифрованы данные;
* изменены сами зашифрованные данные;
* если для зашифрования использовался пароль, то при расшифровании он был неверно введен;
* неисправно устройство шифрования.

Сетевая Таблица

Для обмена зашифрованной информацией между N узлами необходимо N*(N-1) ключей (каждый с каждым). Фактически, это таблица, где в заголовках строк и столбцов проставлены номера узлов, а в ячейках хранятся ключи. Эта матрица симметрична, т.е. ключ для передачи от узла А узлу Б (сетевой ключ А-Б) в точности равен сетевому ключу Б-А. Сетевая Таблица при создании за-

шифровывается на Ключе Сетевой Таблицы (КСТ).

Сетевой Набор

Из полной Сетевой Таблицы необходимо для каждого из узлов сформировать набор ключей для связи с другими узлами. Фактически, такой набор представляет собой одну из строк таблицы. Сетевой Набор хранится в файле NNNNN.SYS в каталоге сетевых ключей, где NNNNN - пятизначный десятичный номер данного узла. Он всегда зашифрован на Ключе Сетевого Набора (КСН), хранящемся в файле NNNNN.KEY в каталоге сетевых ключей. КСН получают вместе с Сетевым Набором от администратора криптографической сети. При получении КСН обычно незашифрован, поэтому рекомендуется перешифровать его.

Иерархическая структура ключей

В данной версии пакета программ КРИПТОН® Шифрование принята иерархическая структура ключей, показанная на рис. 3.

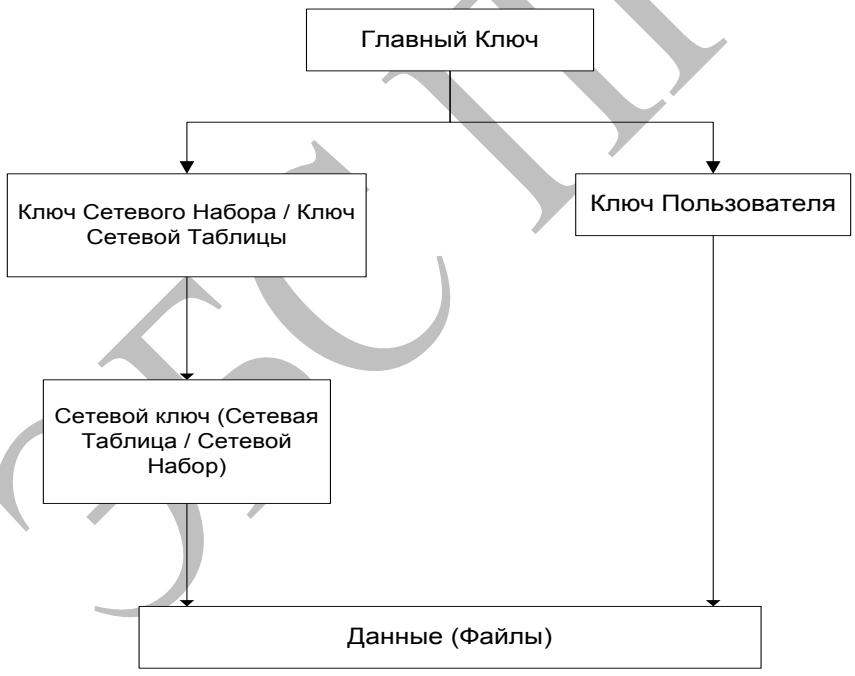


Рисунок 3 - Иерархическая структура ключей

Принципы шифрования

Шифрование файлов в данной системе может протекать по двум схемам: архивное шифрование файлов, обмен которыми не предполагается, и шифрование файлов для передачи в криптографической сети.

Архивное шифрование файлов

Генерируется так называемый ФАЙЛОВЫЙ (или СЕАНСОВЫЙ) КЛЮЧ. Это последовательность из 256 бит, получаемая с датчика случайных чисел устройства шифрования. Вся информация, содержащаяся в файле, шифруется на данном Файловом Ключе.

Так как расшифрование файла без этого Файлового Ключа невозможно, то он записывается в зашифрованный файл. При этом Файловый Ключ шифруется на ключах, указанных пользователем с вычислением имитоприставки.

Применение Файлового Ключа объясняется усилением криптографической устойчивости реализованного механизма шифрования, а также существенным ускорением операции перешифрования, поскольку исчезает необходимость перешифровывать весь файл, достаточно лишь перешифровать сам Файловый Ключ.

Шифрование файлов для передачи в криптографической сети

Файл данных, передаваемый узлом А узлу Б зашифровывается на Файловом (сеансовом) Ключе. Файловый Ключ создается автоматически при зашифровании файла данных и передается вместе с ним. Так как файловый ключ не может передаваться в открытом виде, то он зашифровывается на Сетевом Ключе А-Б. Этот ключ узел А берет из своего Сетевого Набора.

Сетевой Набор узла А зашифрован на Ключе Сетевого Набора (КСН) узла А, который, в свою очередь, тоже может быть зашифрован на каких либо ключах узла А (как правило, ГК).

Узел Б, по информации, заключенной в зашифрованном файле, понимает, что файл пришел от узла А. Используя свои ключи, узел Б расшифровывает свой КСН.

Затем, используя КСН, узел Б расшифровывает свой набор и достает из него Сетевой Ключ А-Б. Так как этот Сетевой Ключ совпадает с тем Сетевым Ключом, который использовал узел А для зашифрования, то узел Б может расшифровать Файловый Ключ, пришедший вместе с файлом.

Наконец, с помощью Файлового Ключа расшифровывается сам файл.

Перешифрование информации

При перешифровании ключей происходят следующие операции.

Из зашифрованного файла извлекается зашифрованный Файловый Ключ и расшифровывается. Затем производится его зашифрование на новой ключевой информации, предоставляемой пользователем. Сам Файловый Ключ (в расшифрованном виде) при этом остается неизменным, что позволяет оставить тело зашифрованного файла без изменений. В результате перешифрование файла - операция значительно более быстрая, чем зашифрование или расшифрование файла.

Целостность информации

При расшифровании Файловых Ключей производится проверка имитовставки. Если она не совпала с хранимой в файле, то выдается сообщение об ошибке.

Следует отметить, что при расшифровании информации самих файлов никакая проверка целостности данных не производится. Если зашифрованная информация была изменена, никаких диагностических сообщений выдаваться не будет, но получаемый после расшифрования файл не будет эквивалентен исходному.

Ввод пароля

При расшифровании ключей и файлов, зашифрованных с использованием пароля, а также при зашифровании информации на пароле производится запрос пароля.

Если пароль запрашивается для зашифрования объекта (файла или ключа), то пользователю предоставляется диалог запроса пароля с двумя полями ввода. При этом необходимо ввести пароль дважды, что уменьшает вероятность опечатки.

Если пароль запрашивается для расшифрования объекта, то пользователю предоставляется диалог запроса пароля с одном полем ввода. При неправильном вводе пароля выдается сообщение "Пароль не верен", и запрос пароля повторяется до тех пор, пока пользователь не введет верный пароль или откажет-

ся от ввода пароля.

В случае операций над несколькими файлами последний введенный пароль запоминается в оперативной памяти до окончания операции, что избавляет от необходимости ввода одного и того же пароля для каждого файла. По окончании операции пароль стирается из памяти.

Замечание: В целях совместимости с предыдущим программным обеспечением алгоритм свертки пароля был оставлен прежним, в результате остается следующая особенность при анализе пароля: пароль из повторяющейся подстроки равен паролю из одной такой подстроки. Например, "qwertyqwerty" = "qwerty". Это не является ошибкой, поскольку по определению пароль не должен содержать повторяющихся цепочек.

Для проверки работоспособности и начала работы с пакетом программ КРИПТОН® Шифрование нет необходимости в выполнении каких-либо настроек. Ниже описан порядок проверки работоспособности пакета КРИПТОН®

Шифрование (до начала процедуры проверки работоспособности рекомендуется ознакомиться с разделом 4 настоящего документа):

Запустите программу Windows Explorer ("Проводник Windows").

Выделите один или несколько неиспользуемых файлов на Вашем компьютере.

Нажмите на выделении правую кнопку мыши, в появившемся контекстном меню выберите пункт "КРИПТОН® Шифрование \ Зашифровать". В появившемся диалоговом окне "Зашифровать файлы" также нажмите кнопку "Зашифровать". Произойдет зашифрование выбранных файлов на используемом Главном Ключе.

Создайте временный каталог и перенесите в него появившиеся в результате зашифрованные файлы.

Выделите эти файлы снова и нажмите на выделении правую кнопку мыши. Выберите пункт меню "КРИПТОН® Подпись \ Расшифровать". В появившемся окне "Расшифровать файлы" нажмите кнопку "Расшифровать". Зашифрованные файлы будут расшифрованы в текущий каталог.

Сравните исходные файлы с файлами, полученными в результате выполнения зашифрования и расшифрования, с помощью любой программы сравнения файлов (например, fc.exe). Файлы должны быть идентичны.

Пакет КРИПТОН® Шифрование состоит из 3 компонентов:

Программа управления ключами шифрования "Мастер ключей шифрования". Данная программа позволяет изменять настройки пакета.

Расширение Windows Explorer "КРИПТОН® Шифрование" для шифрования файлов. Эта программа обеспечивает добавление дополнительных команд в контекстное меню (а также в меню "Файл") программы Windows Explorer. Эти команды обеспечивают основные криптографические операции над файлами.

Утилита командной строки для пакетной обработки файлов. Эта программа позволяет автоматизировать процесс шифрования файлов, а также легко встраивать функции шифрования в клиентские системы путем вызова данной утилиты с параметрами, передаваемыми в командной строке.

Пакет КРИПТОН® Шифрование поставляется в двух вариантах:

"КРИПТОН® Шифрование".

"КРИПТОН® Шифрование - Администратор".

Вариант "КРИПТОН® Шифрование - Администратор" предназначен для генерации ключевой информации. Данный вариант является полнофункциональным, тогда как в варианте "КРИПТОН® Шифрование" функции генерации ключей шифрования запрещены. Данный документ - "Руководство пользователя" - содержит описание варианта "КРИПТОН® Шифрование".

Данный раздел содержит подробное описание программ пакета КРИПТОН® Шифрование и порядок работы с ними.

Мастер ключей шифрования

Программа "Мастер ключей шифрования" предназначена для выполнения настроек пакета КРИПТОН® Шифрование.

При запуске программы "Мастер ключей шифрования" на экран выводится

ее главное окно. Главное окно программы представляет собой диалоговое окно с двумя панелями. Левая панель содержит список доступных команд, иерархически оформленный в виде дерева. Правая панель отображает параметры выбранной команды и содержит элементы управления для ее выполнения. Для любой команды доступна интерактивная справка, вызываемая по нажатию кнопки "Справка" или клавиши "F1".

Вариант программы для пользователя дает возможность выполнения только одной команды - "Настройка параметров".

При запуске программы активным является корневой элемент дерева команд, называющийся "Мастер ключей шифрования". Данный элемент не является командой, при его выборе правая панель содержит информацию о программе "Мастер ключей шифрования".

Во всех командах программы доступны следующие кнопки, назначение которых не зависит от активной команды:

"Справка". При нажатии на данную кнопку вызывается стандартное окно справочной системы Windows, содержащее справочную информацию о программе "Мастер ключей шифрования".

"Выход". Предназначена для завершения работы с программой.

Команда "Настройка параметров"

После выбора данной команды правая сторона панели содержит следующие настраиваемые параметры:

"Каталог Ключей Пользователя". Следует ввести каталог Ключей Пользователя. В этом каталоге будет производиться поиск Ключей Пользователя в следующих ситуациях:

* Зашифровании файла на Ключе Пользователя.
* Расшифровании файла, зашифрованного на Ключе Пользователя.
* Перешифровании файла, зашифрованного на Ключе Пользователя.

Требуемый каталог можно указать также с помощью кнопки обзора ката-

логов. По данной кнопке на экран выводится меню "Диски"/"Карточки", позволяющее указать каталог с помощью стандартного диалога Windows или диалога выбора устройств SCApi.

"Каталог Сетевых Ключей". Следует ввести каталог Сетевых Ключей. В этом каталоге будет производиться поиск Сетевых Ключей в следующих ситуациях:

* Зашифровании файла на Сетевом Ключе.
* Расшифровании файла, зашифрованного на Сетевом Ключе.
* Перешифровании файла, зашифрованного на Сетевом Ключе.

Требуемый каталог можно указать также с помощью кнопки обзора каталогов, по которой вызывается стандартный диалог обзора папок Windows.

Сетевые Ключи хранятся в Сетевых Наборах в фалах NNNNN.sys, где NNNNN - номер данного сетевого узла - см. главу "Создать Сетевой Набор".

3. "Номер данного сетевого узла". Следует ввести номер сетевого узла - целое число в диапазоне от 1 до 30000, идентифицирующее данный сетевой узел (пользователя или компьютер - в зависимости от организационных решений).

Для ввода в действие сделанных изменений в конфигурации следует нажать кнопку "Применить". Конфигурация будет изменена.

Для отмены внесенных изменений следует нажать кнопку "Отменить".

Следует учесть, что в Windows NT данные параметры являются персональными для каждого локального пользователя Windows NT.

Параметры сохраняются в системном реестре Windows.

Расширение Windows Explorer "КРИПТОН® Шифрование"

Данный программный модуль выполняет основные действия пакета КРИПТОН® Шифрование.

Расширение Windows Explorer "КРИПТОН® Шифрование" встраивается в контекстное меню Windows Explorer, которое активизируется путем выделения одного или нескольких файлов или каталогов в Windows Explorer и последующего нажатия на выделении правой кнопки мыши. Данное расширение

присутствует в контекстном меню Windows Explorer как дополнительный пункт меню, имеющий название "КРИПТОН® Шифрование". При активизации данного пункта меню появляется подменю, содержащее основные команды расширения (см. Рис. 4).

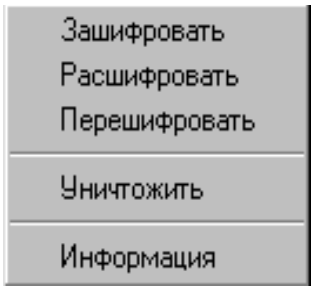


Рисунок 4 - Меню "КРИПТОН® Шифрование"

Все команды меню "КРИПТОН® Шифрование" выполняются над всеми выбранными файлами, а если выбран один или несколько каталогов - то над всеми файлами всех выбранных каталогов и их подкаталогов.

Ниже описан порядок выполнения действий с помощью данного программного модуля пакета КРИПТОН® Шифрование.

Зашифровать

Данная команда предназначена для зашифрования файлов. При ее выборе на экран выводится окно "Зашифровать файлы" (см. Рис. 5).

Перед зашифрованием следует указать параметры выполнения данной

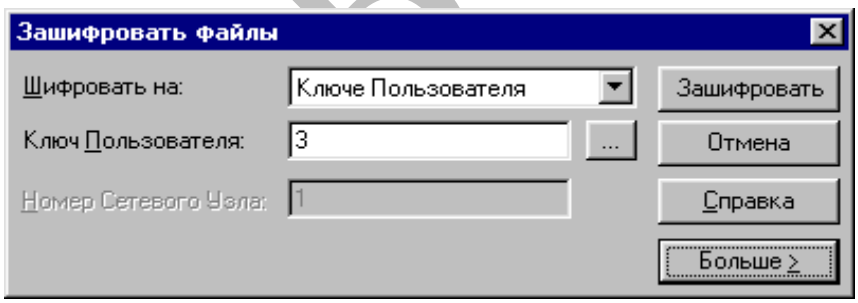


Рисунок 5 - Окно "Зашифровать файлы"

операции в следующих полях окна "Зашифровать файлы":

"Шифровать на". Список, в котором следует выбрать ключевую систему, с использованием которой будут зашифрованы выбранные файлы. Возможные варианты:

* "Ключ пользователя". В этом случае файлы будут шифроваться на Ключе Пользователя, который следует указать в поле "Ключ Пользователя". При необходимости (в зависимости от способа защиты выбранного Ключа пользователя) может быть запрошен пароль. Данный режим устанавливается по умолчанию.
* "Сетевой Ключ". Файлы будут зашифрованы на Сетевом Ключе для узла, указанного в поле "Номер Сетевого Узла". Сетевой Ключ берется из Сетевого Набора, который должен быть предварительно создан и помещен в каталог Сетевых Ключей (см. главу 4.1.3). Кроме того, необходимо предварительно корректно указать номер данного сетевого узла (см. главу 4.1.3).

"Номер Сетевого Узла". Данное поле доступно при выборе значения "Сетевой Ключ" в предыдущем поле. Здесь необходимо указать номер сетевого узла, для которого будут зашифрованы выбранные файлы.

"Ключ Пользователя". Данное поле доступно при выборе значения "Ключ Пользователя" в поле "Шифровать на". Здесь необходимо указать имя файла существующего Ключа Пользователя, на котором будут зашифрованы выбранные файлы. Требуемое имя файла можно также указать с помощью кнопки обзора каталогов, при нажатии которой на экран выводится окно выбора Ключа Пользователя (см. Рис. 6). В этом окне можно выбрать Ключ Пользователя из существующих в каталоге Ключей Пользователя. Кроме того, с помощью находящейся в окне "Выберите Ключ Пользователя" кнопки обзора каталогов можно изменить каталог Ключей Пользователя в стандартном окне обзора папок Windows.

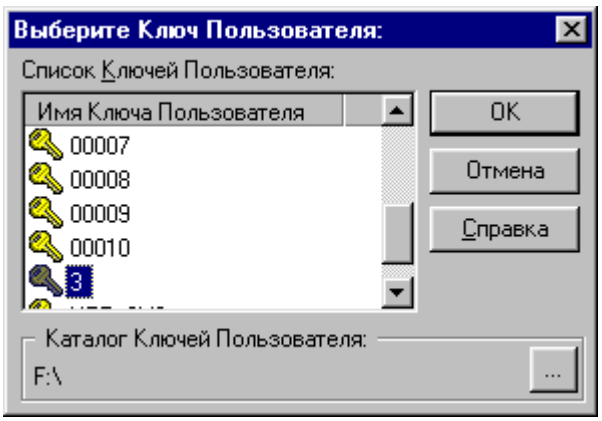


Рисунок 6 - Окно выбора Ключа Пользователя

В окне "Зашифровать файлы" можно указать также дополнительные параметры шифрования. Для этого следует нажать на кнопку "Больше >", после чего окно раскроется в полную форму. При раскрытии окна кнопка "Больше >" заменяется кнопкой "Меньше <", при нажатии на которую окно "Зашифровать файлы" примет первоначальный вид.

В полной форме окна будут доступны следующие параметры:

"Уничтожать исходные файлы". При включении данного флага исходные файлы уничтожаются без возможности восстановления после успешного выполнения операции зашифрования. Если зашифрование файлов по какой-либо причине закончилось неудачей, исходные файлы не уничтожаются.

"Копировать дату и аттрибуты". При включении данного флага дата и аттрибуты каждого зашифрованного файла будут соответствовать дате и аттрибутам соответствующего исходного файла.

"Не использовать сложные имена (file.txt.cry)". При включении данного флага файлы со сложными именами не создаются (порядок именования зашифрованных файлов подробно описан ниже). Этот режим необходим для совместимости с программным обеспечением фирмы "Анкад" для MS-DOS (например, программами Crypton Soft и Crypton Tools). В том случае, если Вы используете только Windows-продукты фирмы "Анкад", рекомендуется данный флаг не включать.

"Размещать зашифрованные файлы в каталоге". При включении данного флага все зашифрованные файлы создаются в каталоге, который следует ука-

зать в соответствующем поле. Каталог можно выбрать с помощью кнопки обзора каталогов, по которой вызывается стандартное окно обзора папок Windows.

Кроме того, в полной форме окна "Зашифровать файлы" присутствует кнопка "Параметры", с помощью которой можно изменить глобальные настройки пакета программ КРИПТОН® Шифрование (см. главу 4.1.3). По данной кнопке вызывается программа "Мастер ключей шифрования", в которой автоматически активизируется команда "Настройка параметров".

Для зашифрования файлов следует нажать кнопку "Зашифровать". Зашифрованный файл помещается в текущий или указанный каталог в зависимости отсостояния флага "Размещать зашифрованные файлы в каталоге". Имя зашифрованного файла формируется из имени исходного файла с добавлением к нему расширения ".cry", например, для файла с именем filename.ext имя зашифрованного файла будет filename.ext.cry. В том случае, если файл с такими именем и расширением уже существует, будет сформирован файл с расширением ".c00" (filename.ext.c00). Если и такой файл уже есть, то будет создан файл с расширением ".c01", и так далее.

Если включен переключатель "Не использовать сложные имена (file.txt.cry)", то при формировании имени зашифрованного файла будет отбрасываться расширение исходного файла, например, для файла с именем filename.ext имя зашифрованного файла будет filename.cry, а если такой файл уже существует, то filename.c00, и так далее.

Все указанные в окне "Зашифровать файлы" параметры сохраняются и предлагаются по умолчанию при следующей операции зашифрования. Форма окна "Зашифровать файлы" (полная или краткая) также сохраняется и восстанавливается при следующей операции.

При выполнении операции зашифрования для каждого выбранного файла последовательно выполняются следующие действия:

* Генерируется Файловый Ключ.
* Файл шифруется на данном Файловом Ключе.

* Файловый Ключ шифруется на указанной в поле "Шифровать на" ключевой системе с вычислением имитоприставки.
* В файл записывается информация, необходимая для последующего расшифрования: старое имя файла, имена ключей и т. д.

Расшифровать

Данная команда предназначена для расшифрования зашифрованных файлов. При ее выборе на экран выводится окно "Расшифровать файлы".

В краткой форме окна присутствует один параметр - переключатель "Если результирующий файл уже существует", который устанавливает действия программы при совпадении имен существующего и расшифровываемого файлов. Возможные значения:

* "Спрашивать подтверждения пользователя". В этом случае для каждого файла с совпавшим именем выводится диалог "Совпадение имен файлов". Данный вариант полезен при расшифровании нескольких файлов. Диалог "Совпадение имен файлов" содержит 6 вариантов реакции, определяющей дальнейшие действия с указанным в диалоге файлом:

◊ "Переписать". В этом случае файл будет перезаписан новым.

◊ "Пропустить". Файл будет пропущен (оставлен существующий файл с совпавшим именем).

◊ "Переименовать". При выборе этого варианта становится доступным поле ввода имени файла. В этом поле ввода Вы можете указать новое имя файла.

◊ "Автопереименовать". Файл будет переименован. При этом он получит имя по следующему правилу: к имени файла добавляется в скобках номер. Например, для файла file.txt порядок автопереименований будет следующим: file(2).txt, file(3).txt и так далее.

◊ "Переписать все". Этот и все последующие файлы с совпадающими именами будут перезаписаны. При этом диалог "Совпадение имен файлов" в данной сессии расшифрования больше выво-

диться не будет.

◊ "Автопереименовать все". Этот и все последующие файлы с совпадающими именами будут автопереименованы (см. "Автопереименовать"). Диалог "Совпадение имен файлов" в данной сессии расшифрования больше выводиться не будет.

* "Перезаписывать файл". В этом случае все файлы с совпадающими именами будут перезаписаны без предупреждений.
* "Пропустить". Все файлы с совпадающими именами будут пропущены (существующие файлы будут оставлены без изменений).
* "Автопереименовывать". Все файлы с совпадающими именами будут автопереименованы - аналогично выбору варианта "Автопереименовать все" в диалоге "Совпадение имен файлов".

В окне "Расшифровать файлы" можно указать также дополнительные параметры. Для этого следует нажать на кнопку "Больше >", после чего окно раскроется в полную форму. При раскрытии окна кнопка "Больше >" заменяется кнопкой "Меньше <", при нажатии на которую окно "Расшифровать файлы" примет первоначальный вид.

В полной форме окна будут доступны следующие параметры:

"Уничтожать исходные (зашифрованные) файлы". При включении данного флага зашифрованные файлы уничтожаются без возможности восстановления после успешного выполнения операции расшифрования. Если расшифрование файлов по какой-либо причине закончилось неудачей, зашифрованные файлы не уничтожаются.

"Копировать дату и аттрибуты". При включении данного флага дата и аттрибуты каждого расшифрованного файла будут соответствовать дате и аттрибутам соответствующего исходного файла.

"Пропускать незашифрованные файлы". При включении данного флага файлы с расширениями, несоответствующими расширениям зашифрованных файлов (".cry", ".c00", ".c01" и т. д.), пропускаются. В противном случае производится попытка расшифровать все выбранные файлы, в этом случае, если

встречается незашифрованный файл, выдается сообщение об ошибке.

"Размещать расшифрованные файлы в каталоге". При включении данного флага все расшифрованные файлы помещаются в каталог, который следует указать в соответствующем поле. Каталог можно выбрать с помощью кнопки обзора каталогов, по которой вызывается стандартное окно обзора папок Windows.

Кроме того, в полной форме окна "Расшифровать файлы" присутствует кнопка "Параметры", с помощью которой можно изменить глобальные настройки пакета программ КРИПТОН® Шифрование. По данной кнопке вызывается программа "Мастер ключей шифрования", в которой автоматически активизируется команда "Настройка параметров".

Все указанные в окне "Расшифровать файлы" параметры сохраняются и предлагаются по умолчанию при следующей операции расшифрования. Форма окна "Расшифровать файлы" (полная или краткая) также сохраняется и восстанавливается при следующей операции.

Для расшифрования файлов следует нажать кнопку "Расшифровать".

Перешифровать

Данная команда предназначена для перешифрования зашифрованных файлов. Перешифровать зашифрованные файлы можно двумя способами:

* Расшифровать зашифрованные файлы и зашифровать их снова на другой ключевой системе или других ключах.
* С помощью команды "Перешифровать".

Второй способ является существенно более быстрым, чем первый, но он неприменим при смене Узла Замены. В этом случае обязательно придется расшифровывать файлы.

В остальных случаях рекомендуется пользоваться именно командой "Перешифровать". По этой команде на экран выводится окно "Перешифровать файлы" в котором следует указать следующие параметры:

"Перешифровать на". Список, в котором следует выбрать ключевую систему, с использованием которой будут зашифрованы после выполнения опера-

ции перешифрования выбранные файлы. Возможные варианты:

* "Ключ пользователя". В этом случае файлы будут шифроваться на Ключе Пользователя, который следует указать в поле "Ключ Пользователя". При необходимости (в зависимости от способа защиты выбранного Ключа пользователя) может быть запрошен пароль.
* "Сетевой Ключ". Файлы будут зашифрованы на Сетевом Ключе для узла, указанного в поле "Номер Сетевого Узла". Необходимо предварительно корректно настроить номер данного сетевого узла.

"Номер Сетевого Узла". Данное поле доступно при выборе значения "Сетевой Ключ" в предыдущем поле. Здесь необходимо указать номер сетевого узла, для которого будут зашифрованы выбранные файлы.

"Ключ Пользователя". Данное поле доступно при выборе значения "Ключ Пользователя" в поле "Перешифровать на". Здесь необходимо указать имя файла существующего Ключа Пользователя, на котором будут зашифрованы выбранные файлы. Требуемое имя файла можно также указать с помощью кнопки обзора каталогов, при нажатии которой на экран выводится окно выбора Ключа Пользователя (см. Рис. 5). В этом окне можно выбрать Ключ Пользователя из существующих в каталоге Ключей Пользователя. Кроме того, с помощью находящейся в окне "Выберите Ключ Пользователя" кнопки обзора каталогов можно изменить каталог Ключей Пользователя в стандартном окне обзора папок Windows.

Для выполнения перешифрования файлов следует нажать кнопку "Перешифровать". Имена зашифрованных файлов при выполнении операции перешифрования не меняются. При попытке перешифровать незашифрованный файл будет выдано сообщение об ошибке.

Уничтожить

Данная команда предназначена для уничтожения выбранных файлов без возможности их восстановления. При уничтожении файла происходит запись

константного значения поверх его содержимого, после чего файл удаляется.

Перед уничтожением запрашивается подтверждение уничтожения выбранных файлов. После получения подтверждения файлы будут уничтожены.

Следует очень внимательно выбирать файлы и, особенно, каталоги для уничтожения, поскольку восстановление уничтоженных файлов будет невозможно. Следует учесть, что данная команда, как и остальные команды расширения "КРИПТОН® Шифрование", выполняется над всеми файлами выбранных каталогов и их подкаталогов.

Информация

Данная команда предназначена для получения информации о различных файлах, имеющих отношение к пакету программ КРИПТОН® Шифрование, а именно, о зашифрованных и ключевых файлах.

При выборе данной команды производится анализ выбранных файлов, результаты которого (информация об анализируемых файлах) выводятся в окно "Информация о файлах" (см. Рис. 4).

Данное окно содержит следующие элементы:

"Каталог". Показывает каталог, содержащий анализируемые файлы.

Список файлов с дополнительной информацией. Список файлов разделен на две части, в левой из которых перечислены анализируемые файлы, а также содержится дополнительная информация о каждом из ключевых или зашифрованных файлов. Например, для файла Ключа Пользователя в качестве дополнительной информации выводятся следующие сведения: используемая для защиты данного ключа ключевая система, срок действия ключа, информационное поле ключа (обычно содержащее информацию о владельце). Получаемая дополнительная информация зависит от конкретного типа анализируемого файла. Особенно полезной может быть дополнительная информация о зашифрованном файле.

Правая часть списка файлов содержит краткое описание типа анализируемого файла или "Неизвестный файл", если данный файл не имеет отношения к пакету КРИПТОН® Шифрование.

Кнопка "Пауза". Данная кнопка появляется в момент анализа файлов и позволяет приостановить данный процесс, например, для просмотра результатов. После нажатия кнопки "Пауза" на ее месте появляется кнопка "Продолжить", позволяющая продолжить анализ файлов.

Кнопка "Прервать". Данная кнопка появляется в момент анализа файлов и позволяет, после подтверждения, прервать данный процесс.

Кнопка "Справка". Вызывает контекстную справочную информацию.

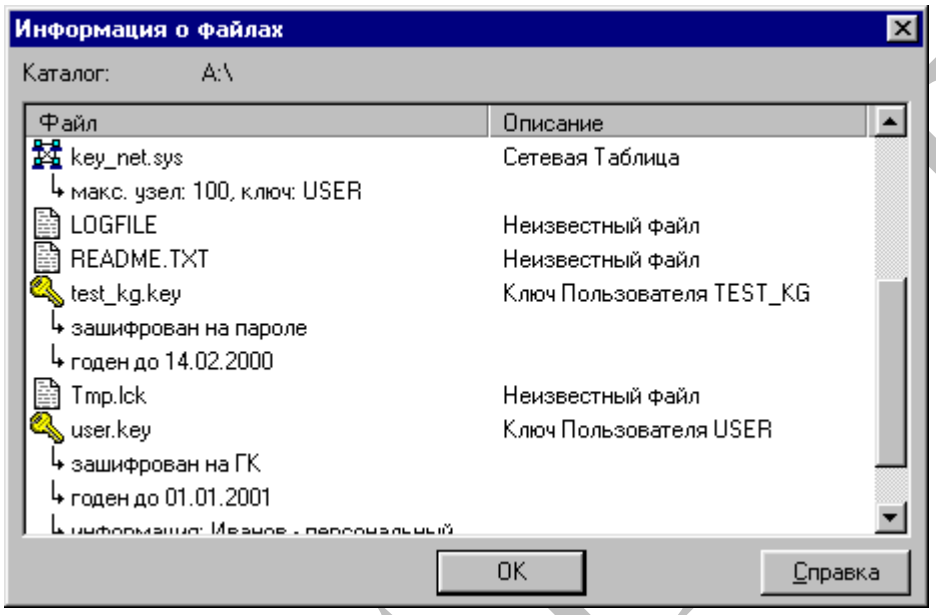


Рисунок 5 - Окно "Информация о файлах"

Кнопка "ОК". Закрывает окно "Информация о файлах".

Crypton API

Запустить программу тестирования функций приложения Crypton API В появившемся окне можно видеть несколько вкладок, каждая из которых выполняет определенную функцию. Например, в окне ключи можно изменять значения ключей К.

Во вкладке шифрование. Предварительно напечатав синхропосылку и строку для шифрования, нажать кнопку зашифровать, выбрав один из двух вариантов. Убедиться в совпадении исходного и расшифрованного текстов. Во вкладке имитовставка вычислить имитовставки для данных на различных ключах. Вкладка ДСЧ (датчик случайных чисел)

позволяет генерировать последовательности случайных чисел в 16- и 10-тиричной форме.

Вкладки скорость и многозадачность позволяют измерять производительность компьютера. Вкладка функции отображает поддерживаемые программой функции.

Кроме того. Вкладка SA 101i позволяет считывать данные со смарт-карт

В данной работе следует проделать выше сказанные операции с целью приобретения новых навыков работы с ПО Crypton

Crypton Disk

Открыть в меню «Пуск» программу Crypton Disc→ Crypton Disc Manager, либо нажать правую кнопку мыши на рабочем столе Windows. Затем выбрать пункт меню Создать → Paragon Encrypted Disc Image (Образ зашифрованного диска).

В окне Crypton Disc Manager выбрать вкладку Диск→Создать образ диска (или нажать Ctrl + N)

Когда программа запросит вставить ключевой носитель с Главным ключом и Узлом Замены (дискета: у преподавателя), вставить дискету и нажать ОК.

Затем запустится специальный Мастер создания файла образа. Выберите местонахождение нового файла образа для зашифрованного образа и его размер. У вас должно быть достаточно свободного места для создания файла образа. Файл образа может быть создан на локальном жестком диске, сменном носителе, таком как JAZ , ZIP, сетевом диске. После создания и копирования данных на зашифрованный диск Вы можете даже переместить файл образа на CDROM. Выберите алгоритм шифрования. В данной версии программы используется алгоритм шифрования ГОСТ 28147-89, hash-алгоритм ГОСТ и алгоритм генерации случайных чисел фирмы Ancud.

Выберите способ шифрования.

Режим 1: Ключ

Режим 2: Пароль

Режим 1: Будет сгенерирован специальный ключ и сохранен в файл на дискете пользователя или другом сменном носителе. Этот ключ используется для зашифровки/расшифровки данных. Пользователю необходимо вставить дискету или другой носитель с файлом, содержащим ключ, для установки зашифрованного диска. По определению, файл, содержащий ключ, имеет то же имя, что и файл образа, и расширение “crk”. Например, файл образа – “Disk1.crd”, файл ключа “disk1.crk”.

Дискета или другой содержащий ключ носитель нужно хранить в безопасном месте!

Режим 2: Пароль пользователя

В этом режиме данные пользователя защищены паролем, который вводится пользователем с клавиатуры. Его использовать более удобно, но из соображений секретности пароль не должен быть простым.

После этого появится окно, в котором:

1) диск можно установить немедленно после создания. Это означает, что в системе появится новая буква диска и пользователь может начать работу с диском:

2) диск может быть установлен или на определенной букве, или на первой доступной.

Диск также можно автоматически установить при входе в систему.

После того как выбраны все опции, будет создан файл образа. Для того чтобы установить диск, его необходимо отформатировать. Поэтому появиться системный диалог форматирования диска. Просто выберите необходимый способ форматирования и нажмите кнопку “Начать”. После окончания форматирования созданного диска нажмите кнопку “Закрыть”

Если форматирование прошло успешно, диск будет установлен (согласно параметрам). После этого в правой части окна Crypton Disc Manager можно увидеть значок (значки) созданного образа зашифрованного диска (левая часть - дерево установленных виртуальных зашифрованных дисков). Те образы, которые не были найдены в базе образов Crypton Disk, будут указаны символом

“?”. Это может случиться, когда образ храниться на сменных носителях или сетевом диске, который недоступен. Как только они появятся, достаточно нажать клавишу “F5”, и статус каждого образа обновится.

Размонтировать зашифрованный диск.

Чтобы закрыть доступ к зашифрованному диску, просто размонтируйте его. Вы можете сделать это в Windows Explorer щелчком правой кнопки мыши или из окна программы CryptonDisk.

Диск можно размонтировать, если на нем нет открытых файлов. Более того, когда Windows Explorer просматривает диск, он открывает корневую директорию как файл. Это значит, что для того чтобы размонтировать зашифрованный диск, Вам необходимо закрыть все окна, которые используют этот зашифрованный диск, и закрыть все документы, которые находятся на этом зашифрованном диске. При выходе из системы диск размонтируется автоматически.

Перешифровать зашифрованный диск.

Для того чтобы перекодировать зашифрованный диск, выберите “Свойства” диска из Windows Explorer или из окна программы CryptonDisk Manager, затем нажать клавишу “Перекодировать” на странице “Шифрование”. Сначала диск будет размонтирован, а затем Вам будет предложено ввести новый пароль или сохранить новый файл ключа.

Удалить зашифрованный диск

Вы можете убрать зашифрованный диск из системы и/или убрать образ.

Запустите программу Crypton Disk Manager и выберите Диск → Убрать диск.

Сначала диск будет размонтирован (см “Размонтирование зашифрованного диска”) поэтому не должно быть никаких открытых файлов на этом зашифрованном диске.

Во-вторых, диалог запросит, нужно или нет стереть образ диска (можно установить флажок «Удалить файл образа с физического диска»).

Отчет по лабораторной работе включает:

1. Цель работы
2. Схему иерархической структуры ключей
3. Описание назначения каждого ключа
4. Выводы о проделанной работе

Контрольные вопросы:

1. Функции Crypton Word
2. Каким образом можно получить новый комплект ключей?
3. На каком алгоритме шифрования основан программный комплекс Crypton ?
4. Что такое узел замены, главный ключ? Пояснить их особенности
5. Что представляет собой имитовставка?
6. Изобразить иерархическую структуру ключей
7. Каким образом осуществляется архивное шифрование файлов?
8. Описать процесс шифрования файлов для передачи в криптографической сети
9. Каким требованиям должен удовлетворять используемый пароль?
10. Назвать характеристики алгоритма ГОСТ 28147-89
11. Пояснить процедуры шифрования информации и ввода пароля
12. Из каких компонентов состоит пакет КРИПТОН® Шифрование **?**