МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра защиты информации и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«___»_____2015 г.

ПРИМЕНЕНИЕ ПРОГРАММНЫХ КРИПТОСИСТЕМ ШИФРОВАНИЯ. ИЗУЧЕНИЕ ПРОГРАММНОГО ПРОДУКТА FOX SECRET

Методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2015

УДК 004.056.55 (076.5)

Составитель: М.А. Ефремов, А.Л. Ханис

Рецензент
Кандидат технических наук, доцент *И.В. Калуцкий*

Применение программных криптосистем шифрования. Изучение программного продукта Fox Secret: методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов, А.Л. Ханис. Курск, 2015. 20 с.: ил. 18.

Содержат сведения о применении программных криптосистем шифрования на примере программного продукта Fox Secret. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы - ознакомление с работой программных систем шифрования и скрытия данных на примере программного продукта Fox Secret.

2. ЗАДАНИЕ

Произвести установку программного продукта Fox Secret. Настроить требуемые параметры шифрования, изучить применение программного продукта в области криптографической и стеганографической защиты информации.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Сгенерировать ключи.
4. Зашифровать сообщение или файл.
5. Сокрытие информации в графических форматах.
6. Сокрытие данных в звуковых форматах.
7. Сокрытие секретов в документах.
8. Восстановить данные.
9. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Описание выбора требуемых параметров.
4. Процесс выполнения работы со скриншотами.
5. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

Программный продукт Fox Secret - это приложение с возможностью реализации стеганографических и криптографических алгоритмов для обеспечения защиты и укрытия вашей конфиденциальной информации от других пользователей и злоумышленников.

Возможности Fox Secret:

- поддержка защиты и сокрытия любых типов данных, включая текст, файлы или сейфы со сложной структурой из каталогов и файлов;
- возможность шифрования информации проверенными временем симметричными алгоритмами для шифрования: Blowfish, 3Way, IDEA, ГОСТ 28147-89 (Российский стандарт), RC5 и AES32;
- наличие возможность для реализации шифрования с несимметричным алгоритмом RSA;
- возможность сжатия данных перед началом шифрования при помощи встроенного архиватора;
- возможность проверки хеша сокрытых данных с использованием для данного мониторинга алгоритмов MD5, SHA 256, SHA или ГОСТ 34.11-94;
- возможность сокрытия данных с использованием графических форматов: Windows BMP (с возможностью выбора между 16-битным, 24-битным или даже 32-битным цветом), JPEG, PNG или TIFF;
- возможность сокрытия данных с использованием звуковых форматов: WAV (PCM) или MP3;
- возможность сокрытия данных с использованием документов: TXT – в качестве обычного текста, RTF – как отформатированный текст или HTML – в качестве гипертекстового формата для страниц интернета;
- наличие поддержки операции Drag'n'Drop, используя оболочку Windows (проводник) для окна сейфа;

– наличие поддержка защищённой базы с возможностью хранения ключей RSA;
– наличие возможности установки подписей RSA ключами любого выбранного файла и, соответственно, проверка такой подписи.

Преимущества:

– возможность реального и окончательного удаления с носителей файлов с данными;
– возможность встроить некоторые функции приложения в оболочку системы Windows.

5.2 Установка программы

Запустить программу fs_setup_ru.exe. Появится окно приветствия (рис.1). Нажимаем кнопку Next.

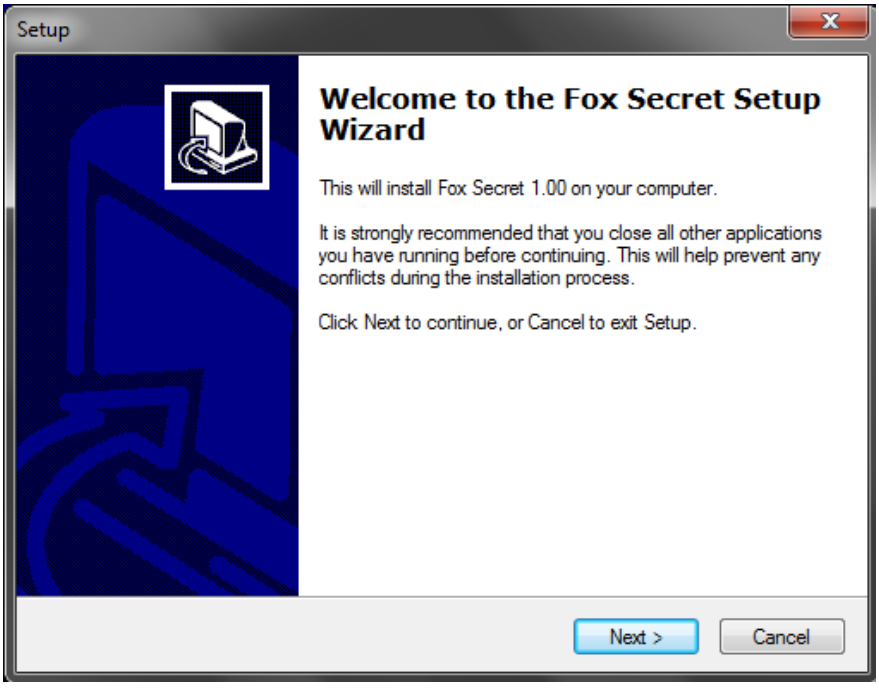

Рисунок 1 – Окно приветствия программы

Нажав кнопку Next, переходим к окну лицензионного соглашения (рис.2).

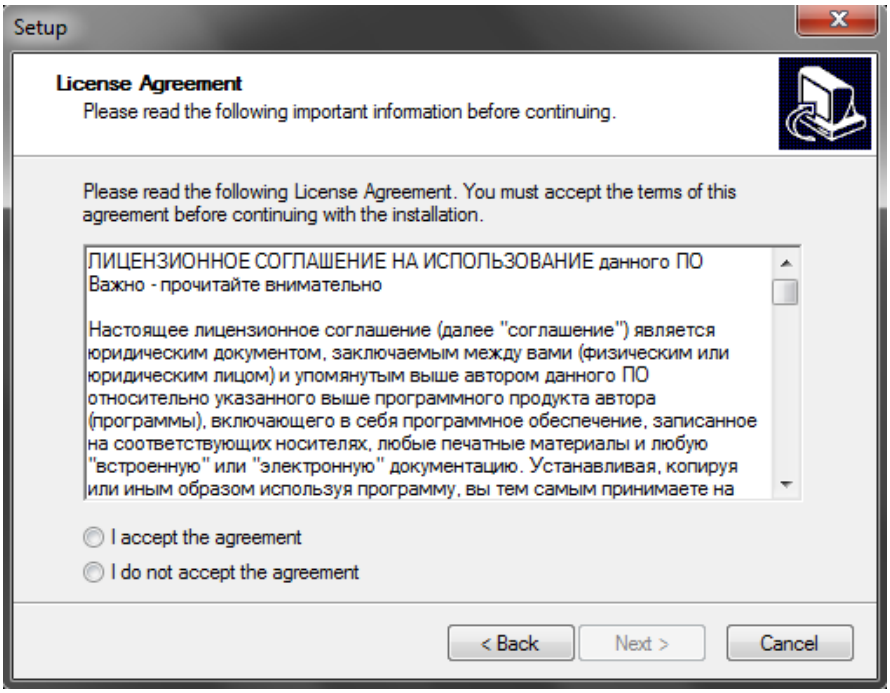

Рисунок 2 – Принятие лицензионного соглашения

Внимательно читаем лицензионное соглашение на использование данной программы, соглашаемся с ними, подтвердив выбор возле надписи “I accept the agreement”. Жмем Next и попадаем в окно описание программы, в котором мы можем прочитать основные особенности Secret Fox (рис.3).

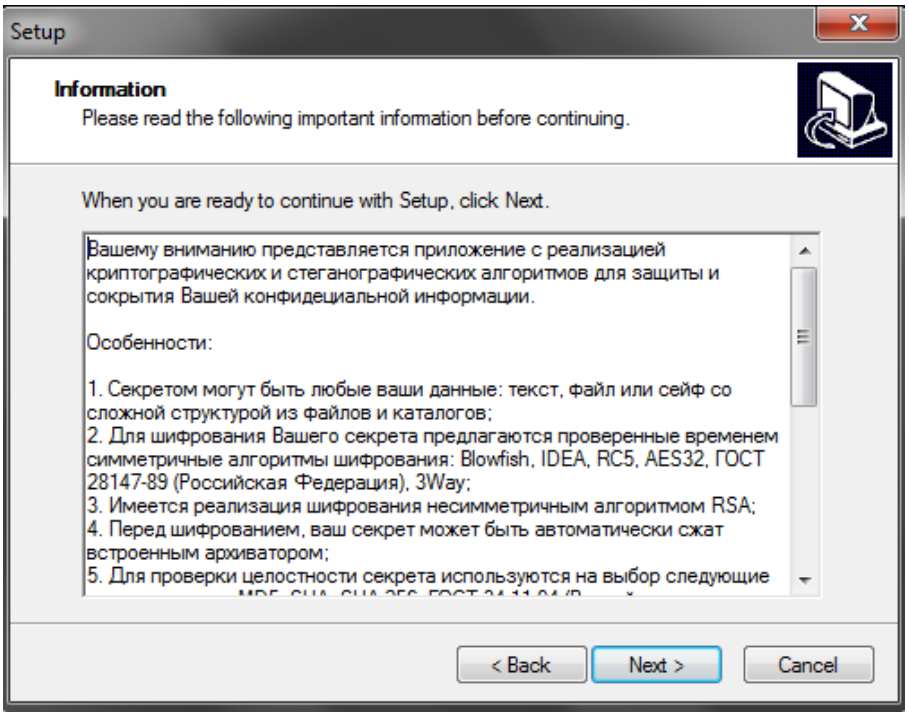

Рисунок 3 – Описание особенностей программы

Ознакомившись с особенностями программы, жмем Next, чтобы продолжить установку. Далее мы попадаем в меню выбора каталога, в который будет произведена установка компонентов Fox Secret. Мы видим, что вес программы составляет 1.2 Mb. Выберите каталог и нажмите Next (рис.4).

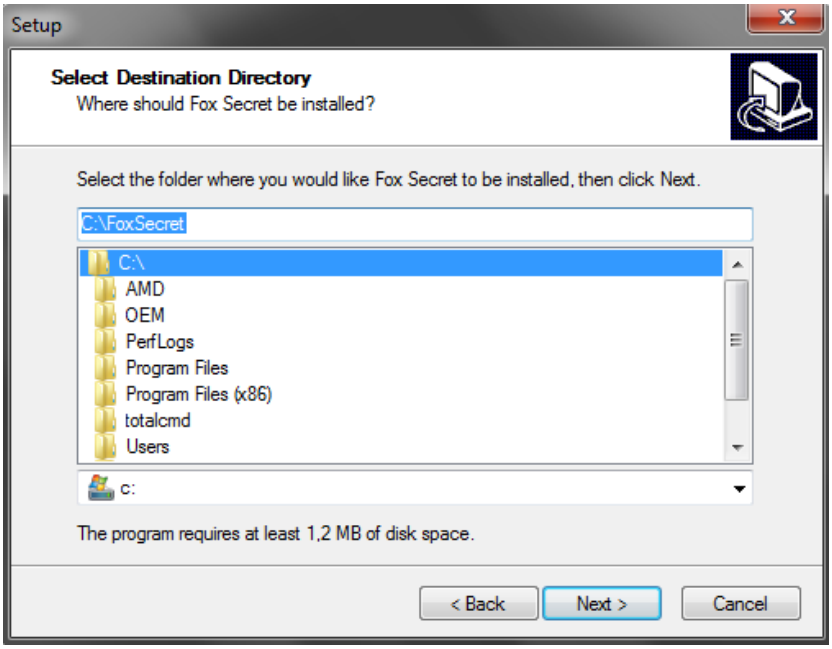

Рисунок 4 – Выбор каталога для установки программы

Далее выбираем компоненты, которые будут установлены помимо основного контента программы и нажимаем Next (рис.5).

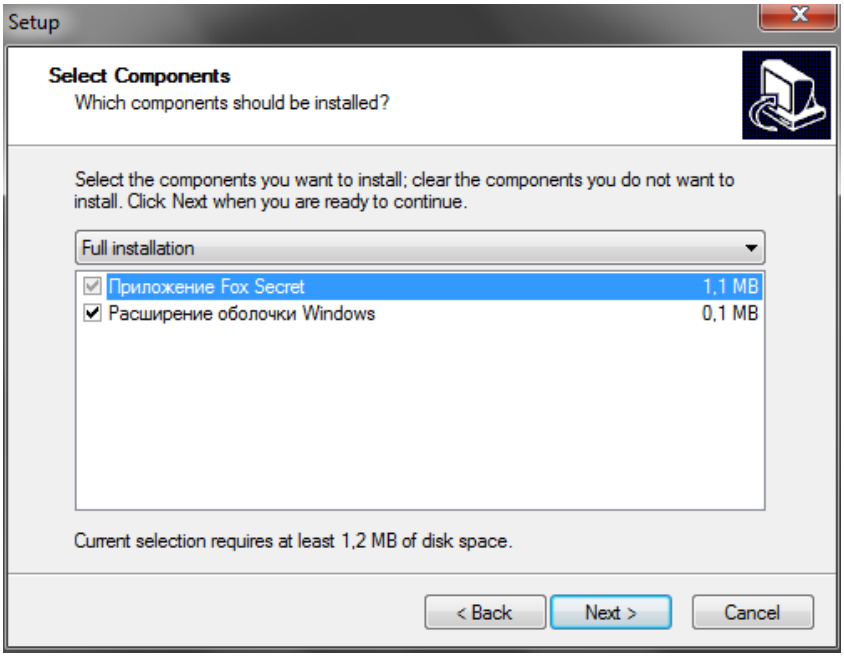

Рисунок 5 – Выбор компонентов программы для установки

Следующим шагом установки является выбор каталога ярлыка программы в меню ПУСК «Все программы». Выбираем, нажимаем Next (рис.6).

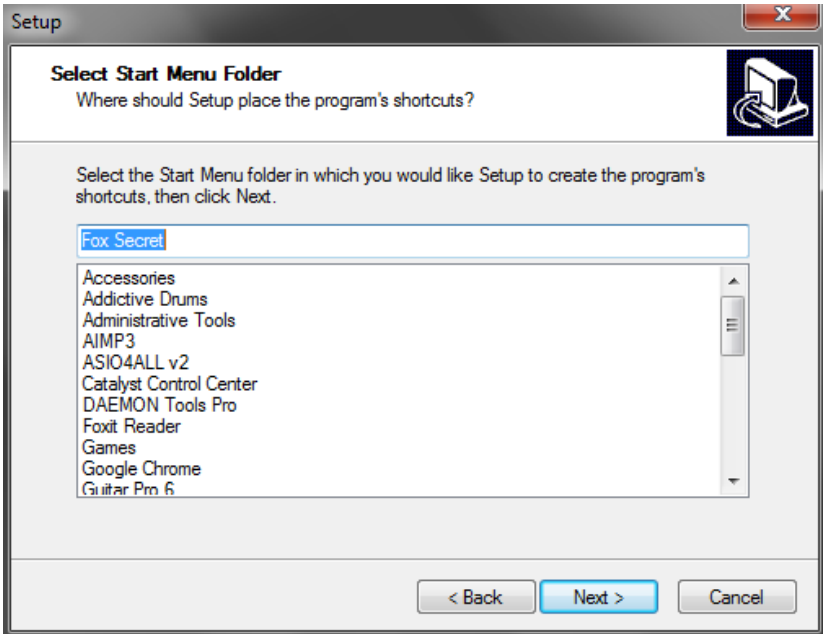

Рисунок 6 – Выбор ярлыка программы

В следующем окне, по желанию, выводим ярлыки на рабочий стол и панель быстрого запуска соответственно. Нажмите Next, а далее кнопку Install, чтобы установить программу (рис.7)

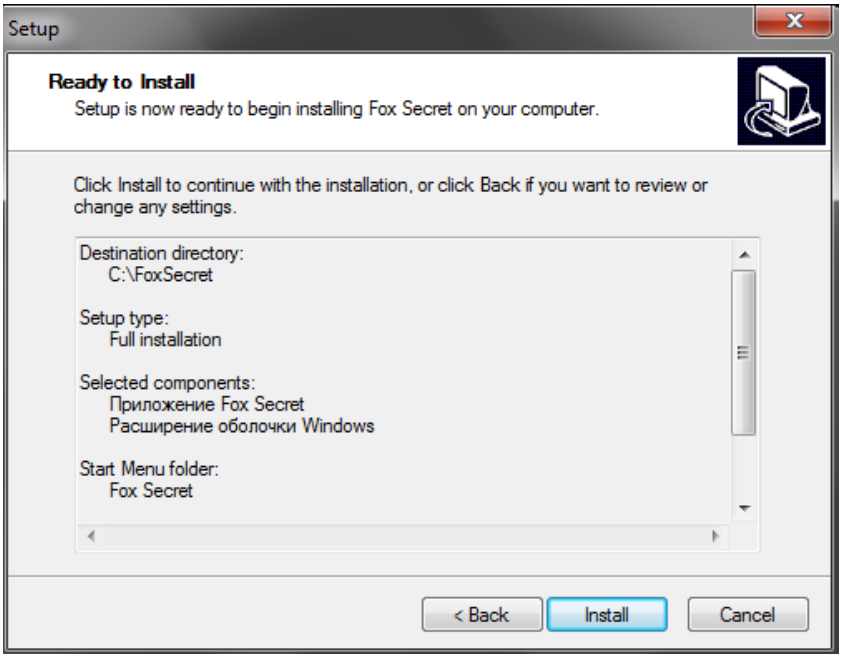

Рисунок 7 – Описание особенностей программы

По завершению установки нажмите Finish.

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Начало работы с программой

В начале работы вам доступны следующие операции над секретами:

- Создать секрет - Вы можете создать новый файл секрета или сохранить новый секрет внутри картинки, звука или документа.
- Открыть секрет - Вы можете открыть ранее созданный секрет из файла с расширением fss или спрятанный внутри картинки, звука или документа.
- Переоткрыть секрет - этот пункт поможет Вам быстро найти секреты, с которыми Вы работали ранее. Сюда заносятся только секреты внутри файлов с расширением fss.

Помимо операций с секретами, доступны и дополнительные функции:

- Настройка - позволяет настроить типы автоматически архивируемых файлов и параметры шрифта текста. Здесь же можно выбрать активный язык системы.
- Физическое удаление - функция удаления файла с носителя информации без возможности восстановления. Будьте внимательны с этой функцией.
- Хранилище ключей - позволяет вызвать окно хранилища RSA ключей и выполнить в нём необходимые манипуляции с RSA ключами.
- Создать подпись - предоставляет возможность создать файл-подпись, удостоверяющий, что хозяин некоторого закрытого ключа заверил подлинность содержимого указанного файла. Автор приложения должен заметить Вам, что эта подпись не имеет юридической силы, так как не поддерживает сертификацию и не лицензирована государством. Но в силу использованных технологий может служить вашим личным обеспечением целостности содержимого некоторого файла.
- Проверить подпись - позволяет установить подлинность подписывания субъектом (владельцем закрытого ключа, предоставившего свой открытый ключ) некоторого файла.

Содержание помощи - это справочное руководство.

6.2 Создание нового секрета

Первым шагом создания секрета будет выбор типа секрета. Для этого нажмите по кнопке Создать новый секрет. Здесь Вам будут доступны три типа секрета (рис.8).

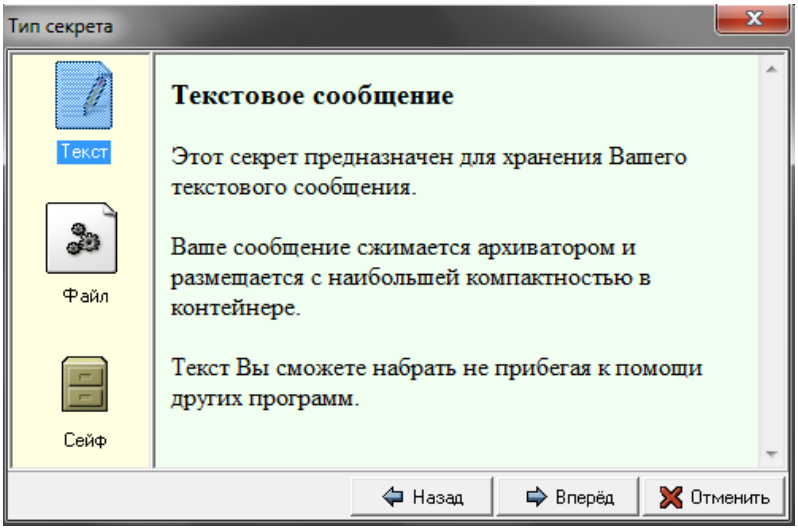

Рисунок 8 – Выбор типа секрета

1. *Текстовое сообщение* - простой текст, содержащий Ваше некоторое сообщение без форматирования. Приложение предоставляет простые возможности по редактированию этого текста, работы с буфером обмена и поиском. Перед сохранением, текст сообщения будет сжат встроенным архиватором.
2. *Одиночный файл* - секретом будет информация из одного некоторого файла. Это может быть файл любого формата. Если расширение файла имеется в списке архивируемых файлов, то файл, при размещении внутри секрета, будет автоматически сжат встроенным архиватором.
3. *Сейф* - это организация секрета в виде хранилища со сложной внутренней структурой, позволяющей сохранять совокупности файлов и каталогов. Файлы могут быть любых форматов и при добавлении могут быть автоматически сжаты встроенным архиватором.

Следующим шагом необходимо выбрать тип контейнера для секрета, который будет обеспечивать скрытность секрета: нажать кнопку Вперед (рис.9).

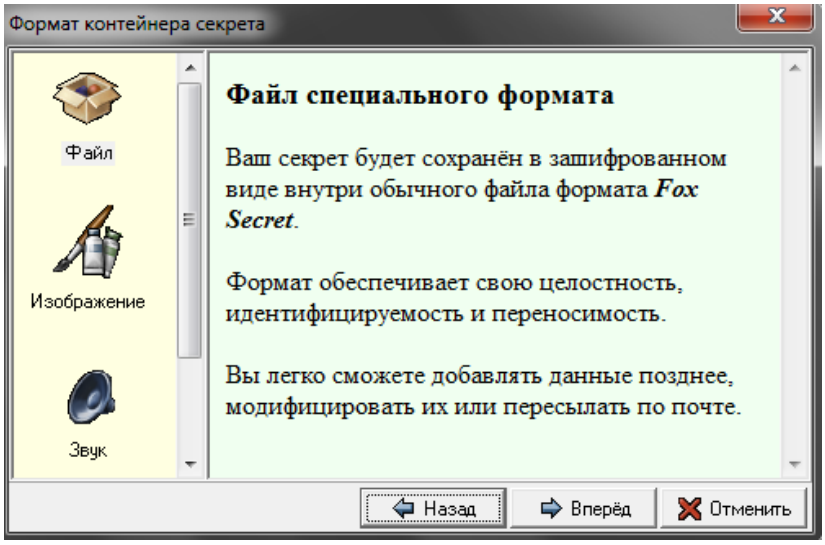

Рисунок 9 – Выбор типа контейнера

1. Файл формата Fox Secret - это файл собственного формата приложения со своими заголовками, идентификационными полями и внутренней структурой. Работа с таким файлом обеспечивает наибольшую скорость и переносимость. Формат поддерживает свою целостность и идентифицируемость. Это означает, что формат не будет спутан с другим и, в случаи успешного создания или открытия, информация секрета будет сохранена в неизменности.
2. *Картинка* - этот класс контейнеров предусматривает сокрытие зашифрованного секрета внутри графического файла. Поддерживаются следующие форматы графических файлов:
   - BMP
   - PNG
   - JPEG
   - TIFF
3. *Звук* - сокрытие секрета внутри файлов звукового формата. Поддерживаются WAV и MP3 форматы.
4. *Документ* - Ваш секрет будет "растворён" внутри текстового, HTML или RTF документа.

Важно помнить, что после создания секрета внутри графического, звукового или текстового формата файла, сам файл-носитель секрета ни в коем случаем нельзя редактировать или пересохранять в другом редакторе.

Следующем шагом Вам будет предложено указать файл для контейнера. В случае стеганографии - Вы должны будете указать существующий файл соответствующего формата, а для сохранения секрета в файл - просто новое имя файла.

После успешного выбора файла, нажав кнопку Вперед, появится окно с параметрами секрета (рис.10).

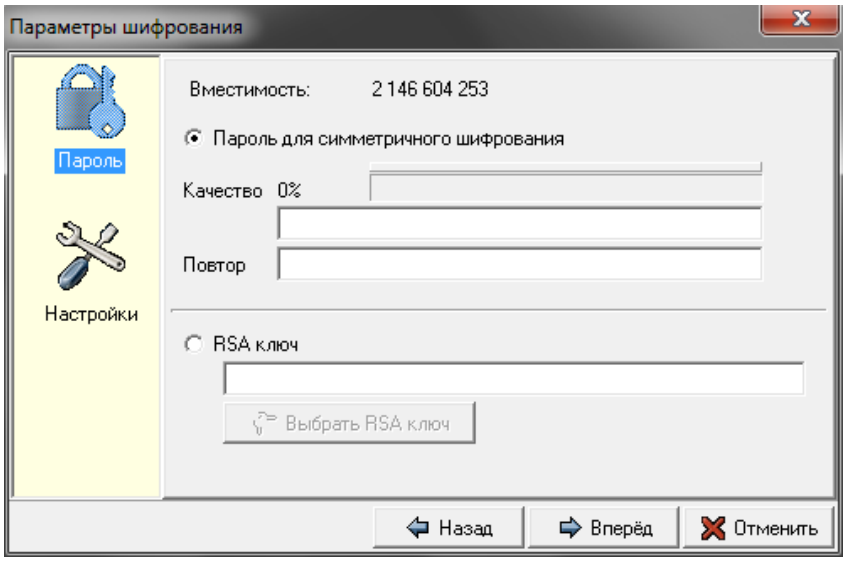

Рисунок 10 – Параметры шифрования

Если был указан стеганографический контейнер, то будет указана вместимость контейнера в байтах. Это важная информация, которая позволит Вам оценить применимость контейнера для Ваших задач защиты данных. Не забывайте, что реальная вместимость контейнера может быть большей, если учитывать сжатие внутренним архиватором некоторых Ваших файлов при размещении в секрете.

Вы можете выбрать один из двух способов задания пароля для секрета - для симметричного шифрования и для шифрования открытым ключом по методу RSA.

Для симметричного шифрования необходимо задать пароль - кодовый набор слов, который нельзя раскрывать постороннему. Пароль должен быть достаточно сложным, чтобы быть

устойчивым к методу словарного перебора. Лучше будет, если Вы будете сочетать большой и маленький регистры букв, добавлять цифры и знаки препинания. Пароль ограничен 56 символами и чем длиннее - тем более устойчив. Степень устойчивости показывается процентным и цветовым индикаторами. Впрочем, система примет и Ваш пустой пароль.

При шифровании открытым ключом RSA (не забывайте, что в состав закрытого ключа RSA также входит открытая часть и, таким образом, закрытый ключ тоже подходит для шифрования), выбор ключа будет предложен вам из отдельного окна. Если база ключей ещё не открывалась, Вы должны будете указать пароль к базе RSA ключей. Если Вы шифруете открытым ключом не из закрытого ключа, то учитывайте, что после закрытия секрета, открыть его не сможете. Открыть секрет с RSA шифрованием можно только при наличии соответствующего закрытого ключа.

На второй вкладке можно выбрать алгоритмы шифрования и расчёта значения хэша секретных данных (рис.11).

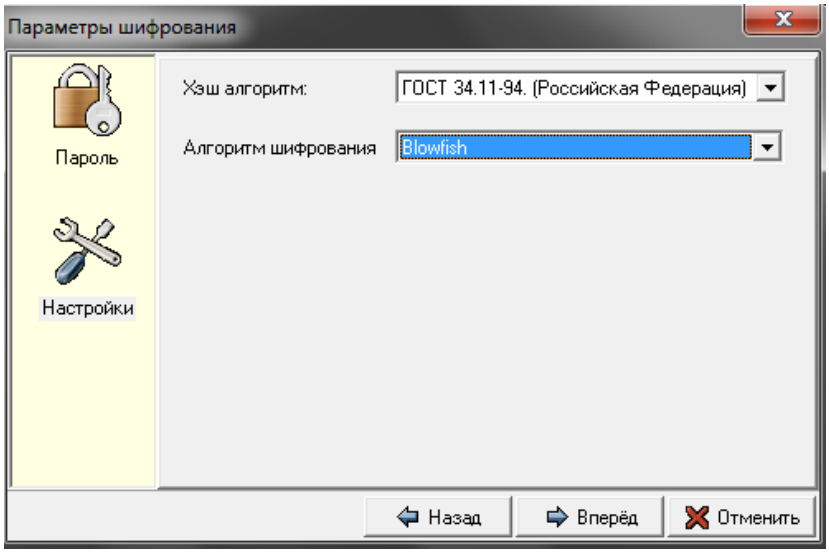

Рисунок 11 – Выбор алгоритма шифрования

После выбора параметры и перехода далее, если не возникло ошибки, приложение перейдёт в режим работы с секретом. Для текстового сообщения - это будет редактор текста, для одиночного файла - окно с указанием файла, а для сейфа - проводник файлов и каталогов сейфа.

6.3 Выбор секрета

Для начала, Вам надо указать файл, содержащий секрет (Рис.12):

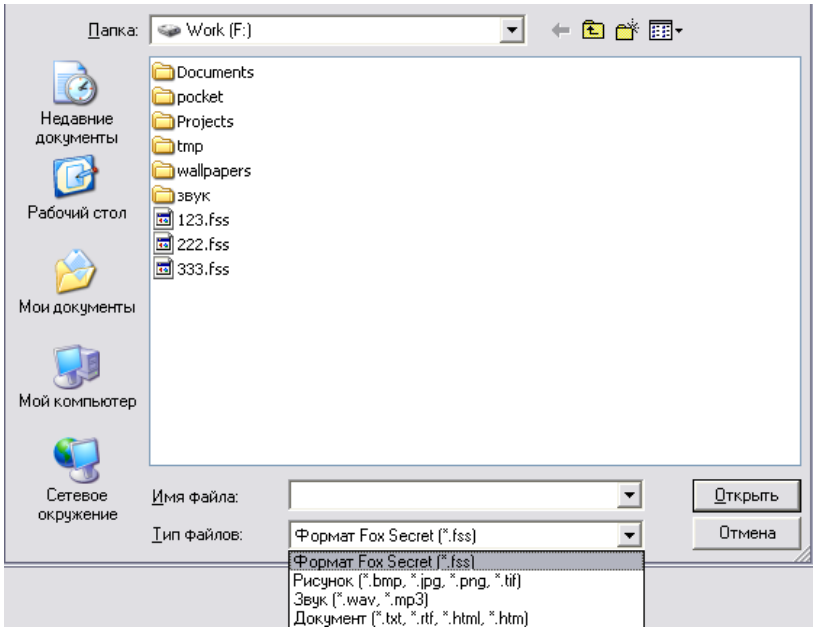

Рисунок 12 – Выбор файла с секретом

Как видно из картинки, Вам предлагается выбрать один файл из 4 групп и 10 форматов. Кроме первого формата - собственного формата Fox Secret, все остальные предполагают сокрытие данных.

Если секрет будет обнаружен и если его формат является корректным, то приложение проверяет тип шифрования секрета.

Если секрет зашифрован открытым ключом RSA, то будет предпринята попытка подобрать закрытый ключ из базы ключей RSA. В случае неудачи, будет выдано соответствующее предупреждение и секрет не будет открыт.

Для секретов, зашифрованных симметричным алгоритмом, появится диалог следующего этапа (Рис. 13).

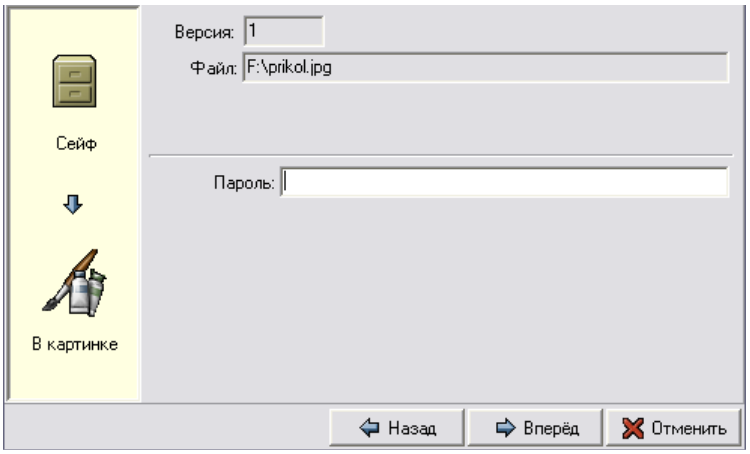

Рисунок 13 – Окно для ввода пароля

В этом окне Вам необходимо указать правильный пароль. Слева в окне Вам будет показан тип содержащегося секрета - текст, одиночный файл или сейф. Если пароль будет верен, то приложение перейдёт в режим редактирования и просмотра секрета.

6.4 Хранилище RSA ключей

Если после установки приложения на компьютер Вы ещё не работали с хранилищем RSA ключей, то Вам будет предложено его создать и назначить пароль (Рис.14).

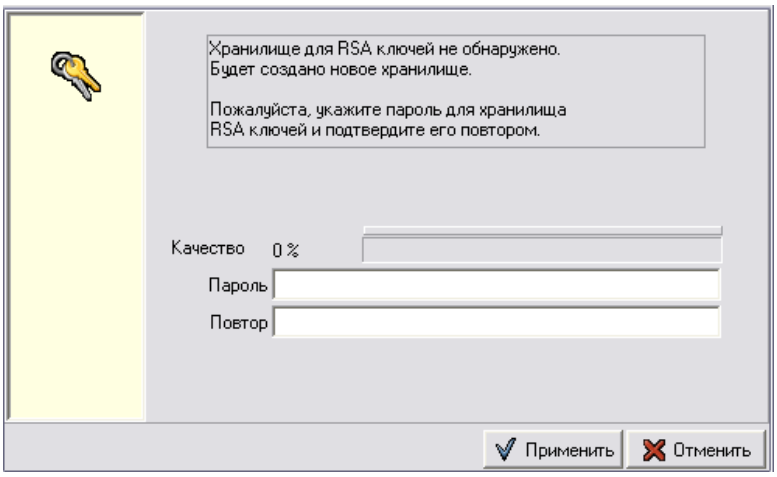

Рисунок 14 – Создание хранилища RSA ключей

Укажите в этом окне пароль на хранилище и подтвердите его повторным набором. Качество пароля указывается процентным и цветовым индикаторами.

Если же база ключей была ранее создана и ещё не открывалась, то появится следующий диалог (Рис.15).

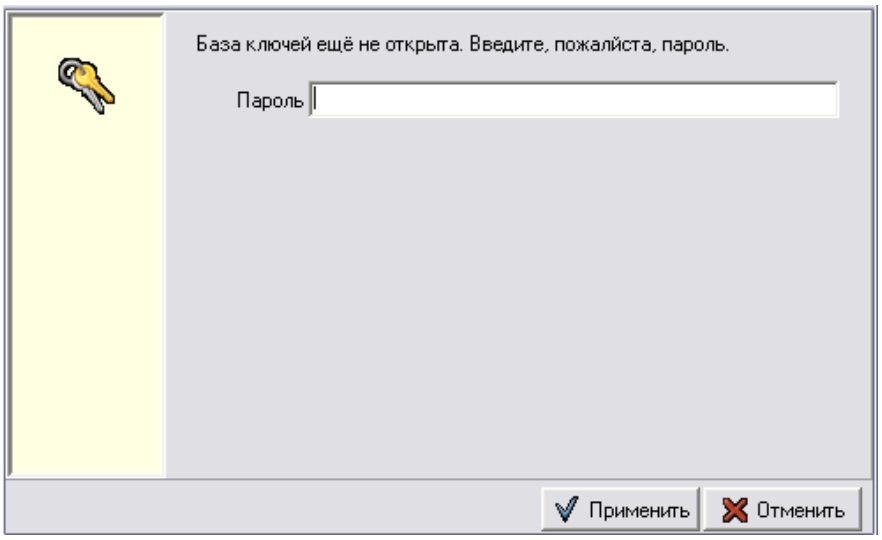

Рисунок 15 – Окно для ввода пароля

Здесь Вы должны будете указать пароль к хранилищу RSA ключей. В случае корректности пароля, появится окно редактора базы (рис.16).

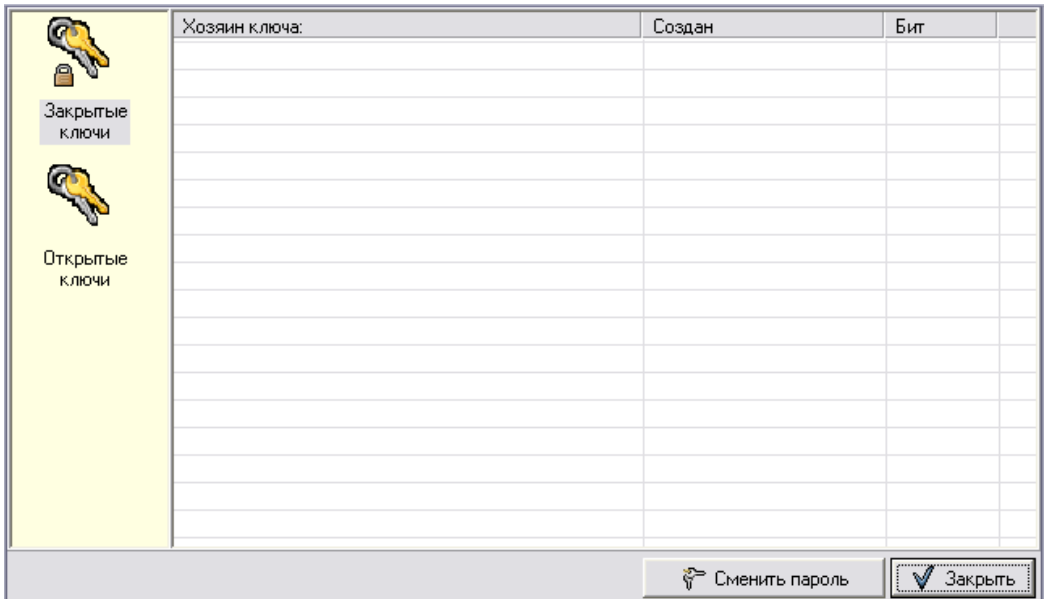

Рисунок 16 – Окно редактора базы

В редакторе Вам доступны закрытые и открытые ключи, вы можете сменить пароль на базу.

6.5 Всплывающее меню

В редакторе базы правым кликом мыши Вы можете вызвать специальное всплывающее меню (рис.17).

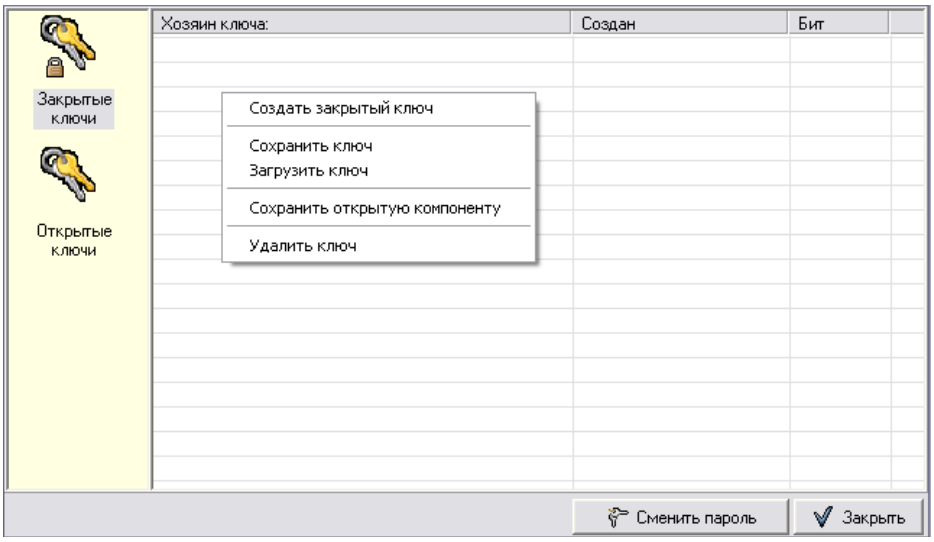

Рисунок 17 – Всплывающее меню

Рассмотрим подробнее эти команды:

Создать закрытый ключ - позволяет создать новый закрытый ключ. Для этого необходимо заполнить следующую форму (рис.18).

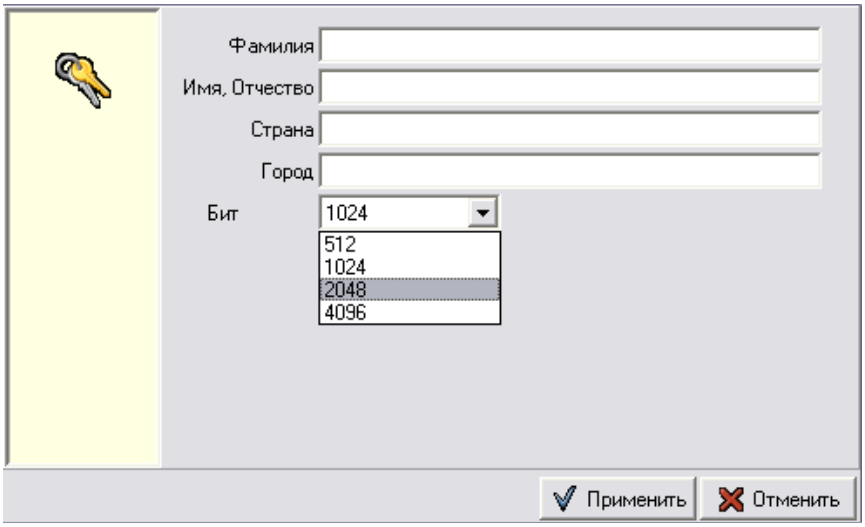

Рисунок 18 – Создание закрытого ключа

Будьте внимательны - после создания ключа его параметры нельзя будет изменить.

Сохранить ключ - позволяет сохранить выбранный ключ в отдельный файл. Будьте внимательны - закрытый ключ не должен попадать в чужие руки. Лучше поместите сохранённый ключ в отдельный зашифрованный секрет.

Загрузить ключ - загрузить ключ, сохранённый из приложения Fox Secret ранее, в Вашу базу ключей. Это может быть сохранённый Вами ранее ключ, или присланный Вам открытый ключ Вашим знакомым.

Сохранить открытую компоненту - позволяет отдельно в файл сохранить открытую компоненту закрытого ключа. Этот файл вы можете затем передать другому лицу, и он сможет загрузить его в своём приложении Fox Secret как Ваш открытый ключ. Таким образом он сможет проверять Ваши подписи и присылать Вам зашифрованные секреты Вашим открытым ключом.

Удалить секрет - удаляет безвозвратно выделенный ключ из списка.

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Для чего служит программный продукт Fox Secret?
2. Какие алгоритмы лежат в основе работы Fox Secret?
3. Каким образом шифруется сообщение?
4. Какие типы файлов можно использовать для скрытия данных?
5. Какие операции над секретами вам доступны в начале работы?
6. Какие типы секретов доступны в программе?
7. Какие типы контейнеров для помещения туда секретов реализуются в программе?
8. Как создать хранилище RSA ключей?
9. Как создать закрытый ключ?
10. Для чего используется всплывающее меню?
11. Как происходит восстановление исходных данных?
12. Для чего предназначена программа Fox Secret?