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 KREMLIN

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 Kremlin: 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 Kremlin. 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 – научиться применять программные криптосистемы шифрования, на примере программного продукта Kremlin.

2. ЗАДАНИЕ

Ознакомиться с теоретическим материалом. Произвести установку программного продукта Kremlin. Зашифровать текстовый файл, выбрав алгоритм шифрования и соответствующие параметры ключа. Отправить зашифрованное сообщение по электронной почте. Расшифровать криптограмму, удалить расшифрованную криптограмму, без возможности для восстановления, различными способами. Очистить историю работы на компьютере.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Зашифровать текстовый файл.
4. Расшифровать криптограмму.
5. Удалить расшифрованную криптограмму, без возможности для восстановления, различными способами.
6. Отправить зашифрованное сообщение по электронной почте.
7. Очистить историю работы на компьютере.
8. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Описание процесса выполнения работы со скриншотами.
4. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

Kremlin обеспечивает кросс-платформенный пакет безопасности для ПК. Он строит стену вокруг данных, защищая личную информацию от перехвата злоумышленниками.

Kremlin способен легко зашифровать-расшифровать файлы, простым перетаскиванием файлов. Зашифрованные файлы могут быть переданы легко между ПК.

Возможно также запрограммировать Kremlin так, чтобы файлы автоматически шифровались при выходе из системы компьютера и расшифровывать файлы, когда в систему снова вошли.

Kremlin имеет надежное удаление (корзина), позволяющее безопасно удалить файлы, так же конфиденциальность обеспечивается за счет стирания всех записей деятельности с жесткого диска и из памяти, когда произведен выход из системы или компьютер бездействует.

Использовать Kremlin, возможно еще и как защищенный полнофункциональный текстовый редактор для того, чтобы автоматически шифровать документы, заметки и сообщения электронной почты.

Единый графический интерфейс позволяет использовать Kremlin, не беспокоясь о компьютерной платформе. Kremlin обеспечивает построение надежной и экономически эффективную систему безопасности для защиты корпоративных и персональных данных.

5.2 Установка программы

Запустить программу KremlinInstaller.exe, после чего появится окно приветствия, представленное на рисунке 1.

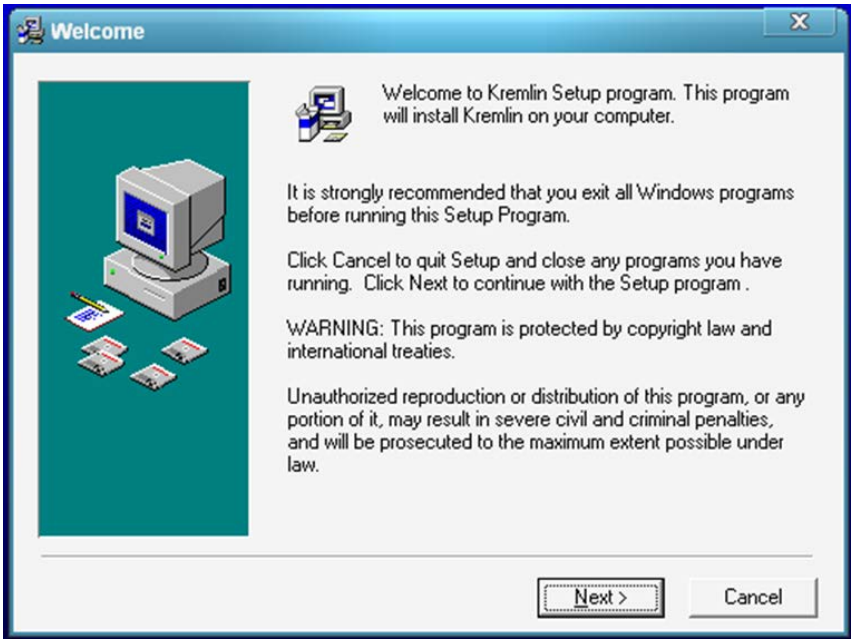

Рисунок 1 – Запуск программы

Нажав кнопку NEXT (Далее) переходим к окну лицензионного соглашения, представлено на рисунке 2.

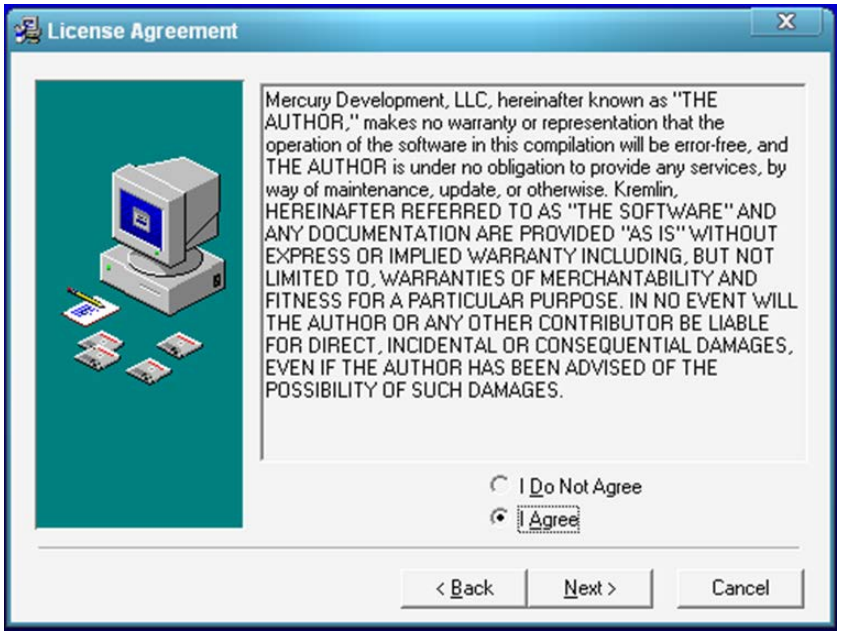

Рисунок 2 – Лицензионное соглашение

Ознакомившись с положением, нажимаем кнопку NEXT (Далее) и переходим к окну с заметками для пользователей ОС Win NT и пользователей версий (данной программы). Прочитав их, нажимаем кнопку NEXT (Далее). Определяем место установки программы, нажимаем NEXT (Далее), представлено на рисунке 3.

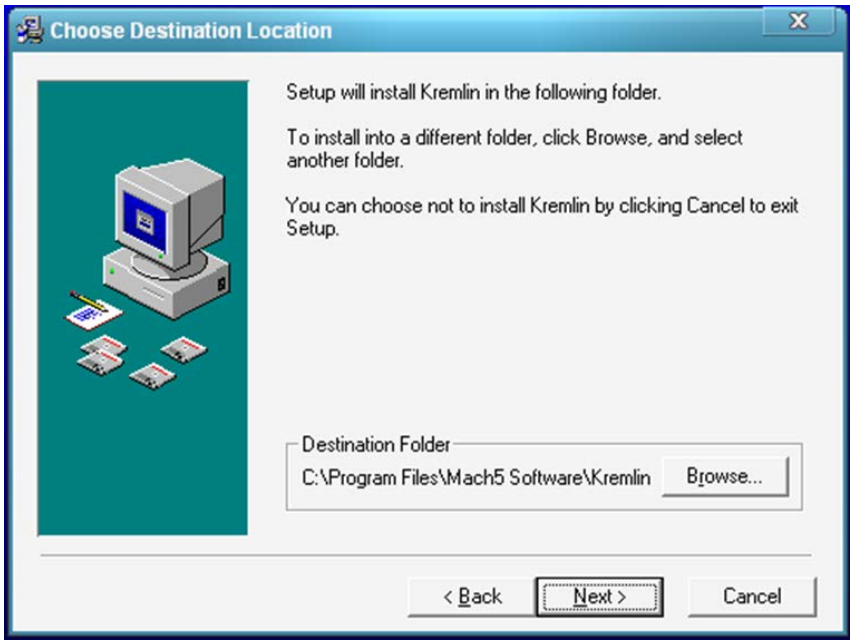

Рисунок 3 –Место установки

После проверки места для файлов программы, появится окно с запросом в какую группу ярлыков поместить ярлыки программы. Затем программа сообщит, что теперь она готова к установке, одобряем запрос кнопкой NEXT (Далее). После завершения копирования появится окно, благодарящее нас за установку Kremlin, которое представлено на рисунке 4. Снова нажимаем кнопку NEXT (Далее).

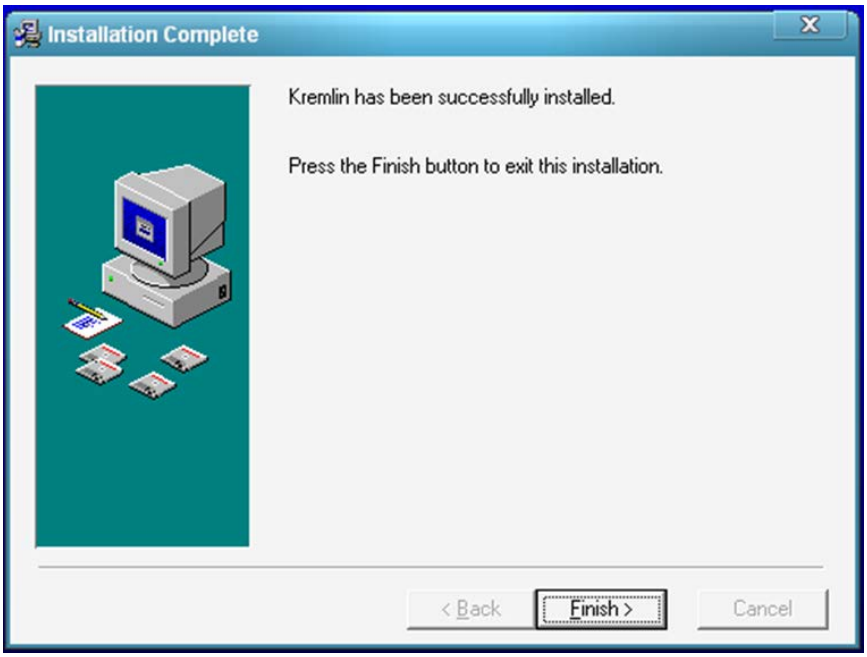

Рисунок 4 – Завершение установки

Следующий этап - возможность настроить комплекс при помощи Мастера Настройки. Появится окно Мастера Настройки, представленное на рисунке 5, - нажимаем кнопку NEXT (Далее).

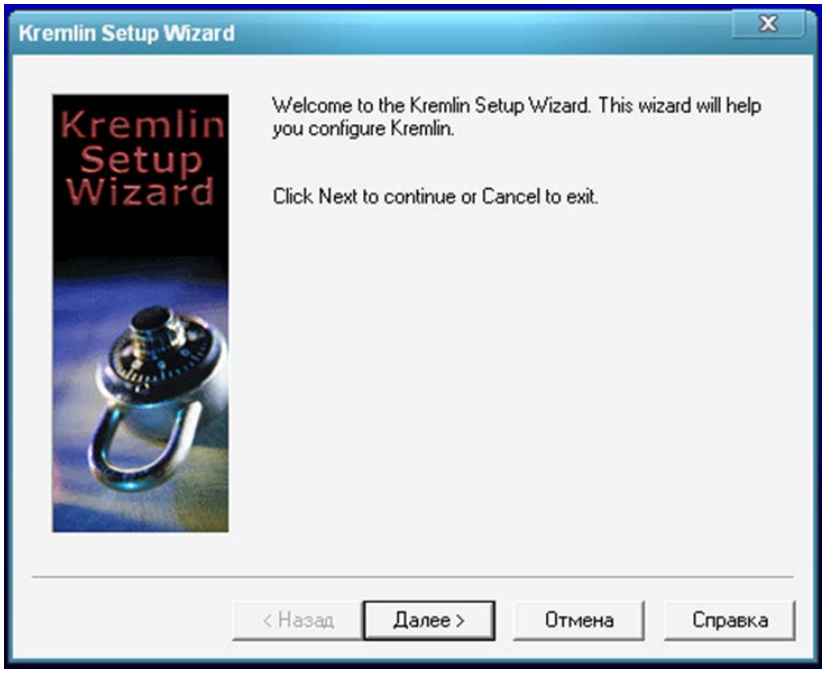

Рисунок 5 – Мастера Настройки

После очередного нажатия кнопки NEXT (Далее) появится окно, приглашающее внести список файлов и (или) каталогов, представленное на рисунке 6, которые будут автоматически зашифровываться при выключении компьютера и расшифровываться при его включении. Можно просто нажать кнопку NEXT (Далее) для того чтобы оставить этот список пустым, или нажать кнопку ADD (Добавить) для добавления в него файлов и каталогов.

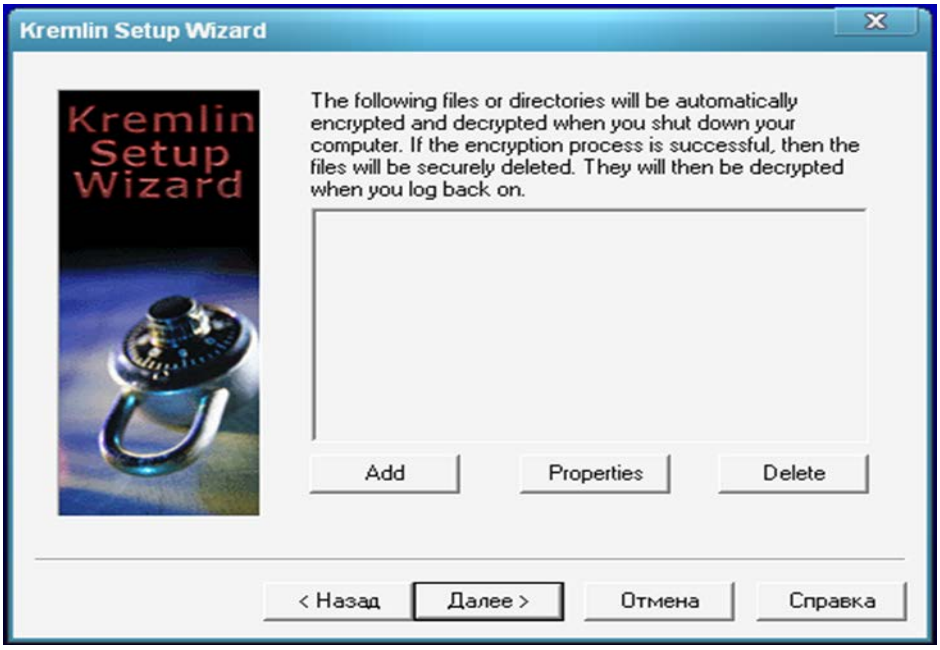

Рисунок 6 – Список автоматически зашифровываемых файлов

В появившемся окошке расположены переключатели алгоритмов шифрования, представленные на рисунке 7. Как видно доступен из них только один. Для того чтобы появились все остальные алгоритмы нужно зарегистрировать программу.

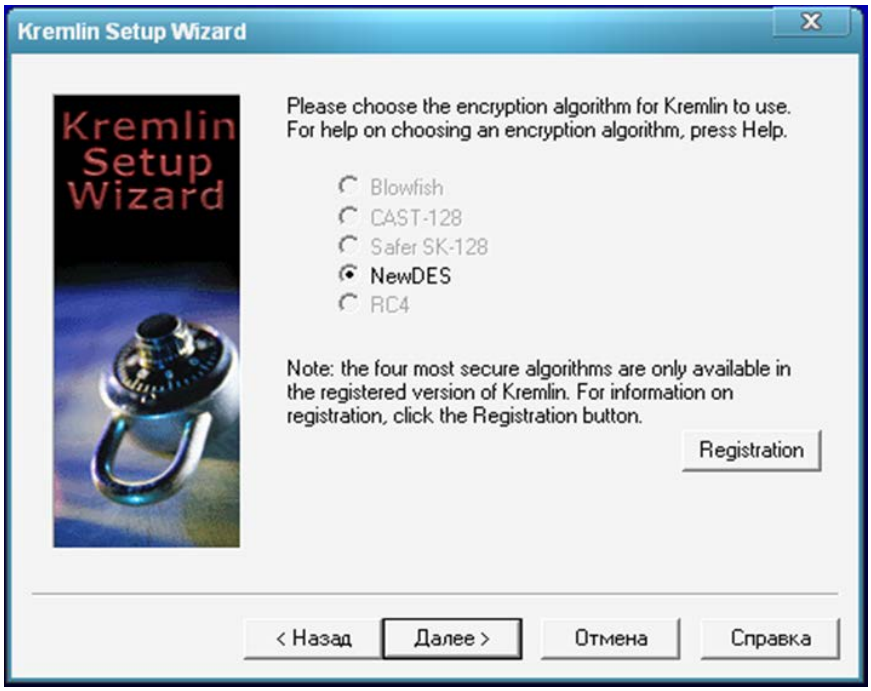

Рисунок 7 – Переключатели алгоритмов шифрования

После очередного нажатия кнопки NEXT (Далее) появится окно с кнопкой FINISH, нажатие на которую приведет к завершению работы мастера.

Запускаем через "Пуск" ("Start") программу Register Kremlin.

В появившемся окне вводим необходимые данные, которые необходимо скопировать из окна программы keygen.exe (рисунок 8). Установка завершена.

Рисунок 8 – Завершение установки

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Шифрование файлов

Kremlin Encrypt.exe – файл предназначенный для непосредственного шифрования файлов (каталогов), представленный на рисунке 9. Для шифровки необходимо "перетащить мышкой" шифруемый файл на значок программы или на его ярлык.

Рисунок 9 - Ярлык Kremlin Encrypt.exe

После чего выбрать алгоритм шифрования, вписать пароль два раза (для подтверждения), представлено на рисунке 10. Для того чтобы уничтожить исходный (шифруемый) файл (оригинал), надо при шифрации в окне программы шифрации поставить галочку в строке: Delete source file(s). Зашифрованный файл получает расширение *.KGB.

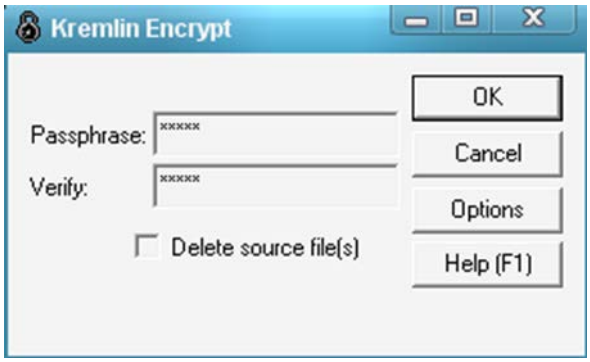

Рисунок 10 – Пароль подтверждения

6.2 Безвозвратное удаление файлов

Kremlin Wipe.exe - предназначена для затирания областей данных как в памяти (RAM) так и на диске (делает их недоступными для восстановления), представлено на рисунке 11.

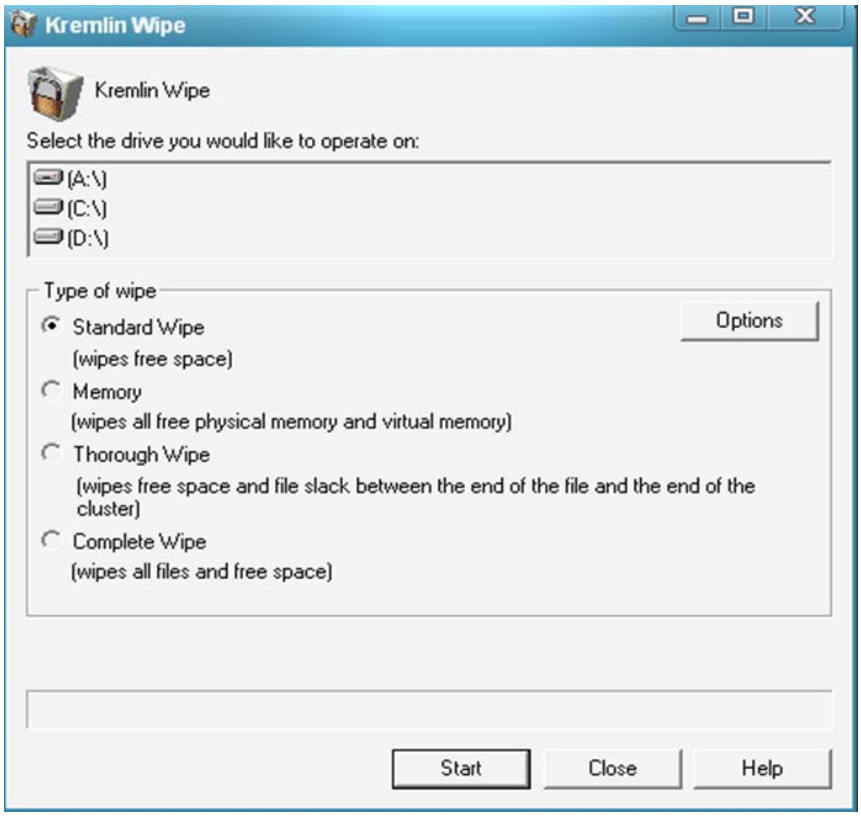

Рисунок 11- Диалоговое окно

Имеет следующие переключающиеся режимы затирания:

• STANDART WIPE - сервисная программа, предназначенная для безвозвратного удаления ненужных данных с диска и из памяти.

Предназначение: после обычного удаления файлов (не в Корзину, а через Shift+Del), их также удаётся восстановить, так как на самом деле данные, содержащиеся в файле всё ещё остаются на диске, удаляется лишь имя файла из Таблицы Размещения Файлов (FAT), т.е. он становится невидимым и находится в так называемой "свободной" области диска. После обработки такого типа данные удалённого файла исчезают (затираются - поверх этих данных записываются случайные данные типа 0...1...00...111 и т.п. и так несколько раз).

• MEMORY - затирание всей свободной оперативной памяти и абсолютно всей виртуальной памяти.

Предназначение: Злоумышленник может прочесть открытые вами файлы из оперативной памяти компьютера, которые случайно там "застряли" после их закрытия и удаления, или как минимум узнать выполненные вами действия, если компьютер после этого

(удаления файлов) не выключали. Естественно что через файл подкачки всё это можно узнать и после выключения компьютера.

- THOROUGHT WIPE - вытирает свободное пространство и информацию между концом файла и кластером.

Весь диск на котором хранятся данные разделён на маленькие ячейки памяти именуемые как "кластеры". Эти кластеры имеют строго определённый размер, который зависит от ёмкости диска и варьирует от 4-ёх Кбайт до 32-ух Кбайт (в Windows NT может быть и 64 Кбайт). Каждый файл занимает один и более кластеров, в зависимости от своего размера. В один кластер может быть записан только один файл. Здесь-то и вся загвоздка... Представим себе такой вариант: кластер 16 Кбайт, а файл имеет размер 6 Кбайт, он все равно занимает один кластер, т.е. свободная область в этом кластере (10 Кбайт) потеряна и остаётся свободной. Но если до этого в этом кластере уже была записана информация (от старого файла) и новый файл лишь перезаписывает её, то естественно, что в недописанных участках данного кластера (в нашем случае 10 Кбайт) останутся данные старого файла...

Так вот с помощью этого метода затираются не только свободные области диска, но и свободные области недописанных кластеров. Замечу только, что эту операцию программа не может выполнять по отношению к скрытым и системным файлам.

Предназначение: Как уже было сказано после обычного удаления файлов их удаётся восстановить, так как на самом деле данные, содержащиеся в файле всё ещё остаются на диске, но при записи новых файлов на диск они (новые файлы) записываются поверх той области, где находились данные старого (удалённого) файла. При этом частично заполненные кластеры могут содержать данные старого (удалённого) файла, что может стать достоянием злоумышленника.

- COMPLETE WIPE - вытирает все файлы и свободное пространство с многократным перезатирание файлов (количество перезаписи можно выбрать в меню, вызываемом кнопкой Options).

Предназначение: Стоит заметить, что нужно быть осторожным с данной программой, так как данные после её применения восстановить невозможно. Время затирания одного

диска зависит от количества перезатирания, а также от скорости работы винчестера.

Kremlin Secure Recycle Bin.exe – это корзина для удаления файлов. Все файлы (или целые каталоги) "брошенные" в эту корзину уже не вернуть, т.е. это есть аналог того же Wiping-а, но не для всего диска, а для определённых файлов и папок, а для удобства эта программа сделана в виде корзины, ярлык которой представлен на рисунке 12.

Рисунок 12 – Ярлык исполняемого файла

6.3 Отправка зашифрованных сообщений

Утилита Kremlin Text.exe - предназначена для отправки зашифрованной почты и сообщений. Принцип работы следующий. Вводим текст, нажимаем кнопку Encrypt для шифрации текста, представлено на рисунке 13.

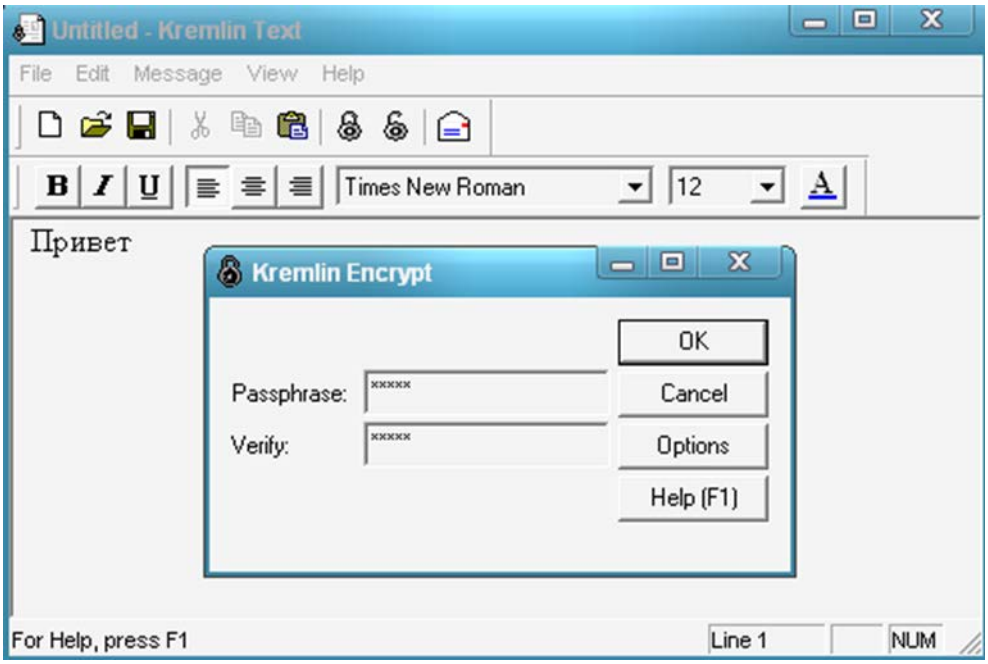

Рисунок 13 – Диалоговое окно

Затем используем кнопку Send Mail для отправки письма. В появившемся окне вводим адрес получателя, тему сообщения, а также (если вы не ввели их до этого) свое имя, свой почтовый адрес и имя SMTP сервера, представлено на рисунке 14. Поставив галочку в строке Remember your name, e-mail address, and SMTP server вы можете сделать эти значения используемыми по умолчанию (если до этого значения по умолчанию были другими, они будут заменены).

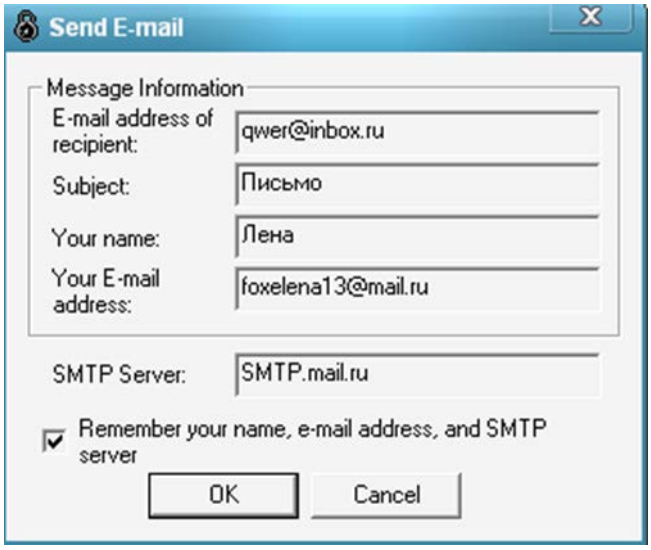

Рисунок 14 – Ввод данных

Предназначение: Злоумышленник может перехватить вашу почтовую переписку или просто взломать ваш почтовый ящик, но ничего ценного для себя (без ключа дешифрации конечно) он там не найдет.

6.4 Очистка истории работы на компьютере

Kremlin Sentry.exe - предназначена для уничтожения "следов" работы на компьютере. После выполнения определённых действий: поиска файлов на диске, использования команды "Выполнить", открытия различных файлов (документов, рисунков, музыкальных файлов), работы в Интернет и т.п., в компьютере остаётся история работы пользователя: какие файлы искались, открывались, скачивались из Интернет, какие сайты были

посещены, какие команды выполнялись и т.п. Данная программа уничтожает всю эту историю в соответствии с настройками, произведёнными в ней (может стереть все истории, а может и не все - выбор за Вами).

Настройка:

Следует запустить программу двойным щелчком по ней, или по её ярлыку (как и для всех программ), затем в системном лотке (где находятся часы) кликнуть двойным щелчком по появившемуся "замочку", представлено на рисунке 15.

Рисунок 15 – Вызов меню настройки

Появится меню настройки программы, представлено на рисунке 16 (в то же меню можно попасть с помощью программы Kremlin Options).

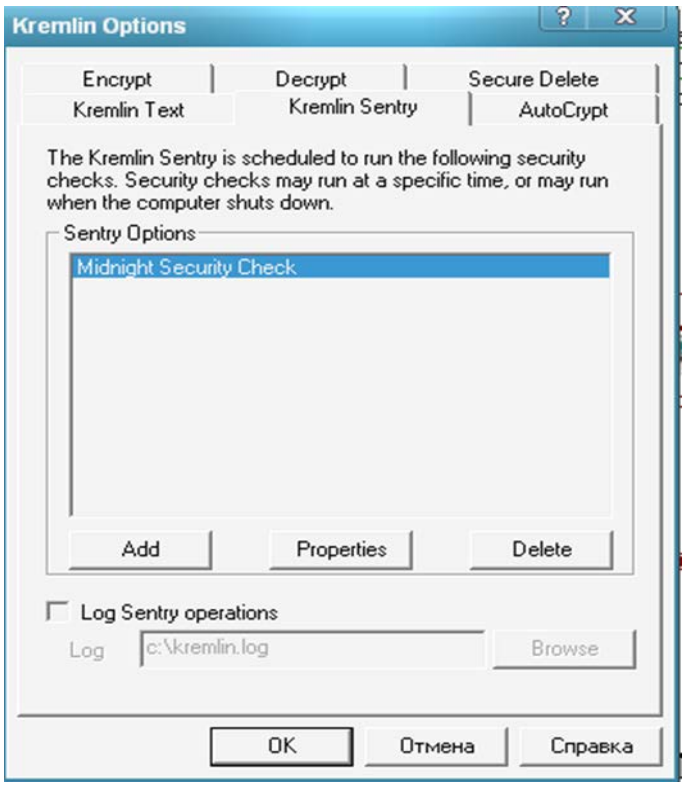

Рисунок 16 – Меню настройки программы

С помощью кнопки ADD создаём действие для программы - это операция с помощью которой мы избавимся от ненужной информации содержащейся на компьютере. В появившемся окне можно выбрать когда именно проводить данную операцию, представлено на рисунке 17.

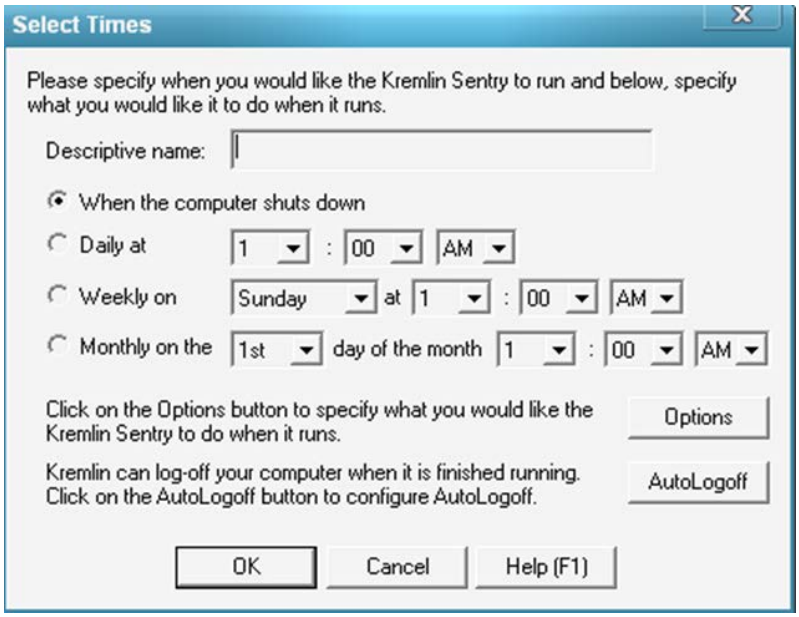

Рисунок 17 – Меню настройки параметров

When the computer shuts down - когда будет выключаться компьютер

Daily at HH : MM : AM/PM - ежедневно в "HH" часов "MM" минут "до полудня/после полудня"

Weekly on XXXX at HH : MM : AM/PM - еженедельно в "XXXX" день недели, в "HH" часов "MM" минут "до полудня/после полудня"

Monthly on the XX day of the month HH : MM : AM/PM - ежемесячно в "XX" день месяца, в "HH" часов "MM" минут "до полудня/после полудня"

Необходимо задать "Имя" для выполняемой операции в строке Descriptive name. Имя для операции (если оно несет в себе какой-либо смысл) позволит нам быстро понять, что именно она выполняет. Можно создавать несколько операций на одном компьютере для проведения разных действий в различное время.

Нажимаем кнопку AutoLogoff для того чтобы выбрать что именно должна сделать программа после завершения назначенной операции (заметьте для каждой операции такое действие может быть различным):

Shutdown the computer (turn it off) - выключить компьютер;

Restart the computer - перезагрузить компьютер;

Logoff the computer - войти под другим именем компьютер.

Вне зависимости от того какое действие вы выбрали при завершении работы с компьютером - перезагрузку, завершение сеанса или выключение, будет выполняться то действие которое вы установили данной опцией.

После нажатия кнопки Options появляется окошко в верху которого три переключателя, позволяющих выбрать на каких дисках и каким методом проводить wiping, и проводить ли его вообще, представлено на рисунке 18. Ниже можно установить галочку в строке Wipe all memory (wipes all avialabel physical and virtual memory) – для wiping-а доступной оперативной и всей виртуальной памяти (см. подробнее о wiping-е в разделе Kremlin Wipe.exe). Можно также установить галочку в строке Clear Windows and Browser Histories для уничтожения "следов" работы на компьютере. Кнопка Details позволяет определить программе какую историю уничтожать.

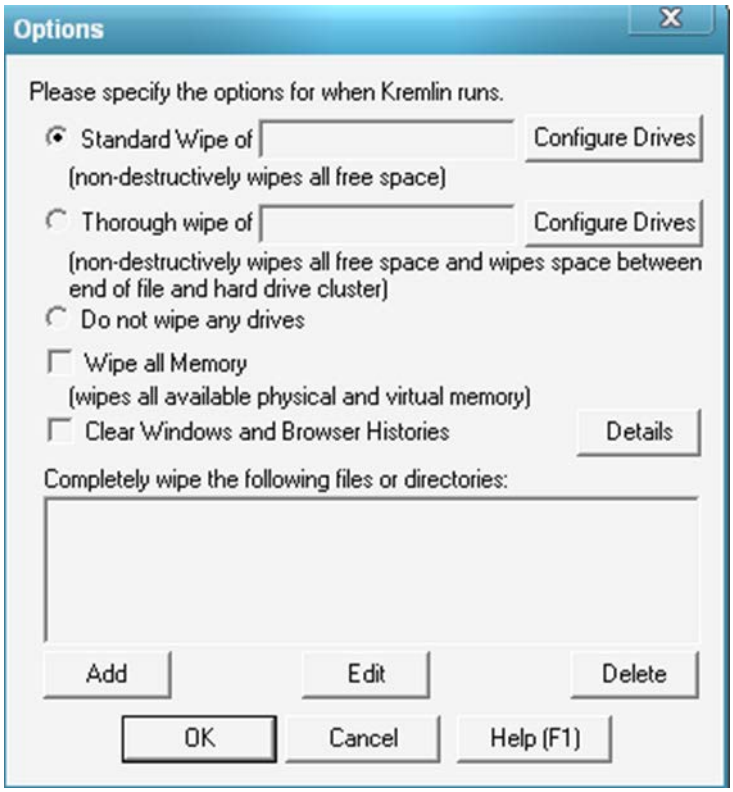

Рисунок 18 – Подтверждение параметров

Далее в самом низу окна находится небольшое окошко, в котором указаны файлы и (или) папки которые программа будет автоматически затирать (wiping) при завершении работы компьютера. Нажатие кнопки ADD выводит окно в котором Вы выбираете что именно файл или папку следует затереть, а затем кнопкой Browse указываете какой именно файл или папка подлежит wiping-у.

Нажатие кнопки EDIT на предварительно выделенном файле или папке позволяет изменить его название или расположение (переустановить задание для программы).

Нажатие кнопки DELETE на предварительно выделенном файле или папке позволяет удалить его (её) из списка затираемых.

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие программные криптосистемы шифрования вы знаете, назовите их.
2. Назовите основные функциональные возможности Kremlin?
3. Перечислите исполняемые файлы Kremlin?
4. Как осуществляется шифрование файлов?
5. Как происходит отправка зашифрованных сообщений?
6. С помощью каких процедур осуществляется безвозвратное удаление файлов?
7. Какими методами возможна очистка истории работы на компьютере при помощи Kremlin?
8. Какие функции КМИЗ выполняет Kremlin?