МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ижевский государственный технический университет
имени М.Т.Калашникова»
Кафедра «Программное обеспечение»

Отчет
по лабораторной работе №1
на тему: «Сравнительная таблица программных продуктов»
по дисциплине: «Управление программными проектами»

Выполнил:
студенты группы Б17-191-1: А.В.Елесина
Е.О.Овсейко
Принял:
старший преподаватель М. О. Еланцев

Ижевск 2020

1. ПОСТАНОВКА ЗАДАЧИ

1) Разработать документ содержащий:

- Название проекта
- Краткое описание сути проекта (2-3 предложения)
- Цель (одна)
- Аналитический обзор
    - не менее 4-ех конкурентов или альтернатив
    - сводная таблица сравнения функциональных возможностей
- Результаты проекта
    - в каком виде реализовано (сайт, мобильное приложение, десктопное приложение, может быть несколько)
    - ~10-15 ключевых характеристик/свойств продукта. Должны быть достижимыми и проверяемыми
- Задачи проекта (~3-4).
- Допущения и ограничения

2) Разработать презентацию продукта, содержащую слайды:

- Название (1 слайд)
- Описание проблемы, которая решается вашим продуктом (1-2 слайда)
- Продукт проекта (1-2 слайда). Опишите, как именно продукт проекта будет решать проблему
- Целевая аудитория (1 слайд)
- Команда проекта: ключевые компетенции и опыт (1 слайд)
- Слайд "Спасибо за внимание"

2. ПРОЕКТ

1. *Название проекта*: DarkCript

2. *Краткое описание*:

DarkCript - программа для защиты информации, использующая современные алгоритмы шифрования (RSA, AES, BlowFish и др.). Предоставляемый DarkCript набор инструментов и функций применяется во всех сферах работы с информацией: защита

конфиденциальной информации, защита E-mail корреспонденции, создание и проверка цифровых подписей.

3. *Цель*: уменьшение вероятности утечек данных пользователя в открытый доступ

4. *Результат проекта*: десктопное приложение

5. *Ключевые функциональные характеристики*:

1) Шифрование по стандарту ГОСТ (длина ключа 128 бит) и сертифицированного криптопровайдера КриптоПро, что позволяет использовать программу не только частным лицам и коммерческим организациям, но и государственным учреждениям.

2) Сокрытие файлов и папок от других пользователей и трекеров в интернете

3) Шифрование сообщений, голосовых сообщений и вложеных файлов отправленных с помощью почтовых клиентов и месенджеров: email, Viber, WhatsApp

4) Создание зашифрованных «бумажников», хранящих информацию о банковских счетах и картах, кредитах и др. Финансовой информации

5) Создание зашифрованных «паспортов», хранящих информацию о страховке, паспорте, загранпаспорте,медицинском полисе, ИНН и др. Документов с персональными данными

6) Создание защищенных USB/CD/DVD-дисков/жестких дисков

7) Возможность подписания файлов электронной цифровой подписью (ЭЦП) и ее проверка

8) Двухфакторная аутентификация пользователя.

9) Поддерживает набор инструкций AES-NI, что положительно сказывается на производительности программы

10) Система доверенных приложений, позволяющая разрешить доступ к зашифрованным файлам только определенным приложениям.

11) Интеграция с облачным решением управления ключами: все ключи и секреты создаются, управляются и хранятся в облачном хранилище.

6. *Задачи проекта*:

- Создать хорошо защищенные портфели с финансовыми данными, данными о личности которые можно было бы использовать в любой момент времени
- Реализовать защиту, проверку и возможность использование ЭЦП на файлах
- Реализовать алгоритмы шифрования RSA, AES, BlowFish и др. по ГОСТ стандарту
- Реализовать двухфакторную идентификацию

7. *Допущения*:

- Вы доверяете облачному решению по управлению ключами создавать, хранить секреты и ключи организации, а также управлять ими.
- Вы разрешаете доступ к облачной системе управления ключами всем локальным приложениям и службам, которые зависят от служб шифрования или секретов.
- Если у вас есть конфиденциальные данные, которые не должны попадать в журналы трафика или другие диагностические отчеты, предоставляемые ИТ-специалистам, следует шифровать весь трафик между ресурсами в виртуальной сети.
- Вы храните данные, которые не предназначены для повсеместного использования.
- Рабочие нагрузки имеют запас на дополнительную задержку, вызванную шифрованием дисков.

8. *Ограничения*:

- Объемы данных, которые можно зашифровать за 1 раз ограничены в связи с поддержанием эффективной работы ПО
- Не поддерживает системы ниже, чем Windows 8

3. АНАЛИЗ КОНКУРЕНТОВ

1) «CyberSafe Top Secret»

Преимущества программы CyberSafe Top Secret:

+Поддержка алгоритмов шифрования ГОСТ и сертифицированного криптопровайдера КриптоПро, что позволяет использовать программу не только частным лицам и коммерческим организациям, но и государственным учреждениям.

+Поддержка прозрачного шифрования папки, что позволяет использовать программу в качестве замены EFS. Учитывая, что программа обеспечивает лучший уровень производительности и безопасности, такая замена более чем оправдана.

+Возможность подписания файлов электронной цифровой подписью и возможность проверки подписи файла.

+Встроенный сервер ключей, позволяющий публиковать ключи и получать доступ к другим ключам, которые были опубликованы другими сотрудниками компании.

+Возможность создания виртуального зашифрованного диска и возможность шифрования всего раздела.

+Возможность создания самораспаковывающихся архивов.

+Возможность бесплатного облачного резервного копирования, которое работает с любым сервисом — как платным, так и бесплатным.

+Двухфакторная аутентификация пользователя.

+Система доверенных приложений, позволяющая разрешить доступ к зашифрованным файлам только определенным приложениям.

+Приложение CyberSafe поддерживает набор инструкций AES-NI, что положительно сказывается на производительности программы (этот факт будет продемонстрирован далее).

+Драйвер программы CyberSafe позволяет работать по сети, что дает возможность организовать корпоративное шифрование.

+Русскоязычный интерфейс программы. Для англоязычных пользователей имеется возможность переключения на английский язык.

Недостатки программы:

- иногда в программе «проскакивают» нелокализированные сообщения вроде «Password is weak».

- программа не умеет шифровать системный диск

2) «Folder Lock»

Основные возможности программы Folder Lock следующие:

- AES-шифрование, длина ключа 256 бит.
- Сокрытие файлов и папок.
- Шифрование файлов (посредством создания виртуальных дисков — сейфов) «на лету».
- Резервное копирование онлайн.
- Создание защищенных USB/CD/DVD-дисков.
- Шифрование вложений электронной почты.
- Создание зашифрованных «бумажников», хранящих информацию о кредитных картах, счетах и т.д.

Преимущества программы Folder Lock:

+Привлекательный и понятный интерфейс, который понравится начинающим пользователям, владеющим английским языком.

+Прозрачное шифрование «на лету», создание виртуальных зашифрованных дисков, с которыми можно работать, как с обычными дисками.

+Возможность резервного онлайн-копирования и синхронизации зашифрованных контейнеров (сейфов).

+Возможность создания саморасшифровывающихся контейнеров на USB/CD/DVD-дисках.

Недостатки программы:

- Нет поддержки русского языка, что усложнит работу с программой пользователей, не знакомых с английским языком.

- Сомнительные функции Lock Files (которая просто скрывает, а не «запирает» файлы) и Make Wallets (малоэффективна без экспорта информации). Честно говоря, думал, что функция Lock Files будет обеспечивать прозрачное шифрование папки/файла на диске, как это делает программа CyberSafe Top Secret или файловая система EFS.

- Отсутствие возможности подписания файлов, проверки цифровой подписи.

- При открытии сейфа не позволяет выбрать букву диска, которая будет назначена виртуальному диску, который соответствует сейфу. В настройках программы можно

выбрать только порядок, в котором программа будет назначать букву диска — по возрастанию (от A до Z) или по убыванию (от Z до A).

- Нет интеграции с почтовыми клиентами, есть только возможность зашифровать вложение.

- Высокая стоимость облачного резервного копирования.

3) «PGP Desctop»

Программа PGP Desktop от Symantec — это комплекс программ для шифрования, обеспечивающий гибкое многоуровневое шифрование. Программа встраивается в оболочку (Проводник), а доступ к ее функциям осуществляется через контекстное меню Проводника

Разделы программы:

1) PGP Keys — управление ключами (как собственными, так и импортированными с keyserver.pgp.com).

2) PGP Messaging — управление службами обмена сообщениями. При установке программа автоматически обнаруживает ваши учетные записи и автоматически шифрует коммуникации AOL Instant Messenger.

3) PGP Zip — управление зашифрованными архивами. Программа поддерживает прозрачное и непрозрачное шифрование. Этот раздел как раз и реализует непрозрачное шифрование. Вы можете создать зашифрованный Zip-архив (PGP Zip) или саморасшифровывающийся архив (рис. 17).

4) PGP Disk — это реализация функции прозрачного шифрования. Программа может, как зашифровать весь раздел жесткого диска (или даже весь диск) или создать новый виртуальный диск (контейнер). Здесь же есть функция Shred Free Space, которая позволяет затереть свободное пространство на диске.

5) PGP Viewer — здесь можно расшифровать PGP-сообщения и вложения.

6) PGP NetShare — средство «расшаривания» папок, при этом «шары» шифруются с помощью PGP, а у вас есть возможность добавить/удалить пользователей (пользователи идентифицируются на основе сертификатов), которые имеют доступ к «шаре».

Преимущества программы PGP Desktop:

+ Полноценная программа, использующаяся для шифрования файлов, подписания файлов и проверки электронной подписи, прозрачного шифрования (виртуальные диски и шифрование всего раздела), шифрования электронной почты.

+ Поддержка сервера ключей keyserver.pgp.com.

+ Возможность создания саморасшифровывающихся архивов.

+ Возможность шифрования системного жесткого диска.

+ Функция PGP NetShare.

+ Возможность затирания свободного места.

+ Тесная интеграция с Проводником.

Недостатки программы:

- Отсутствие поддержки русского языка, что усложнит работу с программой пользователям, которые не знают английский язык.

- Нестабильная работа программы.

- Низкая производительность программы.

- Есть поддержка AOL IM, но нет поддержки Skype и Viber.

- Уже расшифрованные письма остаются незащищенными на клиенте.

- Защита почты работает только в режиме перехвата, который быстро вам надоест, поскольку окно защиты почты будет появляться каждый раз для каждого нового сервера.

4) «BitLocker»

BitLocker шифрует том, а не физический диск. Том может занимать часть диска, а может включать в себя массив из нескольких дисков.

BitLocker является стандартным компонентом Windows Professional и серверных версий Windows, а значит в большинстве случаев корпоративного использования он уже доступен. В противном случае вам понадобится обновить лицензию Windows до Professional

У BitLocker есть два неоспоримых преимущества: во-первых, им можно управлять через групповые политики; во-вторых, он шифрует тома, а не физические диски. Это

позволяет зашифровать массив из нескольких дисков, чего не умеют делать некоторые другие средства шифрования. Также BitLocker поддерживает GUID Partition Table (GPT), чем не может похвастаться даже наиболее продвинутый форк «Трукрипта» VeraCrypt. Чтобы зашифровать с его помощью системный GPT-диск, придется сначала конвертировать в формат MBR. В случае с BitLocker это не требуется.

В целом, недостаток один — закрытые исходники. Если шифровать домашний диск BitLocker отлично подойдет. Если же твой диск забит документами государственной важности, лучше подыскать что-то другое.

Таблица №1. Сравнительная таблица функциональностей ПО

Сравнительные характеристики	«DarkCript »	«CyberSafe Top Secret»	«Folder Lock»	«PGP Desktop»	«BitLocker»
Trial версия (free)	Да	Да	Да	Да	Нет
Виртуальные зашифрованные диски	Да	Да	Да	Да	Да
Шифрование всего раздела	Да	Нет	Да	Да	Да
Шифрование системного диска	Да	Нет	Да	Нет	Да
Интеграция с почтовыми клиентами	Да	Нет	Нет	Да	Нет
Шифрование сообщений электронной почты	Да	Да (ограничено)	Да	Да	Да
Шифрование файлов	Да	Нет	Да	Да	Да
ЭЦП, подписание	Да	Нет	Да	Да	Нет
ЭЦП, проверка	Да	Нет	Да	Да	Нет
Прозрачное шифрование папки	Нет	Нет	Нет	Да	Нет
Самораспаковывающиеся архивы	Нет	Да	Да	Да	Нет
Облачное резервное копирование	Да	Да (платно)	Нет	Да (бесплатно)	Нет
Система доверенных приложений	Нет	Нет	Нет	Да	Нет
Поддержка сертифицированного	Да	Нет	Нет	Да	Нет

криптопровайдера					
Поддержка токенов	Нет	Нет	Нет (поддержка прекращена)	Да (при установке КриптоПро)	Нет
Собственный сервер ключей	Нет	Нет	Да	Да	Да
Двухфакторная аутентификация	Да	Нет	Нет	Да	Нет
Сокрытие отдельных файлов	Да	Да	Нет	Нет	Да
Сокрытие разделов жесткого диска	Да	Да	Нет	Да	Да
Бумажники для хранения платежной и персональной информации	Да	Да	Нет	Нет	Нет
Поддержка шифрования ГОСТ	Да	Нет	Нет	Да	Нет
Русский интерфейс	Да	Нет	Нет	Да	Да
Последовательная чтение/ запись (DiskMark), Мб/с	-	47/42	35/27	62/58	70/80
Стоимость	-	40$	180-250$	50$	Включена в стоимость ОС