Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Математики, физики и информационных технологий
(институт)
Прикладная математика и информатика
(кафедра)
09.03.03 Прикладная информатика
(код и наименование направления подготовки, специальности)
Бизнес-информатика
(наименование профиля, специализации)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему «Проект внедрения системы шифрования данных в ООО «Новая высота»»

Студент И.В. Агафонов _____
(И.О. Фамилия) (личная подпись)

Руководитель О.В. Аникина _____
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заведующий кафедрой к.т.н., доцент, А.В. Очеповский _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)

«_____»_____20_____г.

Тольятти 2018

Аннотация

Бакалаврская работа на тему: «Проект внедрения системы шифрования данных в ООО «Новая высота»». Работа включает: 46 страниц, 3 таблицы, 22 рисунка, 2 приложения, 5 англоязычных и 20 русскоязычных используемых источников литературы.

Ключевые слова: алгоритм, шифрование, ключи, криптография, ПО, угрозы, внедрение, тестирование, несанкционированный доступ.

Объект исследования – это документооборот бухгалтерского отдела предприятия «Новая высота».

Предмет исследования – это программный комплекс предприятия, а конкретно бухгалтерского отдела.

В первой главе представлена характеристика и вид деятельности организации, построена организационная структура. Рассмотрен документооборот бухгалтерского отдела, проведен сравнительный анализ программ шифрования данных.

Вторая глава содержит описание алгоритма работы программы, построение диаграмм вариантов использования и последовательностей действий. Описание этапов внедрения и тестирование программы.

Третья глава посвящена оценки и обоснованию экономической эффективности проекта.

Цель работы: внедрение программы шифрования для передачи исходящих документов бухгалтерского отдела по сети Интернет в организации ООО «Новая высота». По результатам сравнительного анализа предложена лицензированная программа шифрования, удовлетворяющая потребности организации.

Практическая ценность бакалаврской работы заключается в том, что внедрение ПО реализовано и программа готова к использованию с целью обеспечения защиты передаваемых данных организации.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Шифрование данных – это актуальная тема программирования, так как защита информации давно стала актуальной и является такой и по сей день. Интернет постоянно развивается, хищение личных данных и конфиденциальной информации будет происходить постоянно.

Актуальность темы обусловлена необходимостью повышения защиты исходящих документов бухгалтерского отдела организации для передачи по сети Интернет.

Многие предприятия постоянно озабоченны усилением защиты собственных данных. Специально под конкретные предприятия и определенный типы файлов проводятся работы по шифрованию (разработки или внедрения), но чаще всего алгоритм не распространяется.

Целью данной работы является адаптация и тестовое внедрение программы шифрования для передачи исходящих документов бухгалтерского отдела по сети Интернет.

Для достижения поставленной цели необходимо решить следующие **задачи:**

1) Проанализировать научную и учебно-методическую литературу, необходимую для внедрения программы шифрования.

2) Провести анализ документооборота бухгалтерии.

3) Определить необходимость внедрения программного обеспечения (ПО).

4) Адаптировать программу шифрования файлов выбранными средствами.

5) Провести тестирование программы.

6) Определить эффективность программы шифрования в работе предприятия.

Задача повысить защищенность конфиденциальных данных предприятия. **Объект исследования** – это документооборот бухгалтерского отдела предприятия «Новая высота». **Предмет исследования** – это программный комплекс предприятия, а конкретно бухгалтерского отдела.

В первой главе будет рассмотрен документооборот в бухгалтерском отделе, характеристика организации, вид деятельности организации, основные бизнес процессы, организационная структура предприятия и будет произведен сравнительный анализ программ.

Во второй главе будет рассмотрено внедрение и реализация проектных решений, логическое моделирования бизнес-процесса шифрования файлов, реализация ПО.

В третьей главе будет оценка и обоснование экономической эффективности проекта.

Глава 1 Технико-экономическая характеристика деятельности предприятия ООО «Новая высота»

1.1 Технико-экономическая характеристика ООО «Новая высота»

В 2013 году стала развиваться одна из значимых компаний для Пермского края по поставкам строительного и промышленного оборудования - ООО «Новая высота». Чтобы стать ключевых игроком на рынке, компания в течение нескольких лет зарабатывала репутацию и стала надежным партнером для своих клиентов.

На данный момент ООО «Новая высота» может насчитать в своём портфеле десятки заключенных контрактов с самыми известными производителями строительного и промышленного оборудования мирового масштаба. Основное преимущество компании это дилерские цены, которые позволяют избегать торговой наценки. Компания работает с физическими лицами, частными предпринимателями среднего и малого рынка, а также с крупными промышленными компаниями.

По всем вопросам, которые могут возникнуть в процессе эксплуатации строительного и промышленного оборудования, сможет помочь и проконсультировать квалифицированный штат сотрудников организации. Качество обслуживания — это фактор, по которому покупатели часто обращаются в компанию и становятся постоянными клиентами.

В территорию, по которой возможна доставка оборудования входит не только Пермский край, но и территория всей России. Быстрая и своевременная доставка, качественное обслуживание, лучшее сертифицированное оборудование — вот то, за что покупатель выбирает оборудование ООО «Новая высота». Обязательное условие для эксплуатации строительного и промышленного оборудования является его сертификация. При обращении в эту компанию, можно всегда быть уверенным в результате.

На рис. 1.1 представлена линейная организационная структура предприятия.

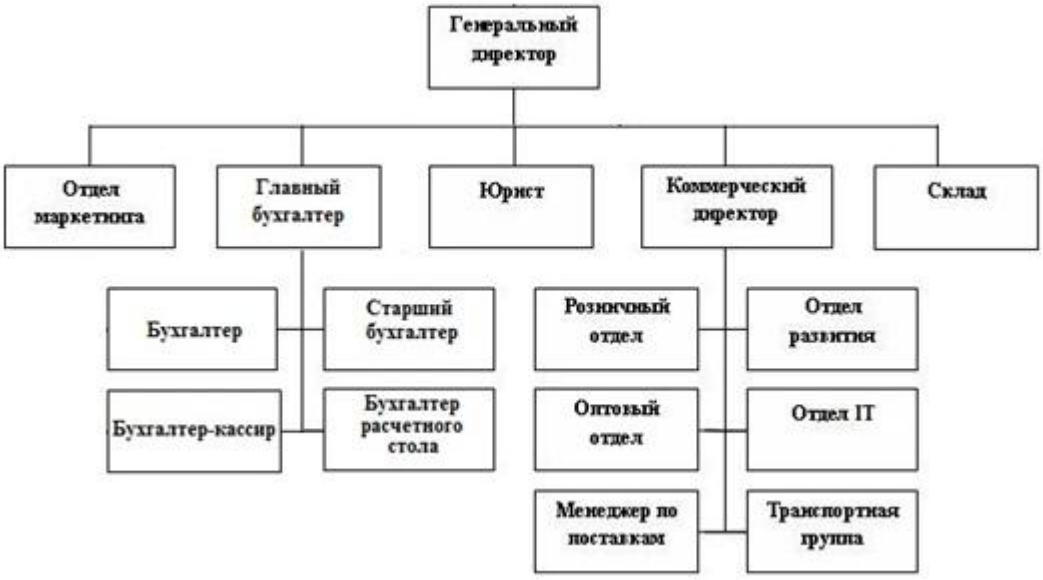

Рисунок 1.1 - Структура предприятия

Судя по данной схеме, в подчинении главного бухгалтера находятся четыре бухгалтера, у каждого бухгалтера своя область ответственности и ряд выполняемых задач.

Бухгалтерия — подразделение хозяйствующего субъекта, в котором собирается вся информация об имуществе и обязательствах организации. В бухгалтерии есть вся документально обоснованная информация, чтобы принять управленческое решение для обеспечения эффективного хозяйствования[1].

Все документы, которые связаны с предприятием обязательно проходят через бухгалтерию. Это сердце денежного оборота любого предприятия, в котором необходим высокий уровень защиты информации, потому что бухгалтерия работает с закрытой (конфиденциальной) информацией.

Основные задачи бухгалтерского отдела:

1) Организация работы в рамках общей государственной социальной политики и существующего законодательства.
2) Использование существующего законодательства в процессе ведения деятельности с финансами компании.

3) Вне зависимости от формы собственности, осуществление взаимодействия с муниципальными органами управления социальной защиты.
4) Улучшение организации ведения учета и контроля, благодаря разработанным предложениям.
5) Выявление и работа над проблемами в процессе ведения бухгалтерского учета. Проведение информационно-аналитической работ.
6) Контроль и выдача средств на целевое использование.

Основные функции бухгалтерского отдела:

1) Организовать бухгалтерский и налоговый учет деятельности организации.
2) Непосредственный контроль:

- за собственностью предприятия и её сохранности;
- за материальными ценностями и денежными средствами, а также соблюдение целевого расходования;
- за инвентаризацией, правильным и своевременным проведением;
- за расчетами по заработной плате, за её корректным ведением.

3) Применять утвержденные типовые унифицированные формы.
4) Для своевременного отображения в бухгалтерском учете, предоставлять в конкретные сроки, качественно сформированные первичные документы.
5) Обеспечить сохранность бухгалтерских документов.
6) Вести учет основных фондов.
7) Принять и провести расчет по хозяйственным договорам.
8) Контролировать денежные средства и их использование. Обеспечить жесткий контроль и соблюдение дисциплины, расчетной и кассовой.
9) Осуществлять заблаговременный контроль за своевременным и верным оформлением бумаг и законностью совершаемых действий.

10) Обеспечить оперативное и верное проведение хозяйственных операций и последующее их отображение в учете и отчетности.
11) Проводить котировки согласно всем методам размещения заказа, мониторинг покупок товаров, оказания услуг, оформление на официальном веб-сайте муниципальных договоров.
12) Оформлять бумаги и содействовать в заседаниях котировочных комиссий.
13) Организовать налоговый учет.
14) Предоставлять статистическую отчетность.
15) Участвовать и проводить внутренние ревизии.
16) Осуществлять мероприятия для увеличения уровня автоматизации учетно-вычислительных работ.
17) Проводить инструктаж:
    1. Для работников, которые несут материальную ответственность и подотчетным лицам организации:
    - по вопросам хранения, учета и сохранности ценностей, которые находятся на их ответственности;
    2. Для специалистов отдела:
    - по охране труда;
    - по технике безопасности.
18) Участвовать в подготовке и исполнении проектов нормативно-правовых документов.
19) Участвовать и проводить семинары и совещания.
20) Подготовка бумаг согласно недостачам, с целью работы по закрытию существующих недостач.
21) Организация работы согласно закрытию дебиторской и кредиторской задолженности.

Все средства протекают через данный отдел, поэтому малейшая ошибка в работе бухгалтерии может стоить дорого.

1.2 Концептуальное моделирование документооборота в бухгалтерском отделе

После исследования процесса документооборота бухгалтерского отдела предприятия «Новая высота» была построена концептуальная модель «КАК ЕСТЬ».

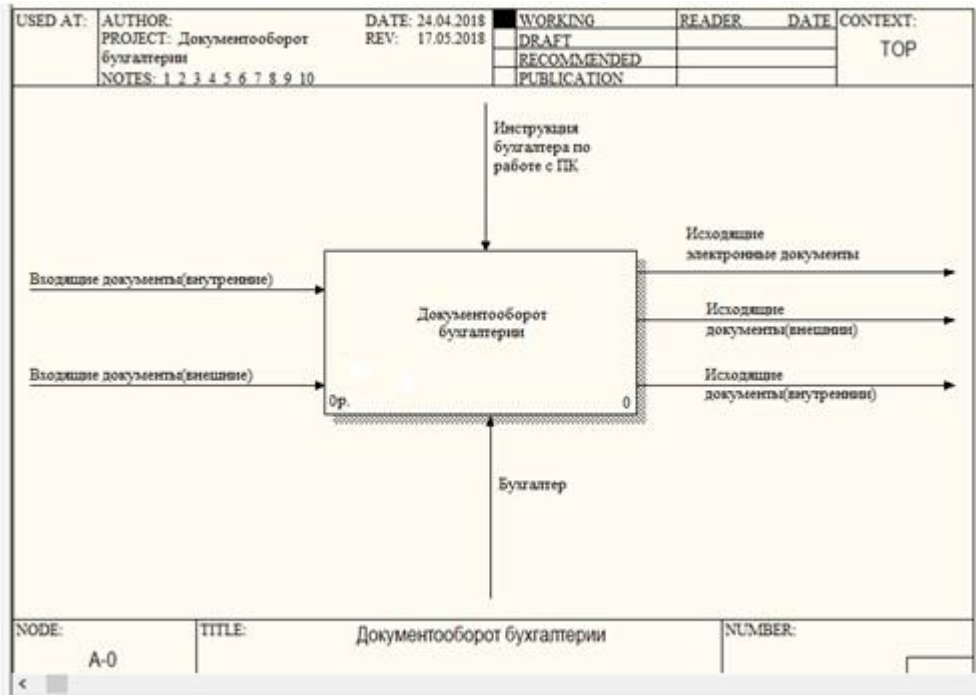

Рисунок 1.2 - Концептуальная модель

Входящие документы (внутренние) – документы по предприятию, не выходящие во внешнею сеть, такие как приказы, отчеты по внутреннему аудиту и т.д.

Входящие документы (внешние) – документы, пришедшие от государственных структур, поставщиков, клиентов. К ним могут относиться накладные, квитанции, стандарты отчетных форм для налоговой и т.д.

Бухгалтер – действующие лицо, человек ответственный за ввод данных в базу данных предприятия, необязательно, что бухгалтер всего один.

Исходящие электронные документы – это может быть копия печатной документации в электронном виде, или же электронный документ, который требует отправки по внешней сети Интернет.

Исходящие документы (внешние) – документы в электронном или печатном формате, но в сеть интернет не выкладываются, передаются на съемных носителях.

Исходящие документы (внутренние) – документ в печатном или электронном формате, который используется внутри предприятия, или электронная копия внешнего документа, для хранения.

Инструкция бухгалтера по работе с ПК – правила использования программного комплекса (ПК), описывает какие программы, для каких операций надо использовать и последовательность действий в программах.

Бухгалтер – данная стрелка подразумевает, что в тестировании будут принимать участие все бухгалтера предприятия.

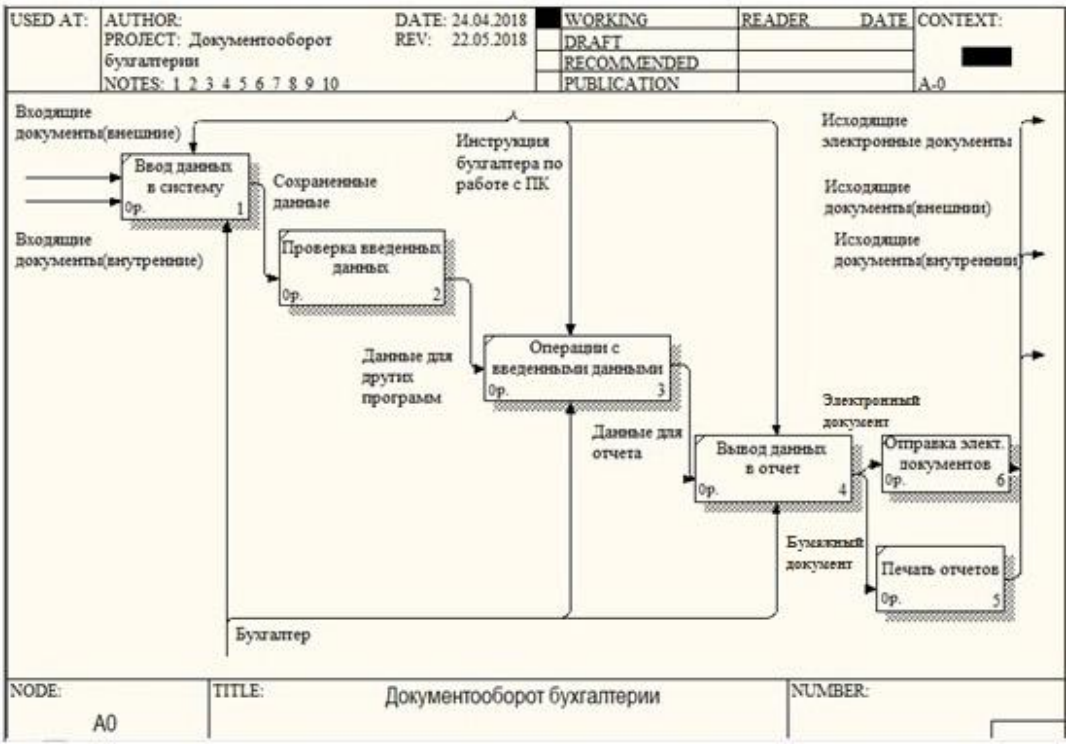

Рисунок 1.2 - Декомпозиция концептуальной модели

Ввод данных в систему – программы для ввода данных с входящих документов, в комплексе их несколько, для каждого справочника или таблицы своя программа (модуль) ввода данных.

Проверка введенных данных – включает в себя, как и проверку от пользователя, так и программную проверку вводимых данных, которые защищают целостность базы данных.

Операции с введенными данными – это использование программ для аналитики, расчетов и сохранения результатов данных расчетов в базе данных.

Вывод данных в отчет – использование программы для формирования различных отчетов, которые в дальнейшем будут распечатаны либо отправлены по сети Интернет.

Отправка электронных документов – отправка документов по сети Интернет.

Печать отчетов – печать бумажного экземпляра документов.

В ходе исследования бизнес-процесса, были найдены недостатки, такие как малая защищенность и не упорядоченность документов при выводе данных во внешние источники. В ходе обсуждения с руководителем IT отдела было принято решение по внедрению тестового ПО для усиления защиты исходящих данных бухгалтерского отдела.

На предприятии ранее не использовалось дополнительное ПО для шифрования данных. Попытка внедрения была предложена Начальником IT отдела, так как на предприятии ограниченное количество разработчиков, то для выделения времени на какую-либо разработку требуется обоснования.

Проведенный в работе анализ и внедряемый программный продукт послужит тестовым вариантом, для получения статистических данных. После трех месяцев работы в тестовом режиме, если программа покажет достаточно хороший результат и усилит программный комплекс, то уже данное направление будет вставлено в план IT отдела. На данном этапе конкретного ТЗ и ожидаемых результатов нет.

На рисунке 1.4 представлена схема «КАК БУДЕТ», с внесенным блоком шифрования.

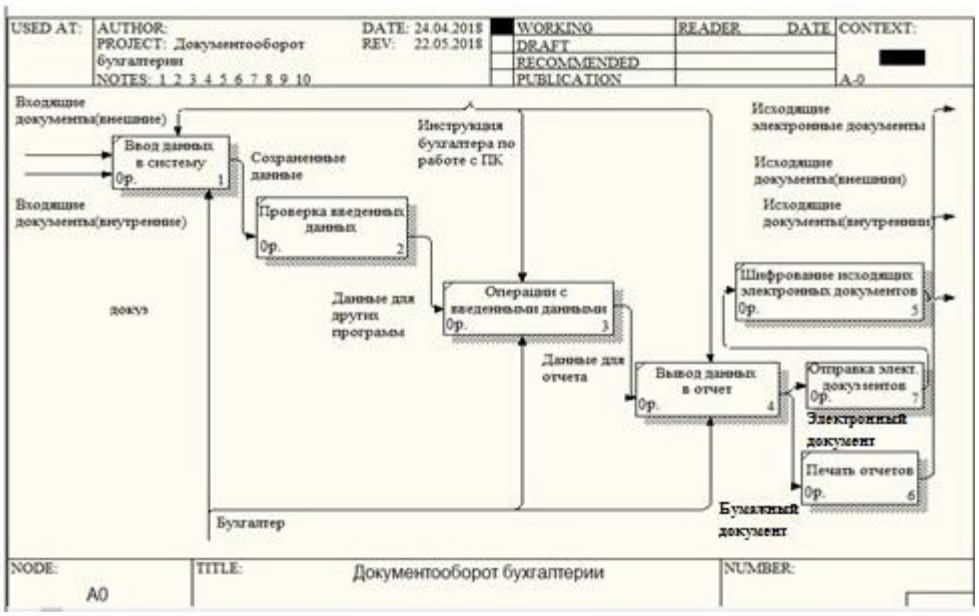

Рисунок 1.3 - Декомпозиция с блоком шифрования

Шифрование исходящих электронных документов – использование программы шифрование для дополнительной защиты от кражи конфиденциальных данных.

Достоинства разрабатываемого алгоритма – это дополнительная защита информации, к недостаткам можно отнести возможное замедление процесса передачи исходящих документов.

Часто отделу приходится пересылать документы по сети Интернет, это могут быть логины и пароли для временного доступа к части файлов, для аудита компании или проведения статистического внешнего анализа, копии накладных или налоговые декларации.

Такие документы требуют дополнительного уровня защиты, ибо их могут перехватить в интернете, взломать почтовый ящик и достать оттуда, поэтому пока я проходил практику предложил внести дополнительное шифрование файлов, пересылаемых по сети Интернет.

На данном этапе было принято решения адаптировать программу для проверки ее работоспособности и эффективности.

На рисунке 1.5 представлена наглядная схема разрабатываемого процесса шифрования.

Рисунок 1.4 – Концептуальная модель процесса шифрования

Входящий документ – документ, на котором будет проходить этап тестирование и проверка алгоритма шифрование, чтобы понять минусы программы и оценить ее эффективность.

Алгоритм шифрования – алгоритм, который используется в программе для шифрования данных.

Исходящий документ – зашифрованный документ, для отправки по сети Интернет.

Стандарт шифрование – внутренний документ разработан на предприятии, информацию из него не разглашается, так как является коммерческой тайной предприятия.

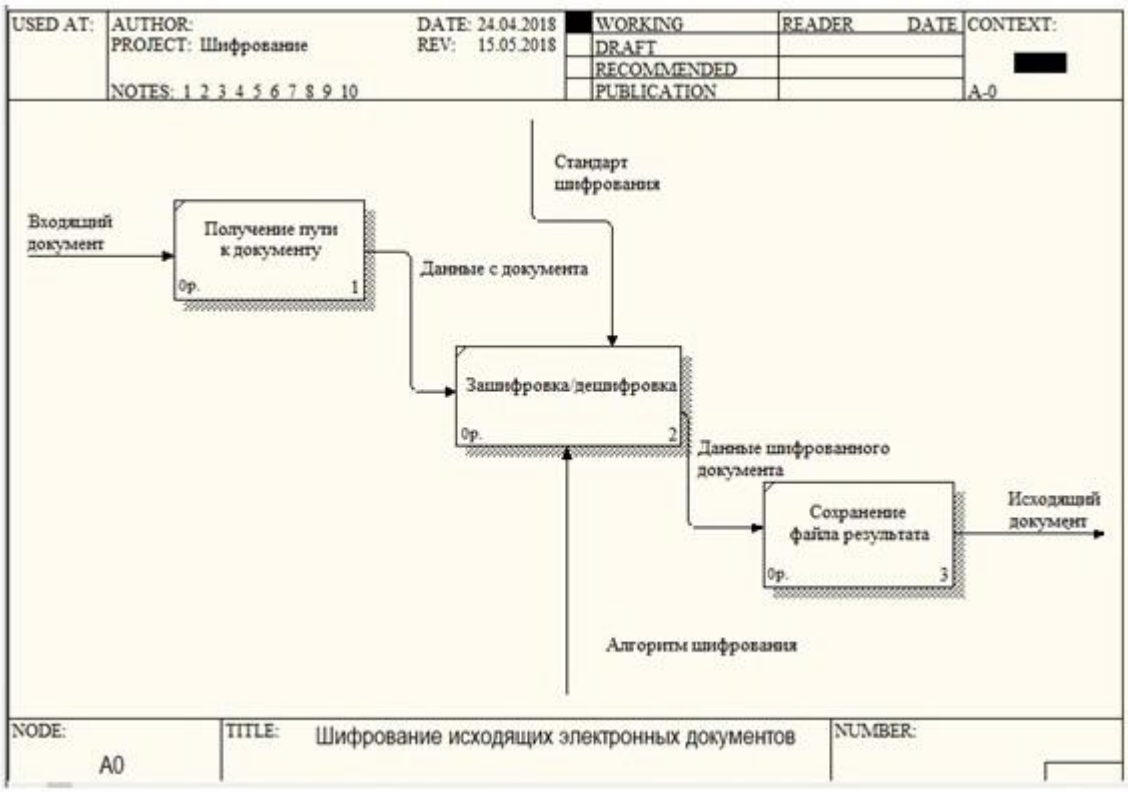

Рисунок 1.5 – Декомпозиция концептуальной модели процесса шифрования

Получение пути к документу – путь к документу для шифрования указываемый пользователем.

Зашифровка/дешифровка – работа алгоритма программы.

Сохранение файла результата – зашифрованный файл, с измененным именем сохраняется по тому же пути что и исходник.

Если программа успешно справится с этой задачей и будет эффективна в шифровании документации, то в дальнейшем она будет доработана и доведена до полной автономии, чтобы как можно больше исключить человеческий фактор из схемы работы программы, и тем самым повысить уровень защиты.

1.3 Анализ существующих разработок и обоснование выбора технологии шифрования документов в бухгалтерии

После принятия решения о внедрении программы шифрования, был промониторен рынок имеющегося готового ПО. Для того чтобы всё ПО

оказалось в одной категории, было принято решение сравнить только программы, у которых открыт исходный код. Для сравнительного анализа были выбраны следующие программы: Folder Lock, PGP Desktop, CyberSafe Top Secret.

Описание программы **Folder Lock**:

Folder Lock – программа для ПК, которая сможет защитить личные и конфиденциальные данные. С этой программой можно установить парольную защиты на файл или папку с важной информацией, а также есть функции для зашифровки и скрытия информации от нежелательных пользователей. Есть возможность защитить пользовательские данные от всевозможных вредителей и заблокировать доступ к внешним носителям.

Программа легка в использовании и имеет привлекательный интерфейс. После перемещения папки или файла в главное окно программы, выполняется скрытие данных. У программы есть online-хранилище, где хранится вся скрытая и защищенная информация. Так же с помощью программы можно удалить всю информацию с жесткого диска безвозвратно.

Folder Lock - это простой продукт, который имеет довольно неплохой функционал, чтобы заинтересовать пользователей. Данное ПО стабильно работает и при установке не запросит высоких требования к ресурсам ПК.

Основные возможности данной программы следующие:

- Скрытие и защита папок и файлов.
- Использует современный AES алгоритм с ключом 256 бит.
- Шифрование файлов «на лету».
- Резервное копирование в online-хранилище.
- Создание защищенных носителей информации.
- В e-mail почте шифруются вложения.

Рисунок 1.7 – Оболочка программы

Достоинства программы:

- Простой и понятный интерфейс для работы с программой неопытных пользователей, но со знанием английского языка.
- Прозрачное шифрование «на лету»
- Работа с обычными дисками не отличается от работы с зашифрованными виртуальными дисками.
- Возможность синхронизировать зашифрованные сейфы и online-копирование.
- Возможность создать самораспаковывающийся контейнер на USB-накопителе, а так же CD и DVD-дисках.

Недостатки программы:

- Работа с программой усложниться у пользователей, не владеющих английским языком. Программа не поддерживает русский язык.

- Сомнительная опция Lock Files (сокрытие, а не «запирание» файлов) и Make Wallets (не эффективна без экспорта информации).
- ЭЦП не поддерживается, нельзя проверить подпись, а тем более подписать файл.
- Невозможно выбрать соответствующую букву при открытии сейфа для виртуального диска, чтобы он именовался как сейф. В настройках программы возможно только выбирать порядок или от A до Z, или от Z до A.
- Функция зашифровки вложения почты, не интегрируется с почтовыми клиентами, только зашифрует вложения.
- Облачное копирование довольно дорогая опция.

Описание программы **PGP Desktop**:

PGP Desktop — это пакет программ, который работает на основе гибкого многоуровнего шифрования. Программа встраивается в системную оболочку, тем самым отличается от других программ. Контекстное меню позволяет воспользоваться функциями программы (рис. 1.8). По контекстному меню видно, что программа может выполнить шифрование файлов, подписать их и т.д. Функция для создания самораспаковывающегося архива работает так же, как и самораспаковывающийся архив, при использовании этой функции происходит не только распаковка архива, а также и расшифровка. Программы, участвующие в сравнении, так же имеют эту функцию.

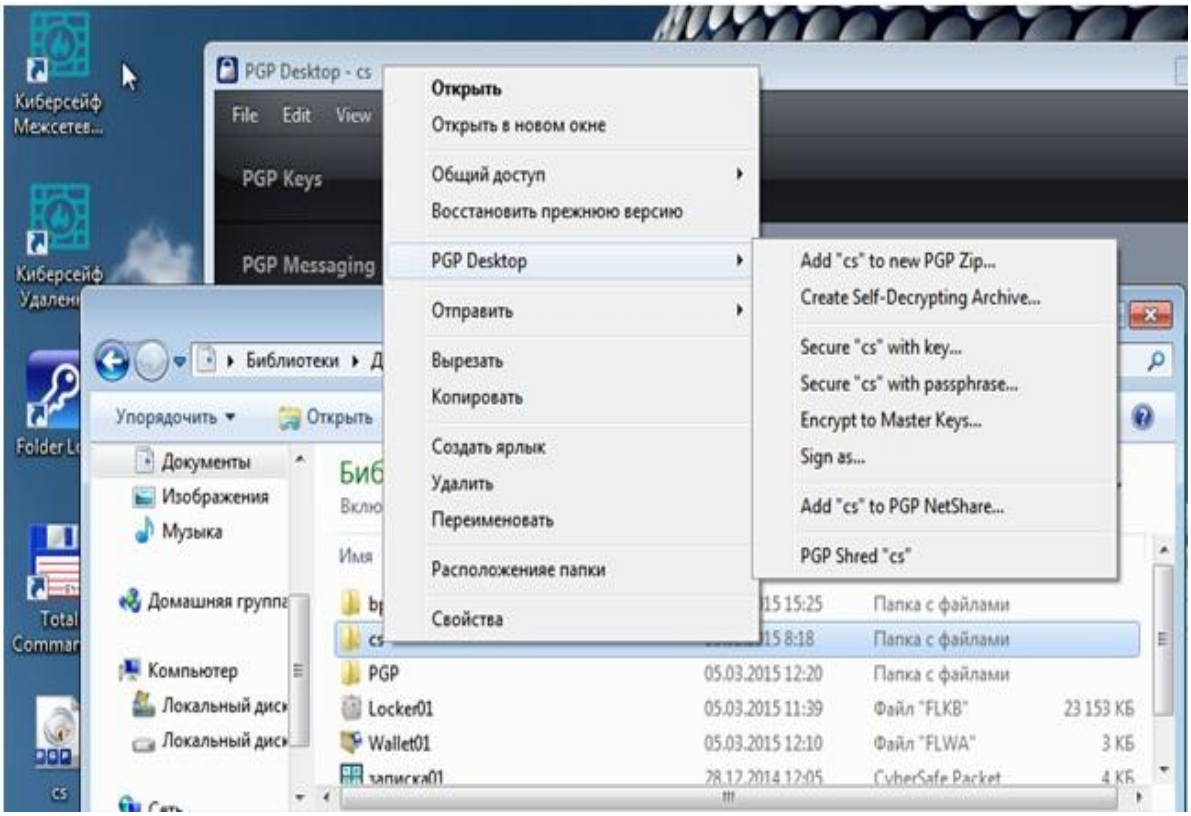

Рисунок 1.8 - Контекстное меню PGP Desktop

Достоинства программы:

- Поддерживает сервер ключей keyserver.pgp.com.
- Функция, которая позволяет создать самораспифровывающийся архив.
- Функция для шифрования системного жесткого диска.
- Функционал для использования ЭЦП.
- Особенность программы, а конкретно интеграция в оболочку.
- Возможность безвозвратного удаления данных.

Недостатки программы:

- Программы не поддерживает русский язык, из-за этого могут возникнуть сложности у пользователей, которые не владеют английским языком.
- Производительность программы ожидает желать лучшего.
- Нестабильная работа программы.
- Поддерживает AOL IM, но не поддерживает Skype и Viber.

- Незащищенными остаются письма на клиенте, после расшифровки.
- Только при включении режима перехвата идет защита электронной почты.

Обзор программы: **CyberSafe Top Secret**

CyberSafe Top Secret – программа для защиты данных, которая использует самые современные алгоритмы шифрования (RSA, AES, BlowFish и др.). Данное ПО имеет отличный функционал, который позволяет работать программе во всех сферах работы с информацией: защита конфиденциальной информации, защита электронной почты, создание и проверка ЭЦП.

Работа программы CyberSafe Top **S**ecret основывается на применение инфраструктуры открытых ключей (Public Key Infrastructure). Возможности программного продукта следующие: зашифровка разделов жесткого диска, создание зашифрованного виртуального диска любого размера, скрытие от посторонних лиц логических дисков и зашифрованных файлов и папок на ПК пользователя.

Функции программы CyberSafe позволяют управлять ключами и сертификатами. Так же у программы есть открытый сервер ключей, для того чтобы опубликовать открытый ключ компании и осуществить обмен ключами с другими компаниями, для последующей передачи зашифрованной информации (см. рисунок 1.9).

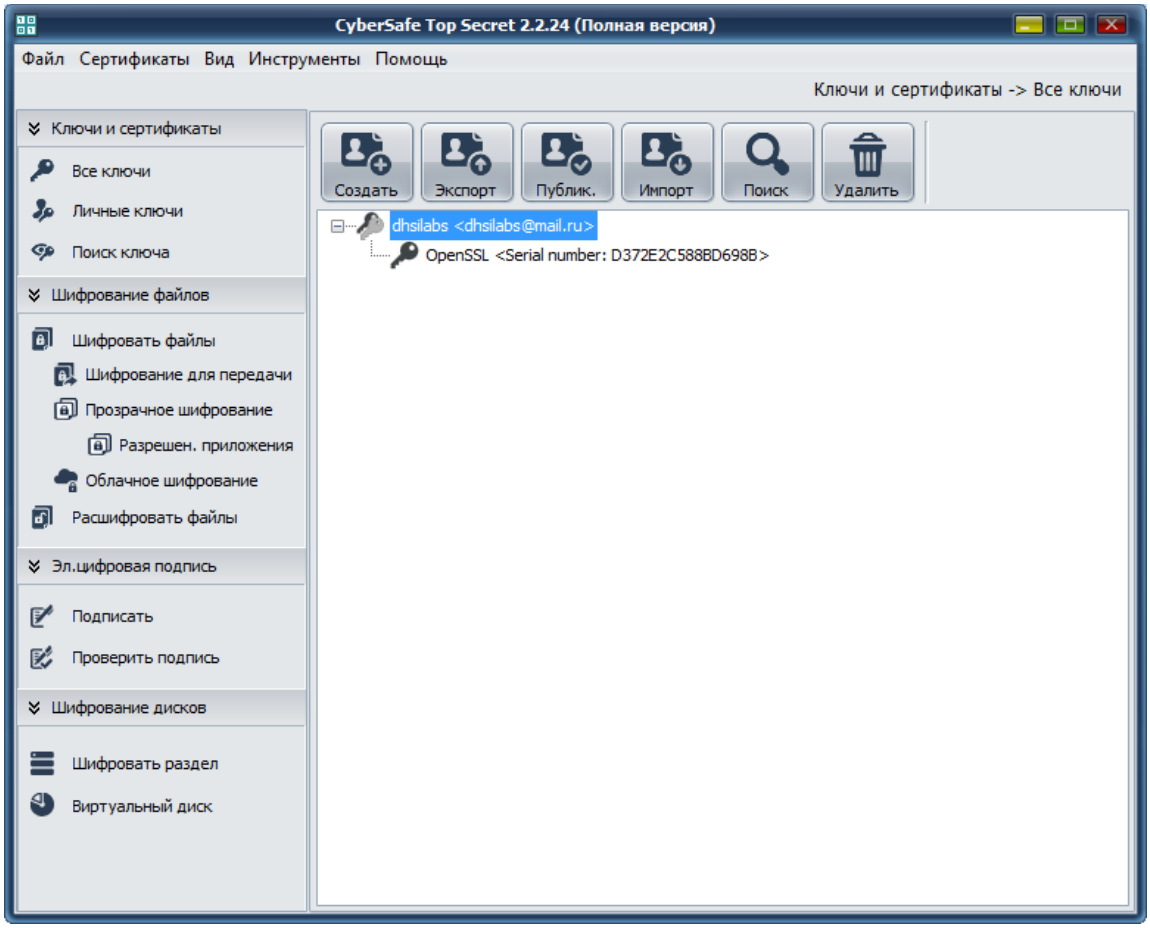

Рисунок 1.9 - Управление ключами

Программный продукт может применяться для зашифровки отдельных файлов. Программу CyberSafe Top Secret можно применять и в банках, и в государственных организациях, так как данный продукт имеет поддержку алгоритма ГОСТ и сертифицированного криптопровайдера КриптоПро.

Достоинства программы **CyberSafe Top Secret**:

- Использование программы возможно не только для частных лиц и коммерческих организаций, но и для государственных учреждений. Фактор, благодаря которому это возможно - это поддержка алгоритмов шифрования ГОСТ и сертифицированного криптопровайдера КриптоПро.
- Функция, которая поддерживает прозрачное шифрование папки.
- Программа поддерживает функцию проверки электронно-цифровой подписи и соответственно способна подписать файлы.

- Отличительная особенность от других программ – это собственный сервер открытых ключей для публикации и обмена ключами между компаниями.
- Функция, которая способна создать виртуальный диск и способна зашифровать весь раздел.
- Возможность программы, которая создает самораспаковывающийся архив.
- Программа предоставляет возможность бесплатного облачного резервного копирования. Эта функция способна работать с любым сервисом — как платным, так и бесплатным.
- Возможность двухфакторной аутентификации пользователя, позволяющая организовать надежную защиту.
- Возможность ограничить доступ к зашифрованным файлам для других приложений. Это позволяет организовать система доверенных приложений.
- Программа CyberSafe поддерживает набор руководств AES-NI, что благоприятно влияет на производительности программы.
- Драйвер программы CyberSafe дает возможность работать по сети, что позволяет осуществить корпоративное шифрование.
- В отличие от других программ, CyberSafe поддерживает русский язык, но при этом есть возможность переключения на английский язык, для англоязычных пользователей.

Недостатки программы:

Особых недостатков у программы нет, но иногда в программе «выскакивают» непредвиденные сообщения такого рода «Password is weak». Также у программы пока нет возможности шифровать системный диск, но в таком шифрование нуждаются далеко не все.

На основе анализа построена таблица функций рассмотренных продуктов (см. Приложение 2).

Учитывая все факторы, лучшим вариантом данного сравнения является программа CyberSafe Top Secret. Одним немаловажным фактором стало то, что у данного продукта есть необходимая лицензия и сертификат ФСБ и ФСТЭК, которые дают право на официальное использование программы в организации. Программный продукт полностью удовлетворяет потребности организации.

А также на использование данного ПО повлиял выбор крупных компаний, которые используют CyberSafe Top Secret: АО «Роснано», ПАО «Банк Уралсиб», ОАО «РЖД», ООО «Бест-Тур», ПАО «Иркутскэнерго».

Такое готовое решение, как программно-аппаратный комплекс “ЗАСТАВА”, “Аккорд” и их аналоги, не было взято для сравнения с программами из-за дорогой стоимости и требований к техническому обслуживанию.

Вывод по главе 1

Произведен анализ документооборота в бухгалтерском отделе предприятия «Новая высота». Были разработаны наглядные схемы процесса, исследована предметная область и теоретическая часть по вопросу шифрования. А также произведён сравнительный анализ программ шифрования.

После анализа можем сделать вывод, что можно приступать к тестированию и адаптации программы, по результатам тестирования определить эффективность внедрения программы в рабочий процесс.

Глава 2 Внедрение и реализация проектных решений

2.1 Логическое моделирование бизнес-процесса шифрования файлов

Первое, что было сделано, это построена диаграмма вариантов использования (Use-case). Эта диаграмма даст возможность понять и определить, как будут действовать участники процесса, как они будут взаимодействовать между собой, и как они будут влиять на весь процесс. Для построения модели процесса в рамках данного аспекта может применяться Use-case диаграмма, диаграмма последовательности действий, диаграмма совместной работы и диаграмма действий.

Логический аспект. Данный аспект дает понять, какими будут функциональные требования процессов. В процессе данного аспекта задается логическая взаимосвязь классов и элементов процесса. Диаграмму классов и состояний можно применять для построения моделей.

Составляющие элементы. Внимание данного аспекта будет акцентироваться на том, каким будет распределение элементов процесса и каким будет их состав. Диаграмма компонентов используется для построения моделей в этом аспекте.

Ввод в действие. Схему процесса в привязке к аппаратному обеспечению информационной системы можно показать с помощью данного аспекта. Только диаграмму топологии можно применить для построения модели в этом аспекте.

Применяя различные аспекты, пользователю предоставляется возможность создавать, анализировать, изменять и управлять моделями. Для этого используется единый объектно-ориентированный подход и единый язык моделирования[2].

Ниже представлена диаграмма вариантов использования, на которой показано взаимодействие бизнес актеров с программой и принцип взаимодействия.

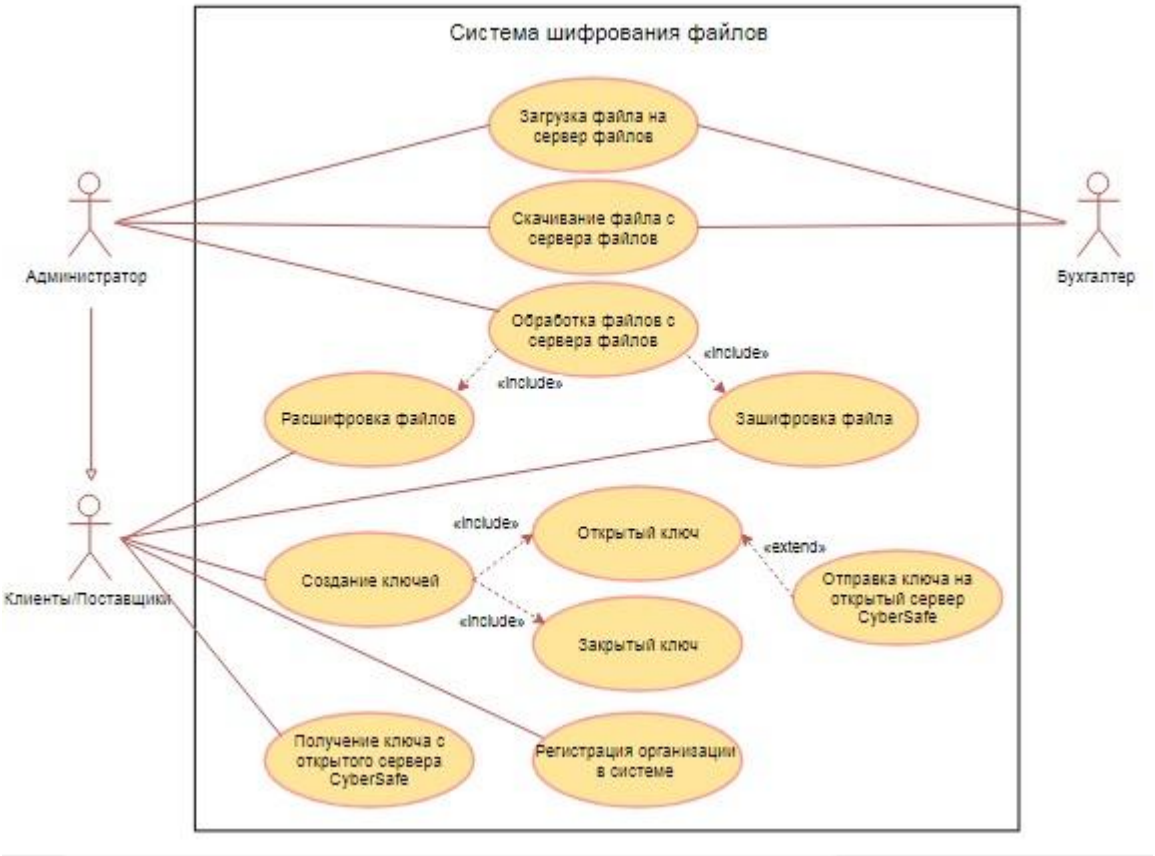

Рисунок 2.1 - Диаграмма вариантов использования

Бухгалтер предприятия – это актеры, это не обязательно будет один человек, но они неотъемлемая часть бизнес процесса, так как именно данные действующие лица будут давать данные для работы, в его задачи входит отправка зашифрованных файлов, принятие файлов от поставщика, помещения файлов на предварительное шифрование.

Администратор предприятия – это актер, человек из отдела IT, который проверяет наличие новых файлов, зашифровывает их, консультирует пользователей по возникшим вопросам и проверяет, чтобы все отправленные файлы с бухгалтерского отдела предварительно зашифрованы. Так же именно администратор будет следить за работой ПО и за статистикой.

Клиент/поставщик – это актер бизнес-процесса, который получает зашифрованные файлы, при их открытии он должен ввести ключ, для дешифровки файла.

Планируется, что программа шифрования данных будет стоять, как на самом предприятии, так и клиент/поставщик предприятия, которым отправляются конфиденциальные данные предприятия.

После диаграммы вариантов и общения с программистами отдела IT были построены диаграммы последовательности действия пользователя и программы. Диаграммы отображают идеальный вариант работы программы, и ее взаимодействия с пользователем.

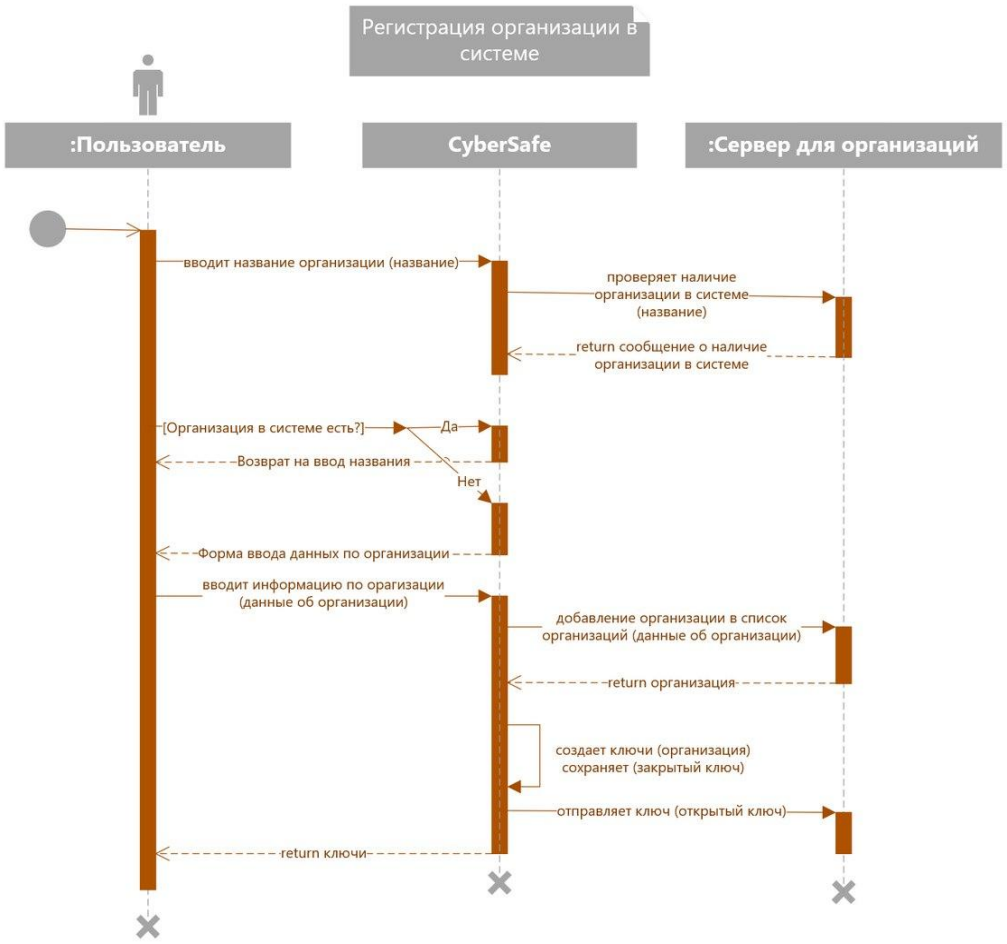

Рисунок 2.2 – Регистрация организации в системе

На рисунке 2.2 показано как проходит регистрация и получение связки ключей (открытого и закрытого ключа).

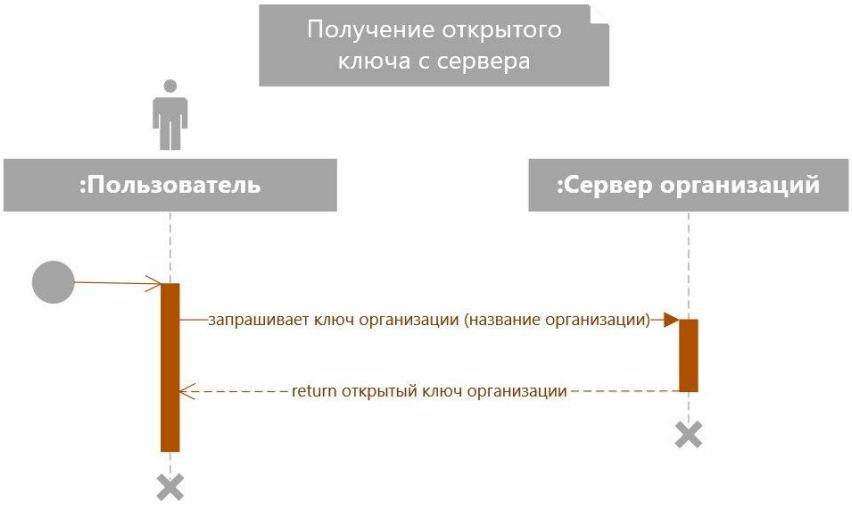

Рисунок 2.3 – Получение открытого ключа

На рисунке 2.3 показано получение открытого ключа.

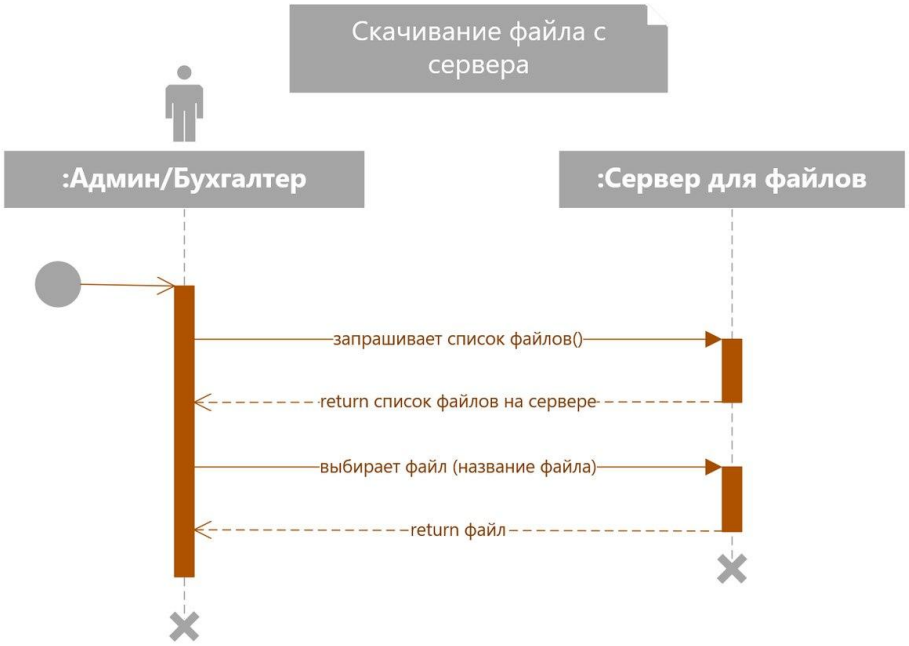

Рисунок 2.4 – Скачивание файла с сервера

На рисунке 2.4 показан процесс скачивания файла с сервера.

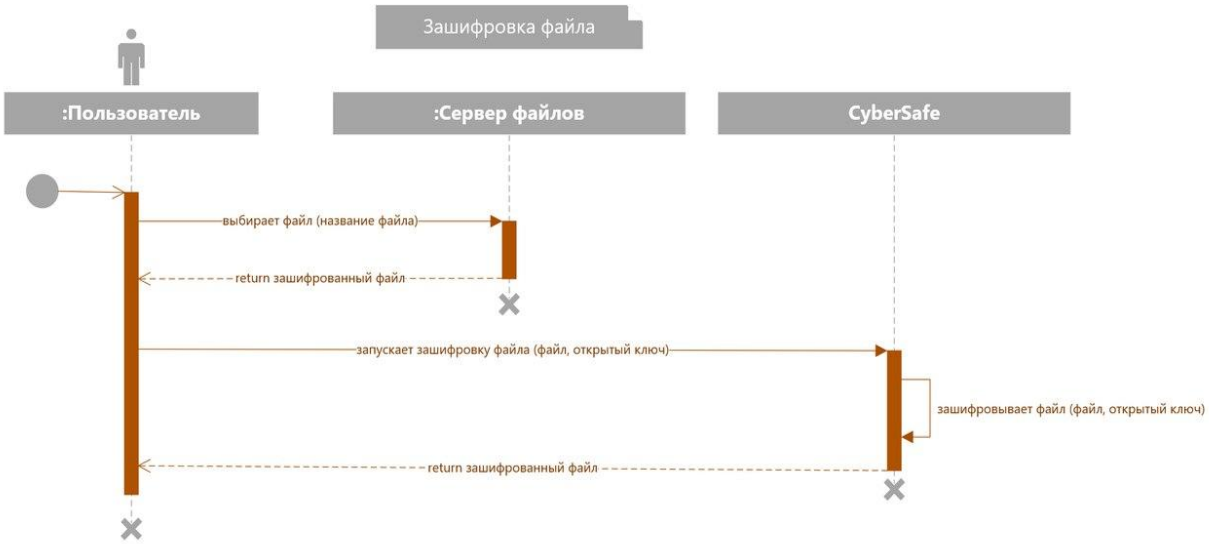

Рисунок 2.5 – Зашифровка файла

На рисунке 2.5 показан процесс зашифровки файла. Описание других прецедентов в приложении (см. Приложение 1).

Шифрование, то есть защита информации является закрытой информацией на любом предприятии, соответственно, чем меньше людей знают обо всех нюансах, тем лучше.

Планируется, что бухгалтера будут копировать файлы для отправки в папку на сервере. Администратор будет видеть добавление нового файла. Далее этот файл будет зашифрован и готов к отправке по сети Интернет по адресу назначения.

2.2 Физическое моделирование АИС процесса шифрования в документообороте предприятия

В данном пункте будет описана архитектура АИС, подробно описан алгоритм работы программы, лица, имеющие доступ к программе, тестирование программного продукта и дальнейшие варианты развития программного продукта

2.2.1 Выбор архитектуры АИС

Выбор архитектуры АИС исходил из уже имеющегося ПО в предприятии и архитектуры их модели. Так как предприятия использует архитектуру «Клиент-сервер», то и будущее ПО соответственно будет внедряться с учетом особенности данной архитектуры.

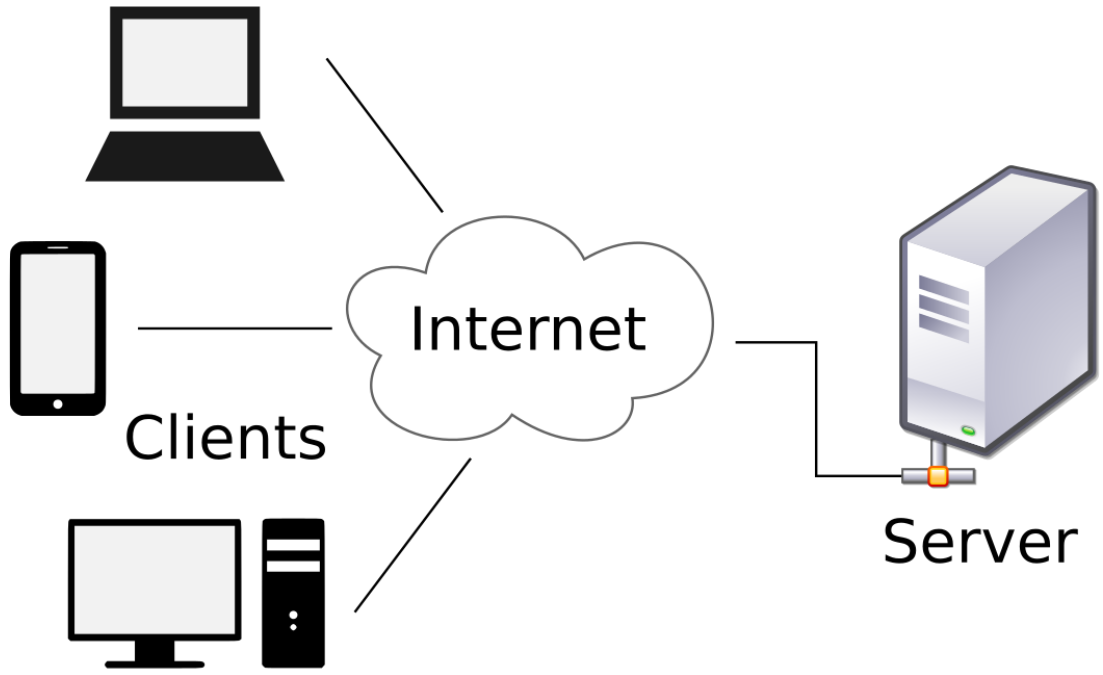

Рисунок 2.6 - Модель архитектуры клиент-сервер

«Клиент - сервер» — вычислительная или сетевая архитектура, в которой задачи или сетевая нагрузка распределяется между поставщиками услуг, именуемыми серверами, и заказчиками услуг, именуемыми клиентами. Как правило, клиент и сервер — это программное обеспечение. Обычно данные программы находятся на разных вычислительных машинах, связь между клиентом и сервером совершается через вычислительную сеть с помощью сетевых протоколов, но они также могут быть установлены и на одну вычислительную машину.

Взаимодействие между клиентом и сервером происходит следующим образом: программы-серверы ожидают запрос, а программы-клиенты отправляют запросы, вызывающие ресурсы сервера в виде данных (например, загрузка файлов с помощью протокола HTTP или FTP, потоковое мультимедиа или работа с базами данных) или в виде сервисных функций (например, работа с электронной почтой, общение с помощью систем мгновенного обмена сообщениями или просмотр веб-страниц во всемирной интернет паутине). Так как одна программа-сервер может осуществлять запросы от большого количества программ-клиентов, для неё специально выделяется вычислительная машина и настраивается особым образом, как правило, вместе с другими программами-серверами, по этой причине производительность этой машины обязана быть высокой.

Преимущества архитектуры:

- Не дублируется код программы-серверы программой-клиентом.
- Низкие требования для компьютера клиента обусловлены тем, что все вычисления происходят на сервере.
- Защита у сервера намного лучше, чем у клиента, поэтому все данные хранятся на нём. Разрешение на доступ может получить только пользователь с соответствующими правами, при организации контроля полномочий на сервере.

Недостатки архитектуры:

- Вся вычислительная сеть может стать неработоспособной, из-за неработоспособности сервера. Таким может считаться сервер, отправленный на профилактику или ремонт, а также сервер, у которого не хватит производительности, чтобы обслужить всех клиентов и т.д.
- Требуется системный администратор для обслуживания и поддержки работоспособности такой системы.
- Дорогостоящее оборудование.

2.2.2 Алгоритм работы программного продукта

Шифрование данных - это методы защиты любой информации от несанкционированного доступа, просмотра, а также её использования, основанные на преобразовании данных в зашифрованный формат.

Расшифровать, восстановить данную информацию или сообщение, обычно можно только при помощи ключа, который применялся при его шифровании. В программе CyberSafe Top Secret будет использоваться алгоритм шифрования AES.

Advanced Encryption Standard (AES) - один из наиболее популярных и часто применяемых, а также максимально безопасных алгоритмов кодирования, доступных на сегодняшний день. Этот алгоритм шифрования используют для обеспечения безопасности конфиденциальных данных с классификацией «Совершенно секретно». Алгоритм шифрования под названием «Rijndael», был разработан бельгийскими криптографами Daemen и Rijmen. Шифр отличается высокой защищенностью, а кроме того производительностью и гибкостью.

Алгоритм вышел на первое место из числа своих конкурентов и был официально представлен в 2001 году новым стандартом шифрования AES. Термин «blockcipher» описывает работу алгоритма AES, которая основана на нескольких подстановках, перестановках и линейных преобразованиях, которые выполняются на блоках, данных по 16 байтов. Такие операции называют «раундами», потому что они повторяются несколько раз. В процессе каждого раунда уникальный ключ раунда будет рассчитан из ключа шифрования и включен в вычисления.

Очевидное достоинство блочной структуры AES перед традиционными потоковыми шифрами в том, что, изменив отдельный бит в ключе или в блоке открытого текста, это приведет к радикально другому блоку зашифрованного текста. Наконец, разница между AES-128, AES-192 и AES-256 - это длина ключа: 128, 192 или 256 бит - это радикальные улучшения по сравнению с 56-битным ключом DES. В качестве примера, используя современный

суперкомпьютер для осуществления взлома 128-разрядного ключа AES, потребуется, намного, больше времени, чем предполагаемый возраст вселенной.

Внедрение программы шифрования проходило в несколько этапов.

Этап 1. Обследование ПО.

Перед установкой программы на сервер она была проверена начальником отдела IT на предмет сопоставимости с комплексом.

Этап 2. Настройка программного продукта.

Обнаруженных ошибок и недочетов кода, чтобы ПО не давало сбоев, начальник отдела IT пересобрал проект с внедрением в исходный код разработанных предприятием библиотек.

Этап 3. Установка ПО на сервер.

Программа была уже адаптирована под используемую на сервере версию Windows Server 2003. Установка прошло успешно.

Этап 4. ТестированиеПО.

Зашифровка тестовых документов, проверка работы программы и исправление обнаруженных ошибок.

Этап 5. Опытная эксплуатация системы.

Опытная эксплуатация системы подразумевает, что будет проходить работа с реальными данными. В среднем этап опытной эксплуатации занимает отчетный период равный одному месяцу.

После окончания всех вышеописанных этапов работ, будет можно говорить о том, что внедрение программного продукта завершено и идет его эксплуатация.

После установки ПО на сервер, начался этап функционального тестирования. Первым этапом было создание папки предварительного шифрования и разрешение доступа к ней определенным пользователям.

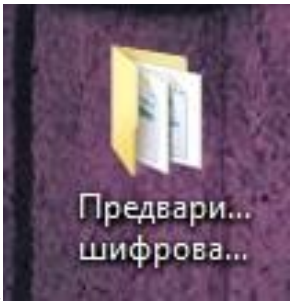

Рисунок 2.7 - Папка предварительного шифрования

Вторым шагом было получение данных от бухгалтерского отдела. Для тестирования программы шифрования. Была предоставлена Расчетная ведомость, в формате .docx, и Персональные данные о сотрудниках, в .accdb формате.

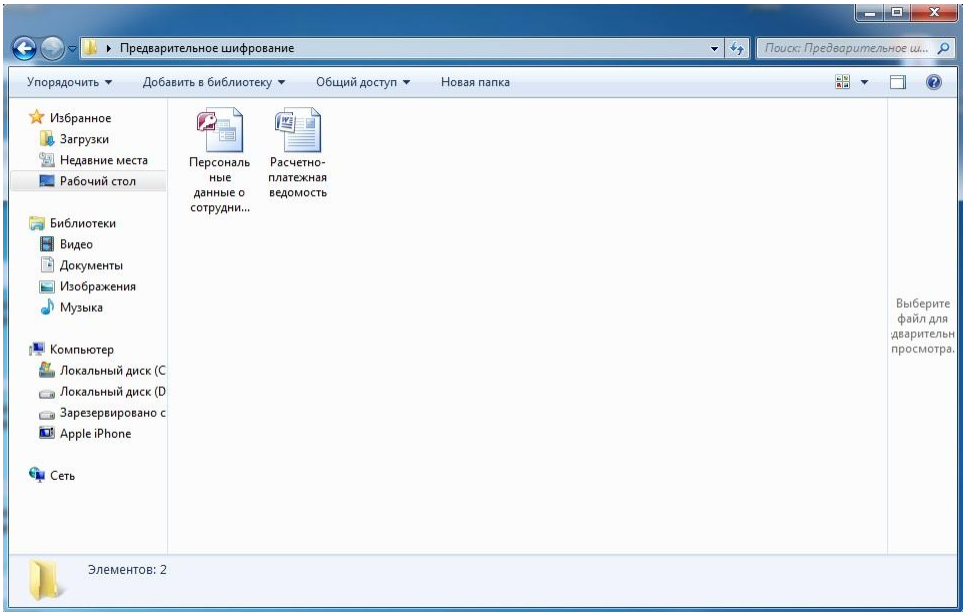

Рисунок 2.8 - Тестовые файлы

После запуска программы были созданы ключи для организации ООО «Новая высота» и найден открытый ключ клиента на сервере CyberSafe.

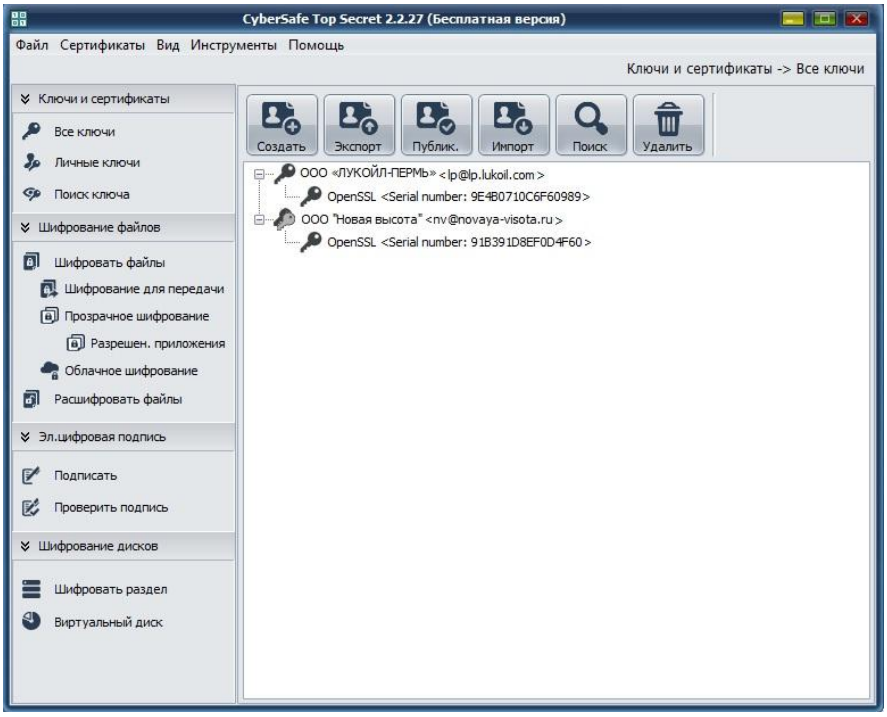

Рисунок 2.9 – Ключи шифрования

Далее, выбираем документ, который будем зашифровывать.

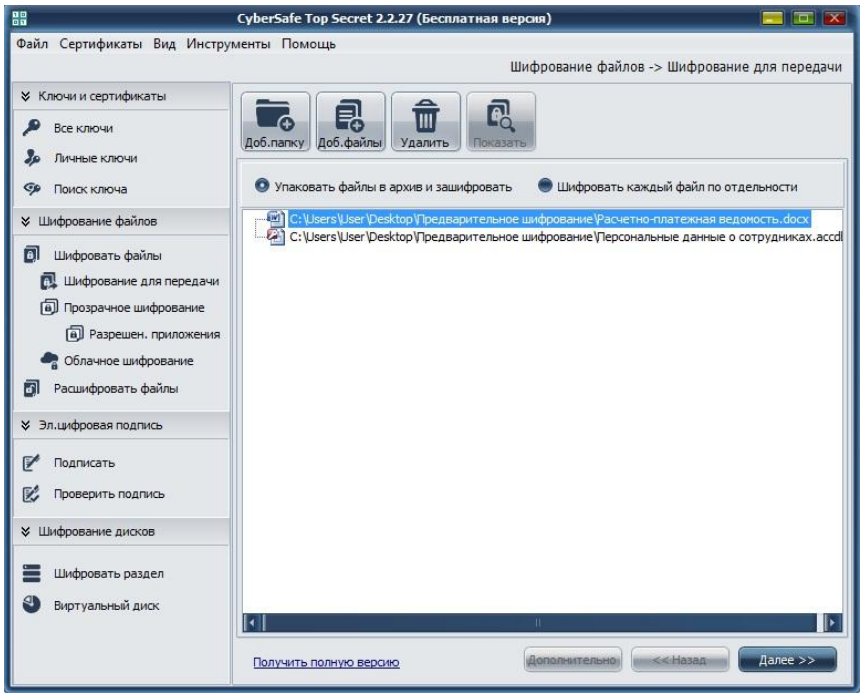

Рисунок 2.10 – Выбор документа

Далее, зашифровываем файл открытым ключом получателя, а конкретно ООО «ЛУКОЙЛ-ПЕРМЬ».

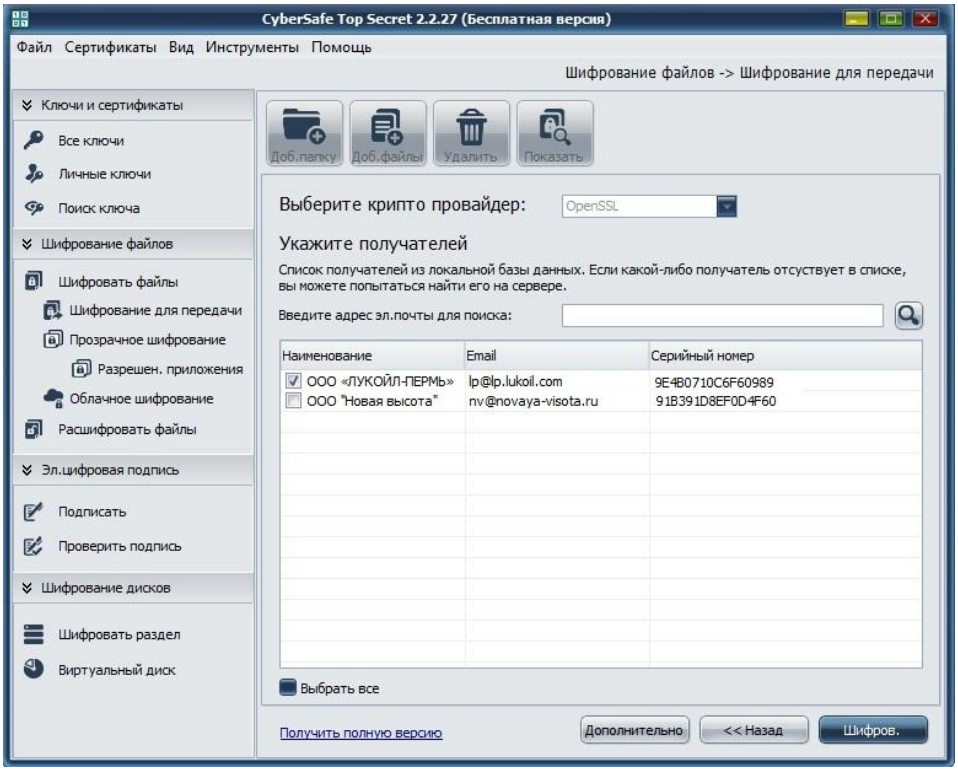

Рисунок 2.11 – Выбор адресата

Получен, зашифрованный файл для отправки по сети Интернет.

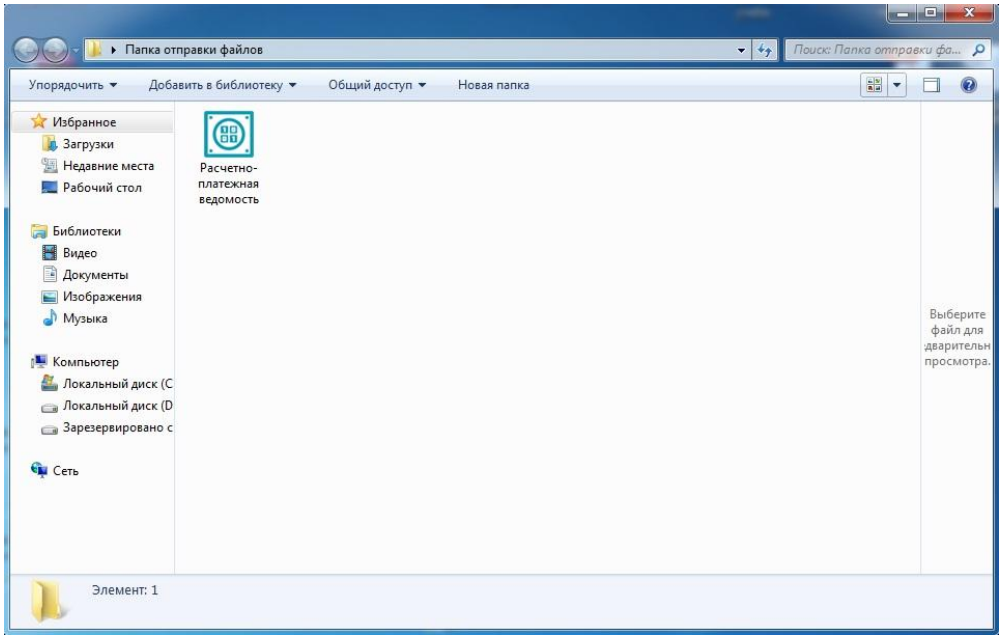

Рисунок 2.12 – Зашифрованный файл

На этапе тестирования данную процедуру будет проводить администратор, над файлами, которые отдел бухгалтерии будет помещать в размещенную на сервере папку.

Вывод по главе 2

После выбора среды внедрения, составление архитектуры и моделирования процесса было проведено тестирование внедряемого ПО. В главе описано пошаговые действия во время тестирования.

После нескольких недель или месяца тестирования, будет понятно стоит ли дальше внедрять данное ПО. Внедрение ПО для дополнительной защиты позволяет создать дополнительный уровень защиты данных, чтобы не потерять данные о личных доходах компании, потерять информацию о ком-то из сотрудников и т.д.

Защита данных – это всегда актуальная задача для любого предприятия.

Глава 3 Оценка и обоснование экономической эффективности проекта

3.1 Выбор и обоснование методики расчета экономической эффективности

Эмпирический метод расчета экономической эффективности проекта заключается в том, что в его основании лежит длительная обработка и сбор информации о всевозможных вариантах возникновения угроз для защиты информации и размер потерь, которые может понести организация от появления такой угрозы. Возможность эмпирическим методом определить некую зависимость между ущербом и коэффициентом, который показывает, как часто могут проявляться угрозы для информации и стоимость потерь при таких угрозах.

Экспертами американской компании IBM, был разработан лучший пример модели для данной разновидности моделей.

Очевидное предположение стало посылкой для разработки модели: с одной стороны, чтобы обеспечить достаточный уровень защиты конфиденциальной информации требуются вложения, с другой, при нарушении защиты информации, компанию могут ожидать непредвиденные потери денежных средств. Чтобы предположить стоимость защиты информации, нужно узнать сумму, которая будет потрачена на организацию защиты и сумму, которую может потерять организация от утечки информации и конфиденциальных данных. Очевидное решение, которое позволит минимизировать общую стоимость защиты данных, это выделить на защиту информации денежных средств, в размере $С_{опт}$.

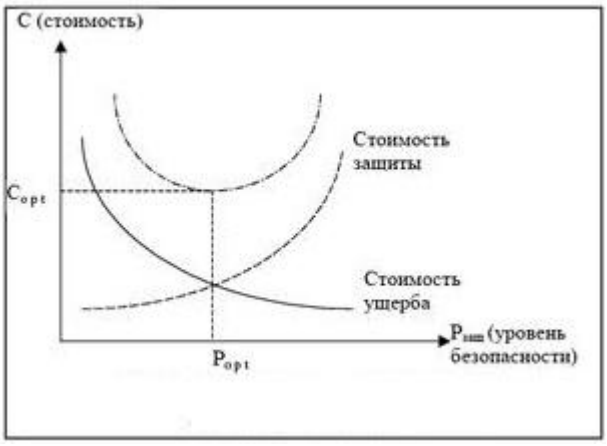

Рисунок 3.1 – Стоимостные зависимости защиты информации

Для того чтобы использовать данный подход к решению проблемы, важно знать, для начала какими будут потери при нарушении защищенности конфиденциальных данных, а также зависимость между уровнем защищенности и средствами, затрачиваемыми на защиту данных.

Решить вопрос и получить ответ о потерях, которые могут ожидать организацию при нарушении защиты и утечки конфиденциальной информации, возможно, получить только тогда, когда речь будет идти о защите промышленной, коммерческой и им подобной тайны, хотя и здесь возможно столкнуться с довольно серьезными трудностями. Что касается оценки уровня издержек при нарушении статуса безопасности данных, содержащей государственную, военную и им подобную тайну, то здесь до настоящего времени строгие подходы к их получению не найдены. Данное обстоятельство значительно сужает вероятную область применения моделей, основанных на рассматриваемых подходах.

Чтобы определить уровень затрат, который необходим, чтобы обеспечить требуемый уровень защиты информации, следует знать по крайне мере, во-первых, полноценный список угроз, которые могут возникнуть, во-вторых, возможную угрозу для информации от каждой из угроз и, в-третьих, необходимый уровень затрат, который потребуется для нейтрализации угрозы.

Так как приемлемое решение вопроса о подходящем уровне расходов на защиту данных заключается в том, что этот уровень должен быть равный уровню предполагаемых издержек при нарушении защиты, достаточно определить только уровень издержек. Экспертами компании IBM предложена следующая эмпирическая зависимость прогнозируемых издержек от угрозы информации: $R_i = 10^{(S_i + V_i - 4)}$

Где Si — показатель, демонстрирует вероятную частоту появления соответствующей опасности; Vi — показатель, демонстрирует значение предполагаемого убытка при её появлении. Предложенные экспертами значения коэффициентов:

Таблица 3.1Значения коэффициента Si

Ожидаемая (возможная) частота появления угрозы	Предполагаемое значение Si
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
12 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7

Таблица 3.2Возможные значения коэффициента Vi

Значение возможного убытка при проявлении угрозы, руб.	Предполагаемое значение Vi
3000	0
30000	1
300000	2
3000000	3
30000000	4
300000000	5

3.2 Расчет показателей экономической эффективности проекта

Проводить оценку эффективности проекта рекомендуется в три этапа:

- Производится определение масштабности проекта, его общественной и финансовой значимости и важности для определенной территории.
- Ведется подсчет показателей эффективности проекта и производится заключение о необходимости инвестиции в него денег.
- Ведется исследование чувствительности проекта к вероятным отрицательным условиям.

Данные в таблице были предоставлены проектировщиком отдела IT на основе внутренней статистики предприятия, по внедрению нового ПО и средним затратам на него.

Таблица 3.3Показатели эффективности от внедрения проекта автоматизации.

	Затраты		Абсолютное изменение затрат	Коэффициент изменения затрат	Индекс изменения затрат
	Базовый вариант	Проектный вариант			
Трудоемкость	T0(час)	T1(час)	T = T0 – T1	KT = T / T0 *100 %	YT = T0 / T1
	10	10,5	-0,5	-0,05	0,95
Стоимость	C0(руб)	C1(руб)	C = C0 – C1	KC = C / C0 * 100 %	YC = C0 / C1
	10 000	9 500	500	0,05	1,05

Данное ПО не как не повышает, или понижает прибыль предприятия, оно направленно на защиту документов предприятия. Не все внедряемое ПО повышает прибыль, у каждого ПО своя область задач.

Разработка ПО – это трудоемкий и дорогой процесс, в среднем на написание программы такой сложности, как шифрование, может уйти месяц, а то и больше.

Это не учитывая этапы внедрения и тестирования. Соответственно для разработки абсолютно нового ПО требует веских основания и много времени, если в цифрах, это 100-150 часов рабочего времени для одного программиста с опытом работы не менее 3 лет.

При этом для внедрения уже разработанной программы, имея исходный код на руках, уйдет в 2 или в 3 раза меньше времени, то есть 50-75 часов рабочего времени. Соответственно остальное время специалист уже затратит на другую задачу, что является как выгодно экономически, так и по показателям продуктивности, так как за месяц будет выполнено больше задач.

Вывод по главе 3

Внедрение программы шифрования данных бухгалтерского отдела в организации предотвратит возможную кражу конфиденциальной информации и позволит быть уверенным в том, что отправляемые данные попадут только в руки адресату.

Так как внедряемый продукт является бесплатным, то данное решение будет экономически выгодным для организации. Данный продукт продлит время, затраченное на бизнес-процесс, но уменьшит стоимость самого бизнес-процесса, так как предприятию не придется тратить свои средства на сторонние источники защиты.

ЗАКЛЮЧЕНИЕ

В ходе написания бакалаврской работы были решены следующие задачи:

- проанализирован документооборот бухгалтерского отдела;
- проведен сравнительный анализ программ шифрования;
- подобрано наиболее подходящее ПО для внедрения;
- выявлены недостатки и произведено тестирование выбранного варианта программы шифрования;
- внедрено ПО для шифрования исходящих документов бухгалтерского отдела.

В процессе выполнения работы были разработаны наглядные схемы процесса, исследована предметная область, теоретическая и практическая часть по вопросу шифрования, произведён сравнительный анализ программ шифрования и внедрен программный продукт.

Итогом проделанной работы стало внедрение программы CyberSafe Top Secret, отражающая суть поставленной цели – повышения уровня защиты данных бухгалтерского отдела для передачи по сети Интернет в организации ООО «Новая высота».

После внедрения программы была улучшена защита конфиденциальной информации организации. Данная программа полностью удовлетворяет потребности организации и является наиболее подходящим, выгодным и лицензированным вариантом программы шифрования данных.

CyberSafe Top Secret является законченным программным продуктом, хотя возможна ее доработка, используя исходный код. Программа обладает удобным и понятным интерфейсом, который будет понятен даже для неопытного пользователя. Цель была выполнена в полной мере, и программа была реализована на практике.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Александр Галкин. Информационная безопасность и целесообразные пути ее улучшения. – М.: Palmarium Academic Publishing, 2014. – 80 с.
2. Астахов, В.П. Бухгалтерский (финансовый) учет / В.П. Астахов. – М.: Юрайт, 2015. – 992 с.
3. А.А. Хлебников. Информатика. Учебник. – Ростов-на-Дону: Феникс, 2014. – 448 с.
4. А.В. Бабаш, Е.К. Баранова. Криптографические методы защиты информации. Учебник. – М.: КноРус, 2016. – 190 с.
5. А.И. Громов, А. Фляйшман, В.Шмидт. Управление бизнес-процессами. Современные методы. – М.: Юрайт, 2016. – 368 с.
6. Б.Е. Стариченко. Теоретические основы информатики. Учебник. – М.: Горячая Линия - Телеком, 2014. – 400 с.
7. Виктор Де Касто. Просто криптография. – М.: Страта, 2014. – 208 с.
8. Владимир Сизов. Абсолютно надёжный поточный криптографический алгоритм шифрования. – М.: LAP Lambert Academic Publishing, 2014. – 88 с.
9. В.Я. Ищейнов, М.В. Мецатунян. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. Учебное пособие. – М.: ДРОФА, 2014. – 256 с.
10. В.Я. Ищейнов, М.В. Мецатунян. Основные положения информационной безопасности. Учебное пособие. – М.: Форум, Инфра-М, 2015. – 208 с.
11. Георгий Бритовund Осипова Татьяна. Моделирование бизнес-процессов. – М.: LAP Lambert Academic Publishing, 2014. – 124 с.
12. Е.В. Сивков. Современный бухгалтерский учет. Основной курс от аудитора Евгения Сивкова. – М.: Евгений Сивков, 2014. – 320 с.

13. И.Н. Васильева. Криптографические методы защиты информации. Учебник и практикум. – М.: Юрайт, 2016. – 350 с.

14. Л.К. Бабенко, Е.А. Ищукова. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2016. – 376 с.

15. М.В. Гаврилов, В.А. Климов. Информатика и информационные технологии. Учебник. – М.: Юрайт, 2014. – 384 с.

16. О.Н. Жданов. Методика выбора ключевой информации для алгоритма блочного шифрования. – М.: Инфра-М, 2015. – 88 с.

17. О.Ю. Полянская, В.С. Горбатов. Инфраструктуры открытых ключей. – М.: Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2014. – 368 с.

18. Сергей Мазаник. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей. – М.: Эксмо, 2014. – 256 с.

19. С.К. Варлатая, М.В. Шаханова. Криптографические методы и средства обеспечения информационной безопасности. Учебное пособие. – М.: Проспект, 2015. – 152 с.

20. С.Ю. Кабашов. Электронное правительство. Электронный документооборот. Термины и определения. Учебное пособие. – М.: Инфра-М, 2015. – 320 с.

21. Amit Kalani, Priti Kalani. MCAD/MCSD Developing XML Web Services and Server Components with Visual C# .NET and the .NET Framework (+ CD-ROM). – M.:Que Certification, 2015. – 1040 с.

22. Clint Huffman. Windows Performance Analysis Field Guide. – M.:Syngress, 2015. – 380 с.

23. C. Shoba Bindu, Dileep Kumar Reddy Pallela and Koneti Sekar. Programming In C and Data Structures. – M.: , 2014. – 344 с.

24. Dusan Davidovic and Ioannis Kanalis. Information Protection in Critical infrastructure protection. – M.: LAP Lambert Academic Publishing, 2014. – 84 с.

25. Nikhil Rahagude and Dr. Michael Hsiao. DFT+DFD: An Integrated Method for Design for Testability and Diagnosis. – M.: LAP Lambert Academic Publishing, 2016. – 96 с.

Приложение

Приложение 1

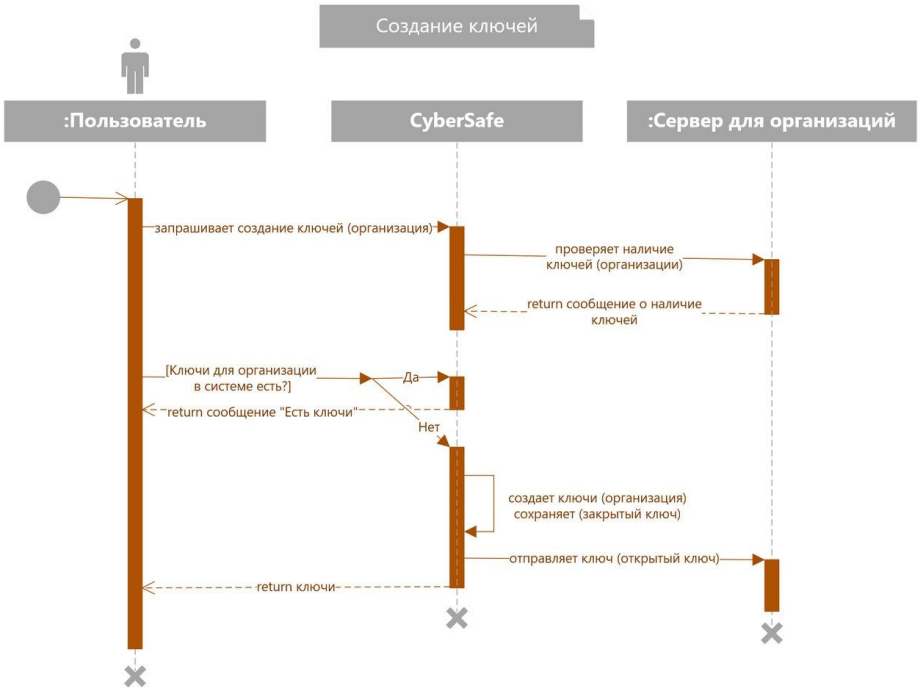

Рисунок 1.10 - Диаграмма последовательности действий (создание связки ключей).

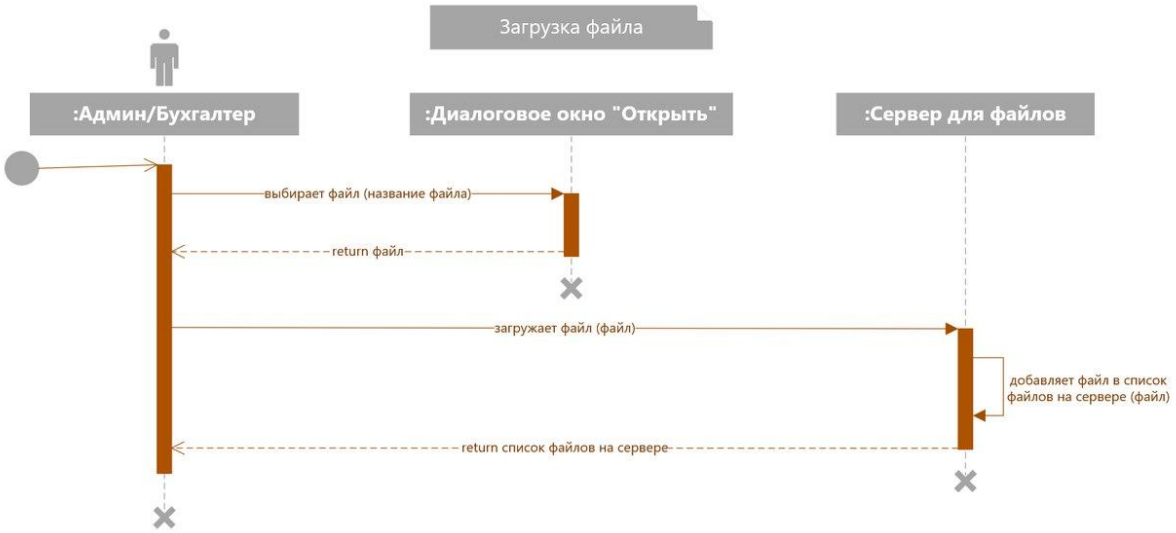

Рисунок 1.11 - Диаграмма последовательности действий (загрузка файла на сервер).

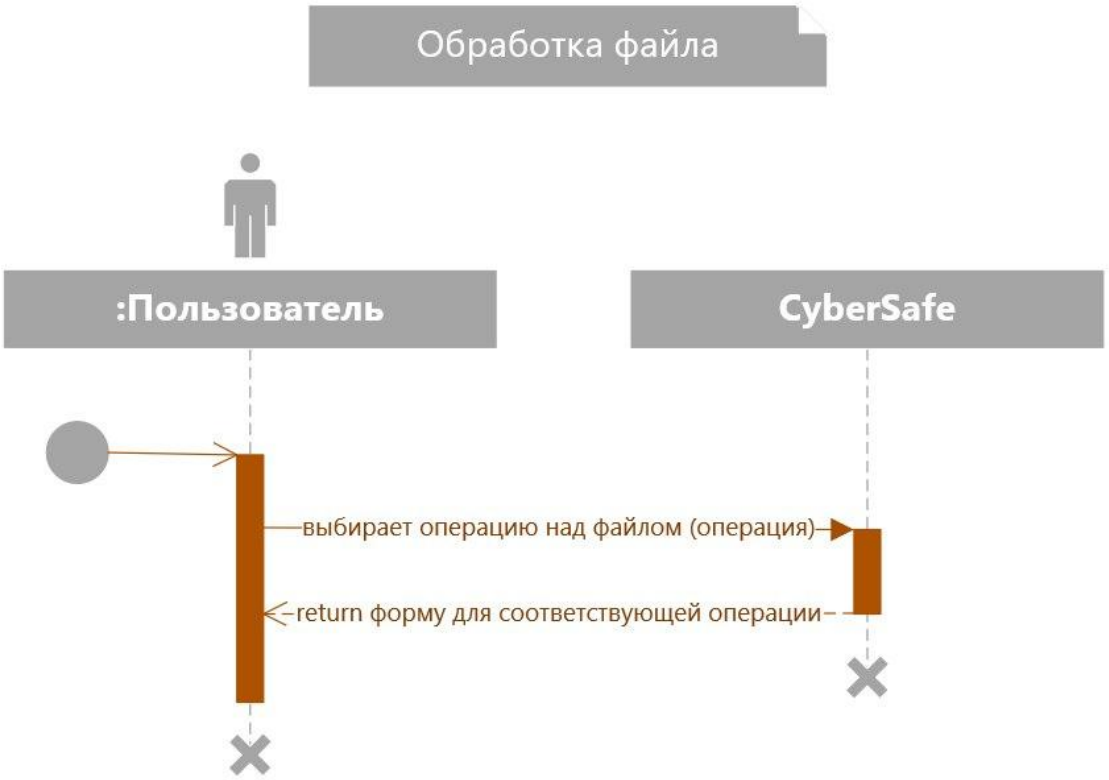

Рисунок 1.12 - Диаграмма последовательности действий (обработка файла).

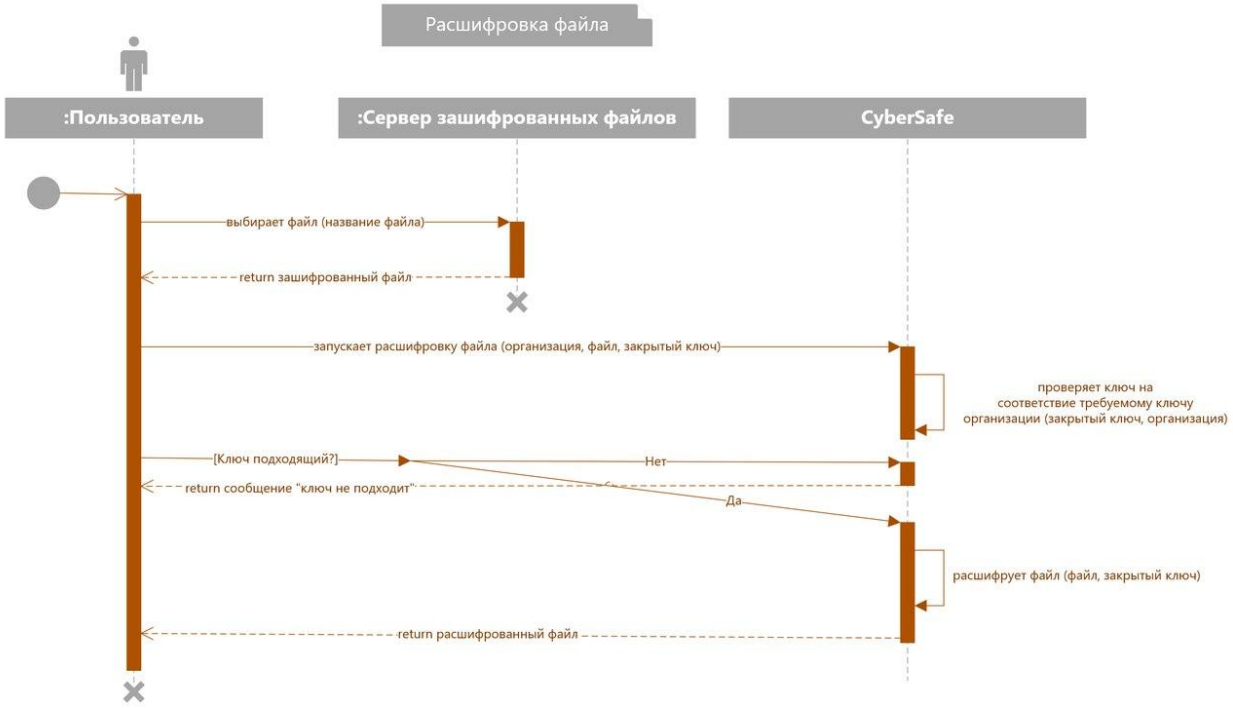

Рисунок 1.13 - Диаграмма последовательности действий (расшифровка файла).

Приложение 2

Таблица 1.1 Программы и функции

Функция	Folder Lock	PGP Desktop	CyberSafe Top Secret
Виртуальные зашифрованные диски	Да	Да	Да
Шифрование всего раздела	Нет	Да	Да
Шифрование системного диска	Нет	Да	Нет
Удобная интеграция с почтовыми клиентами	Нет	Нет	Да
Шифрование сообщений электронной почты	Да (ограничено)	Да	Да
Шифрование файлов	Нет	Да	Да
ЭЦП, подписание	Нет	Да	Да
ЭЦП, проверка	Нет	Да	Да

Продолжение таблицы 1. Программы и функции

Функция	Folder Lock	PGP Desktop	CyberSafe Top Secret
Прозрачное шифрование папки	Нет	Нет	Да
Самораспифровывающиеся архивы	Да	Да	Да
Облачное резервное копирование	Да (платно)	Нет	Да (бесплатно)
Система доверенных приложений	Нет	Нет	Да
Поддержка сертифицированного криптопровайдера	Нет	Нет	Да
Поддержка токенов	Нет	Нет (поддержка прекращена)	Да (при установке КриптоПро)

Продолжение таблицы 1. Программы и функции

Функция	Folder Lock	PGP Desktop	CyberSafe Top Secret
Собственный сервер ключей	Нет	Да	Да
Двухфакторная аутентификация	Нет	Нет	Да
Сокрытие отдельных файлов	Да	Нет	Нет
Сокрытие разделов жесткого диска	Да	Нет	Да
Бумажники для хранения платежной информации	Да	Нет	Нет
Поддержка шифрования ГОСТ	Нет	Нет	Да
Русский интерфейс	Нет	Нет	Да