

**Государственное Бюджетное Профессиональное
Образовательное Учреждение города Москвы
«Колледж связи №54»
имени П.М.Вострухина.**

**Выпускная квалификационная работа
«Обеспечение безопасности конфиденциальной
информации, сопровождающейся разработкой
программного продукта для криптографической защиты»**

*Выполнена студентом
группы 123И00Т1
Квеквескири В.А.*

*Руководитель
преподаватель
Юмаева.А.А.*

Актуальность темы определяется следующими проблемами:

Утечка информации происходит при:

- **хранении,**
- **обработке,**
- **передачи информации на электронных вычислительных машинах.**



Цель работы:

- **изучение вопроса обеспечения безопасности конфиденциальной информации**



- **разработка собственного программного продукта для криптографической защиты информации**

Задачи:

- Изучить методы и средства защиты конфиденциальной информации;
- Изучить виды защиты конфиденциальной информации, особое внимание, уделяя криптографической защите;
- Проанализировать требования, предъявляемые к криптографическим системам;
- Разработать собственное программное обеспечение, предназначенное для криптографической защиты информации;



ГЛАВА 1. СОВРЕМЕННЫЕ СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ



ФЗ № 149 «Об информации,
информационных технологиях и защите
информации»



«конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

Виды конфиденциальной информации



ФЕДЕРАЛЬНЫЙ ЗАКОН
«ОБ ИНФОРМАЦИИ,
ИНФОРМАТИЗАЦИИ
И ЗАЩИТЕ ИНФОРМАЦИИ»




В РЕДАКЦИИ ФЕДЕРАЛЬНОГО ЗАКОНА
от 10.01.2003 № 15-ФЗ

в РЕДАКЦИИ ФЕДЕРАЛЬНОГО ЗАКОНА
от 10.01.2003 № 15-ФЗ

Указ Президента РФ

№ 188 «Об утверждении Перечня сведений конфиденциального характера»



Методы защиты конфиденциальной информации

Препятствие

Маскировка

Регламентация

Управление

Принуждение

Побуждение



**Средства защиты
конфиденциальной
информации**

Технические
(аппаратные)

Программные

Организационные

Виды защиты конфиденциальной информации

```
graph TD; A[Виды защиты конфиденциальной информации] --> B[Правовая]; A --> C[Техническая]; A --> D[Физическая]; A --> E[Криптографическая];
```

Правовая

Техническая

Физическая

Криптографическая

Правовая защита информации

Международное право

Договоры
Патенты
Авторские права
Лицензии

Внутригосударственное право

Государственные

Конституции
Законы
Указы
Постановления

Ведомственные

Приказы
Положения
Инструкции

Технические средства защиты информации

средства
обнаружения



средства активного
противодействия



средства
пассивного
противодействия



Физические системы защиты

Системы
физической и
гражданской
изоляции



Системы
контроля
доступа



Запирающие
устройства и
хранилища





**Методы
криптографического
преобразования
информации**

Кодирование

Шифрование

Стенография

Сжатие

Симметричные криптосистемы



Ассиметричные криптосистемы



Электронные цифровые подписи

— это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого к



Требования к криптографическим системам

Стойкость шифра



Секретность ключа



Неизменность



Ограничение времени шифрования



Программная и аппаратная реализация

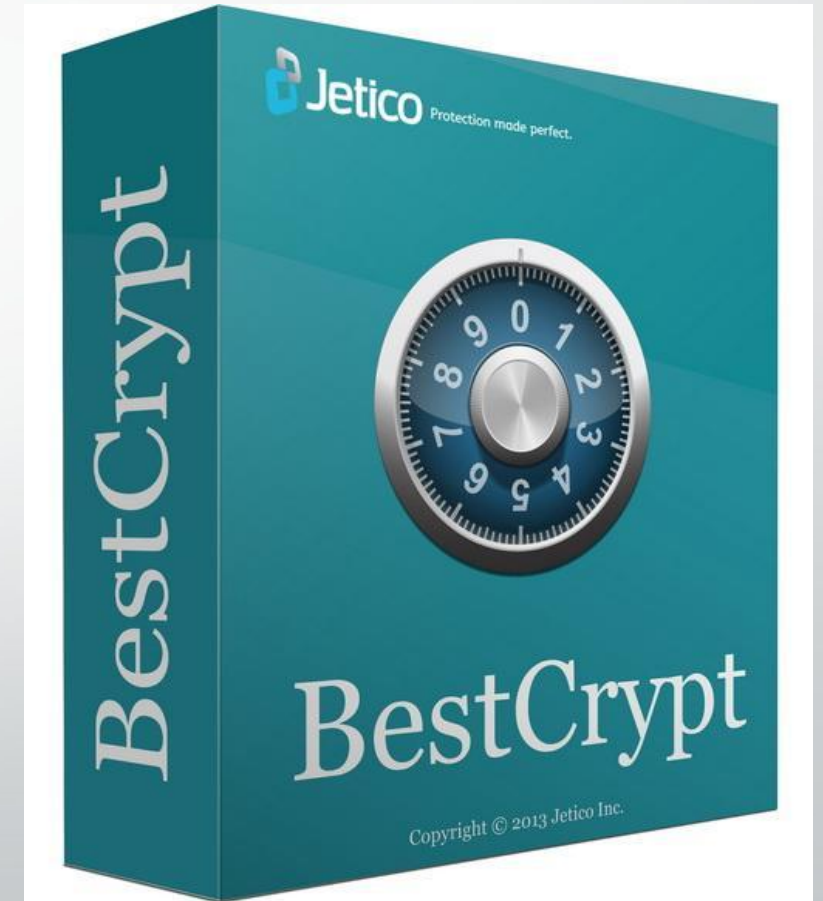


ГЛАВА 2. РАЗРАБОТКА ПРОГРАММНОГО ПРОДУКТА ДЛЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ



BestCrypt

Наименование продукта	BestCrypt
Тип	Программны й
Цена	5 000 руб.
Срок действия	2 года
Работа на с OS Windows	Работает
Алгоритм работы	Симметричный— RSA



Pretty Good Privacy security

Наименование продукта	PGP security
Тип	Программный
Цена	4000 руб.
Срок действия	Неограничен
Работа на с OS Windows	Работает
Алгоритм работы	Ассиметричный -DSA



eToken logon/72K

Наименование продукта	eToken logon/72K
Тип	Программно– аппаратный
Цена	4500 руб.
Срок действия	Неограничен
Работа на с OS Windows	Работает
Алгоритм работы	Асимметричный –DSA

The logo for eToken, featuring the word "eToken" in a stylized font. The "e" is in a red, cursive script, while "Token" is in a black, serif font. A small "TM" trademark symbol is positioned to the upper right of the "n".

**Надежность
передачи
информации**

**Простота
использования**

**Использование
собственного
алгоритма
шифрования.**

**Возможность
обновления
алгоритма
шифрования в целях
предотвращения
раскрытия ключа**

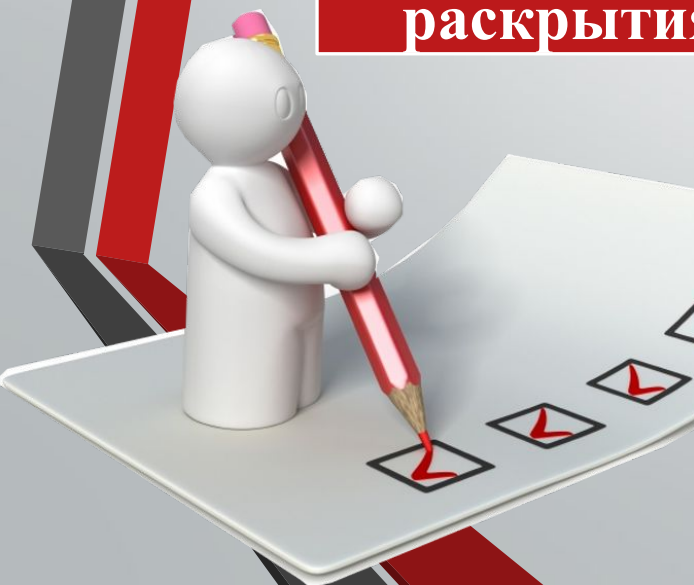
**Невысокие
требования к
вычислительной
мощности
компьютера**

**Поддержка OS
Windows**

**Минимальные
затраты на
разработку и
обслуживание
программы**

**Возможность
использования в
комплексе с
другими методами
защиты**

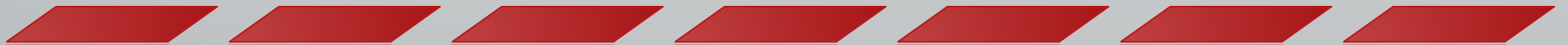
Основные требования



Среда разработки Microsoft Visual Studio



Интегрированная среда разработки программного обеспечения и ряда других инструментальных средств



Генератор шифрования текста

RGB RGB RGB

6	54	56	40	160	200	255	50	100
---	----	----	----	-----	-----	-----	----	-----

Т	О	К
----------	----------	----------

Работа программного комплекса криптографической защиты информации «ХВ»



Для разработки программы потребовались следующие трудовые ресурсы:

- **Один штатный сотрудник в должности программиста;**

В должностные обязанности специалиста входят:

- **Разработка и установка программного продукта;**
- **Создание пакетов обновлений и обслуживания для эффективной работы программы;**
- **Инструктаж сотрудников по эксплуатации данного продукта.**



Соотношение затрат на разработку собственного программного продукта по отношению к рыночным услугам



**Затраты на разработку собственного
продукта «ХВ» в 4,8 раз меньше по
отношению к рыночным ценам, экономия
составит**

151 832,4 руб.,

то есть ~ 79%



Вывод

Несмотря на ценность информации в нашей жизни, по статистике, в большинстве случаев утечка информации происходит при хранении, обработке и передачи информации на электронных вычислительных машинах. Попытки злоумышленников получить доступ к информации необходимо пресекать программными методами. Поставленные цели и задачи выпускной квалификационной работы достигнуты в полном объеме.





**СПАСИБО ЗА
ВНИМАНИЕ!**