**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc212431639)

[1. ДОКУМЕНТАЦИЯ ПО ПРОЕКТИРОВАНИЮ 4](#_Toc212431640)

[1.1 Общая идея проекта 4](#_Toc212431641)

[1.2. Сравнительный анализ существующих решений 4](#_Toc212431642)

[1.3. Нормативно-правовые акты, необходимые при разработке шифратора 5](#_Toc212431643)

[1.4. Техническое описание 7](#_Toc212431644)

[2. СОЗДАНИЕ ОСНОВНОГО ПРИЛОЖЕНИЯ 13](#_Toc212431645)

[3. ЭКОНОМИЧЕСКАЯ ЧАСТЬ 19](#_Toc212431646)

[ЗАКЛЮЧЕНИЕ 22](#_Toc212431647)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 23](#_Toc212431648)

# ВВЕДЕНИЕ

Во все времена люди пытались скрыть ту или иную информацию от других. По мере развития цивилизации информации становилось всё больше, а необходимость её скрывать всё важнее и труднее. Всегда существовала и совершенно секретная информация, которая известна определенному кругу лиц и не должна быть обнародована. Важнейшим элементом цифровой техники, особенно в компьютерах и системах управления, являются шифраторы и дешифраторы, способные преобразовывать открытую информацию в закрытую и обратно. Шифрование выполняется согласно алгоритму шифрования с использованием ключа - небольшой порции информации.

Целью работы является изучение простейших методов шифрования и разработка собственной программы-шифратора с алгоритмами шифрования и дешифрования.

Задачами, поставленными перед разработкой программы, можно назвать изучение азов по программированию на языке программирования Python, создание и разработку алгоритмов шифровки и дешифровки данных.

Объектом исследования является шифрование данных.

Предметом исследования является разработка шифратора «CTIPTOSFER».

Методами исследования являются объектно-ориентированное программирование, сравнительный анализ и математическая обработка данных.

# 1. ДОКУМЕНТАЦИЯ ПО ПРОЕКТИРОВАНИЮ

## 1.1 Общая идея проекта

Шифратор «CRYPTOSFER» - программное обеспечение, основной задачей которого будет являться шифрование и дешифрование данных. Отличительной чертой данного программного обеспечения будет являться интерактивность. Шифратор будет создан, чтобы пользователи могли легко обезопасить свои данные, путём шифрования данных, а также, чтобы пользователи могли самостоятельно изучить, как работают различные методы шифрования.

Шифратор будет ориентирован на широкую целевую аудиторию, охватывающую пользователей различных возрастных групп, начиная с 6 лет.

## 1.2. Сравнительный анализ существующих решений

Чтобы определить, что шифратор будет иметь значение для пользователей, нужно провести сравнительный анализ существующих решений на рынке программного обеспечения для шифрования данных. В таблице 1 представлен детальный анализ конкурентов и моего шифратора «Criptosfer».

Таблица 1.

Сравнение с существующими решениями

| Название шифратора | Достоинства | Недостатки |
| --- | --- | --- |
| VeraCrypt | Бесплатное программное обеспечение;  Открытый исходный код;  Поддержка нескольких операционных систем. | Сложный интерфейс для неподготовленных пользователей;  Ориентация на шифрование файлов и томов, а не текста;  Требует значительных технических знаний;  Не подходит для детей и начинающих пользователей;  Отсутствие игровых или образовательных режимов. |
| GNU Privacy Guard | Мощные криптографические алгоритмы;  Кроссплатформенность;  Поддержка цифровых подписей. | Работа преимущественно через командную строку;  Сложность настройки и использования;  Ограниченный выбор методов шифрования; Необходимость управления ключами;  Отсутствие графического интерфейса в базовой версии;  Не подходит для быстрого шифрования текста. |
| BitLocker | Прозрачное шифрование для пользователя;  Надежная защита данных. | Доступен только в профессиональных версиях Windows;  Ориентация на шифрование дисков, а не текста; Привязка к экосистеме Microsoft;  Отсутствие портативной версии;  Невозможность использования в образовательных целях. |
| Criptosfer | Простой и интуитивно понятный интерфейс;  Поддержка трех различных методов шифрования;  Специализация на текстовом шифровании;  Наличие игрового образовательного режима;  Современный визуальный дизайн;  Минимальные требования к техническим знаниям;  Быстрое выполнение операций шифрования. | Ориентация на базовые методы шифрования;  Отсутствие поддержки шифрования файлов. |

По результатам анализа таблицы разрабатываемый шифратор «CRIPTOSFER» превосходит существующие решения по многим аспектам.

## 1.3. Нормативно-правовые акты, необходимые при разработке шифратора

При разработке программного обеспечения, связанного с шифрованием и дешифрованием данных, необходимо строго соблюдать установленные нормативные правовые акты. Деятельность в этой сфере регулируется, в первую очередь, Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (последняя редакция от 24.04.2024).

Общие положения в сфере защиты информации, включая криптографическую, устанавливает Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция от 24.04.2024).

Конкретные требования к мерам безопасности при обработке персональных данных с использованием криптографии определяются Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации» (последняя редакция от 25.12.2020).

Лицензионные требования, предъявляемые к соискателям лицензии, такие как квалификация сотрудников, оснащение помещений и оборудование, подробно изложены в Постановлении Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств...» (последняя редакция от 30.12.2023).

Процессы разработки, производства и эксплуатации шифровальных средств, не предназначенных для защиты государственной тайны, регламентирует Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (последняя редакция от 15.08.2022).

Порядок обеспечения безопасности при хранении, обработке и передаче информации с использованием криптографии устанавливает Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (последняя редакция от 13.02.2024).

Важную роль играет и Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (последняя редакция от 02.07.2021), поскольку введение режима коммерческой тайны на предприятии является одним из обязательных лицензионных требований для обеспечения конфиденциальности.

Технической основой для создания шифраторов служат государственные стандарты. В области криптографических алгоритмов ключевыми являются ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», введённый 30.06.1990, ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования», введённый 01.01.2013, ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», введённый 01.01.2013, ГОСТ Р 34.12–2018 «Информационная технология. Криптографическая защита информации. Блочные шифры», введённый 01.06.2019, ГОСТ Р 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» (введен 01.06.2019).

## 1.4. Техническое описание

Функциональная модель системы.

Для структурного представления функций проектируемого шифратора «CRYPTOSFER» спроектирована функциональная модель в нотации IDEF0, представленная на рисунке 1.

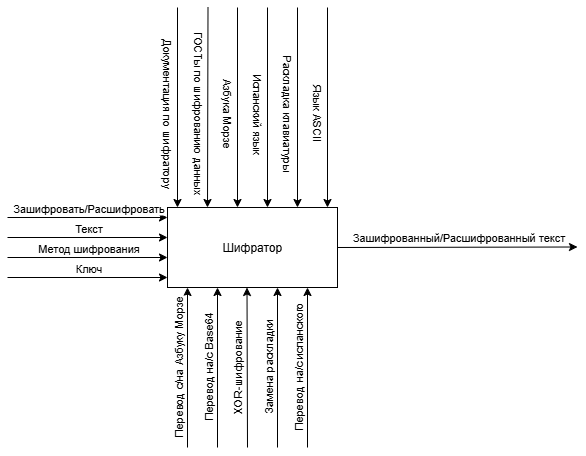


Рисунок 1. IDEF0

Архитектура приложения.

Графический интерфейс будет построен с использованием библиотеки CustomTkinter, которая обеспечит современный внешний вид приложения. Главное окно будет содержать четыре основные кнопки для доступа к функционалу: шифрование, дешифрование, игровой режим и настройки. Каждое из окон функциональности будет иметь единообразный дизайн с кнопкой возврата в главное меню, четким разделением на зоны ввода и вывода данных, а также интуитивно понятными элементами управления.

Приложение будет построено по объектно-ориентированной архитектуре с выделением отдельных классов для каждого основного окна. Будет создан основной класс CryptoApp, отвечающий за главное окно приложения, и производные классы EncryptionWindow для окна шифрования, DecryptionWindow для окна дешифрования и GameWindow для окна игры. Каждый класс будет инкапсулировать всю логику работы соответствующего окна, включая обработку событий, вызов методов шифрования и управление интерфейсом.

Используемые технологии и зависимости.

Для разработки приложения шифратора будет использоваться язык программирования Python версии 3.11. В качестве основной среды разработки будет применяться интегрированная среда разработки Visual Studio Code, представленная на рисунке 2, которая предоставляет удобные инструменты для написания, отладки и тестирования кода.

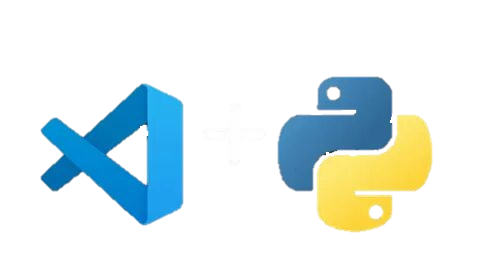


Рисунок 2. Visual Studio Code и Python

Для создания графического интерфейса нужно использовать библиотеку CustomTkinter - современную версию стандартной библиотеки Tkinter с улучшенным внешним видом элементов управления, показанную на рисунке 3. Для реализации функций шифрования будут задействованы встроенная библиотека Python для кодирования Base64, модуль sys, позволяющий закрывать программу и сторонняя библиотека для работы с азбукой Морзе MorseCodePy. Дополнительно будет использоваться библиотека random для генерации случайных элементов в игровом режиме.



Рисунок 3. CustomTkinter

Методы шифрования

Для шифратора необходимо определить доступные методы шифрования. Все методы, которые будут добавлены в шифратор, определены в таблице 2.

Таблица 2.

Методы шифрования

| Метод шифрования | Описание метода |
| --- | --- |
| Азбука Морзе | Метод знакового кодирования, в котором буквы алфавита, цифры, знаки препинания и другие символы представляются в виде последовательностей коротких и длинных сигналов — «точек» и «тире». |
| Base64 | Метод переводит текст в бинарный вид, а затем бинарные данные кодируются в текстовый формат, использующий 64 символа ASCII. |
| По ключу | Метод зашифровывает текст с помощью исключающего или. |
| Замена раскладки клавиатуры | Метод заменяет текст, будто бы пользователь всё это время писал с неправильной раскладкой клавиатуры. |

Механика шифрования

Для шифрования текста, необходимо перейти главного меню, которое показано на рисунке 4. Затем перейти в окно «ЗАШИФРОВАТЬ!», показанное на рисунке 5. В блоке ввода необходимо будет ввести текст, который необходимо зашифровать. Далее, нужно нажать на кнопку с названием выбранного метода шифрования. Если это метод шифрования по ключу, то необходимо ввести ключ в строку ввода, а затем нажать на кнопку «Зашифровать →». Программа зашифрует данные и выведет полученный результат в правый блок.

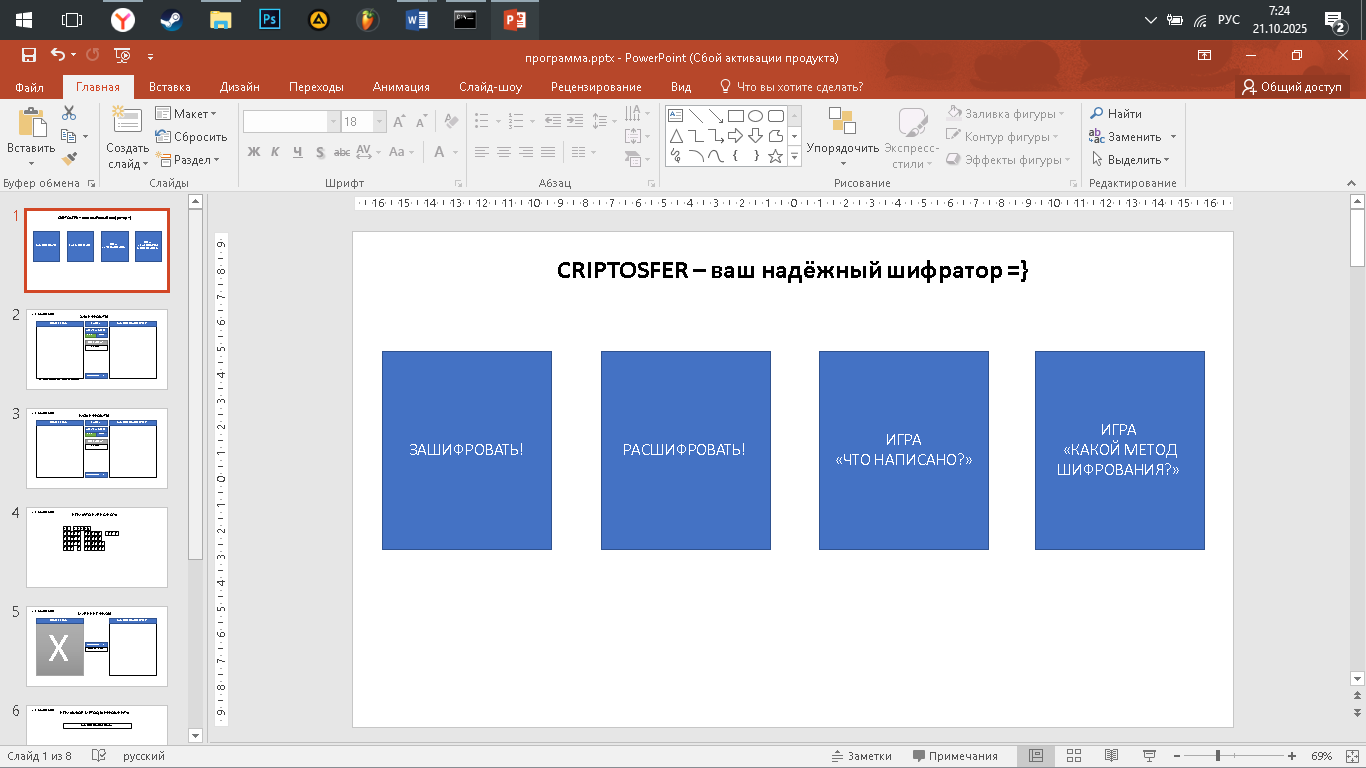


Рисунок 4. Главное меню

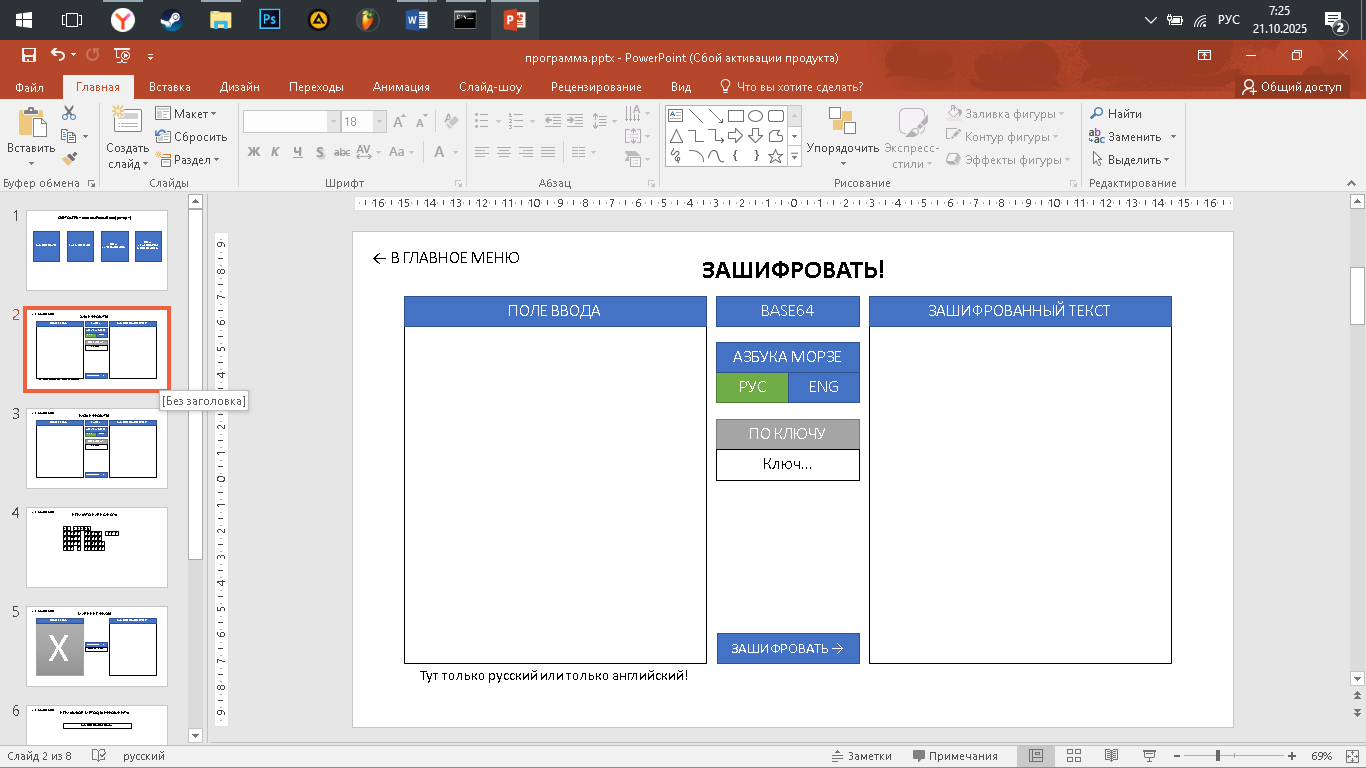


Рисунок 5. Окно зашифровки текста

Для расшифровки текста, необходимо перейти главного меню. Затем перейти в окно «РАСШИФРОВАТЬ!», продемонстрированное на рисунке 6. В блоке ввода необходимо ввести текст, который необходимо расшифровать. Далее, нужно нажать на кнопку с названием выбранного метода шифрования. Если это метод шифрования по ключу, то необходимо ввести ключ в строку ввода, а затем нажать на кнопку «Расшифровать →». Программа расшифрует данные и выведет полученный результат в правый блок.

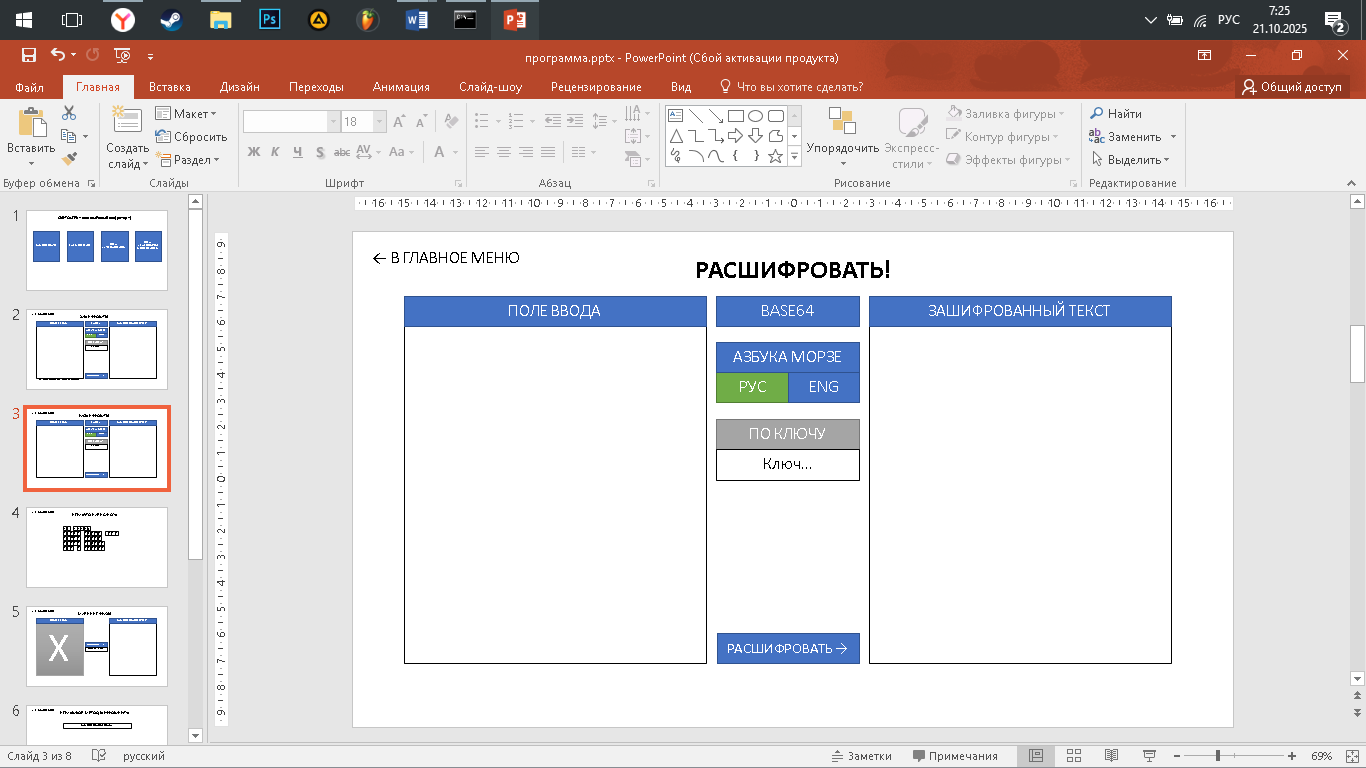


Рисунок 6. Окно расшифровки текста

Для прохождения интерактивной игры, необходимо перейти главного меню. Затем перейти в окно «ИГРА «КАКОЙ МЕТОД ШИФРОВАНИЯ?»», изображённое на рисунке 7. Затем пользователю будет выдан вопрос и 3 кнопки с вариантами ответа на него. Если пользователь правильно ответит на вопрос, то кнопка окрасится в зелёный цвет, что показано на рисунке 8, а если неправильно, то в красный, а кнопка с правильным вариантом ответа окрасится в зелёный цвет, что продемонстрировано на рисунке 9. После нужно нажать на кнопку «Далее →» или на кнопку «← выйти в главное меню», если тест был пройден. Результат того, на сколько вопросов пользователь ответил правильно, будет написан внизу окна.

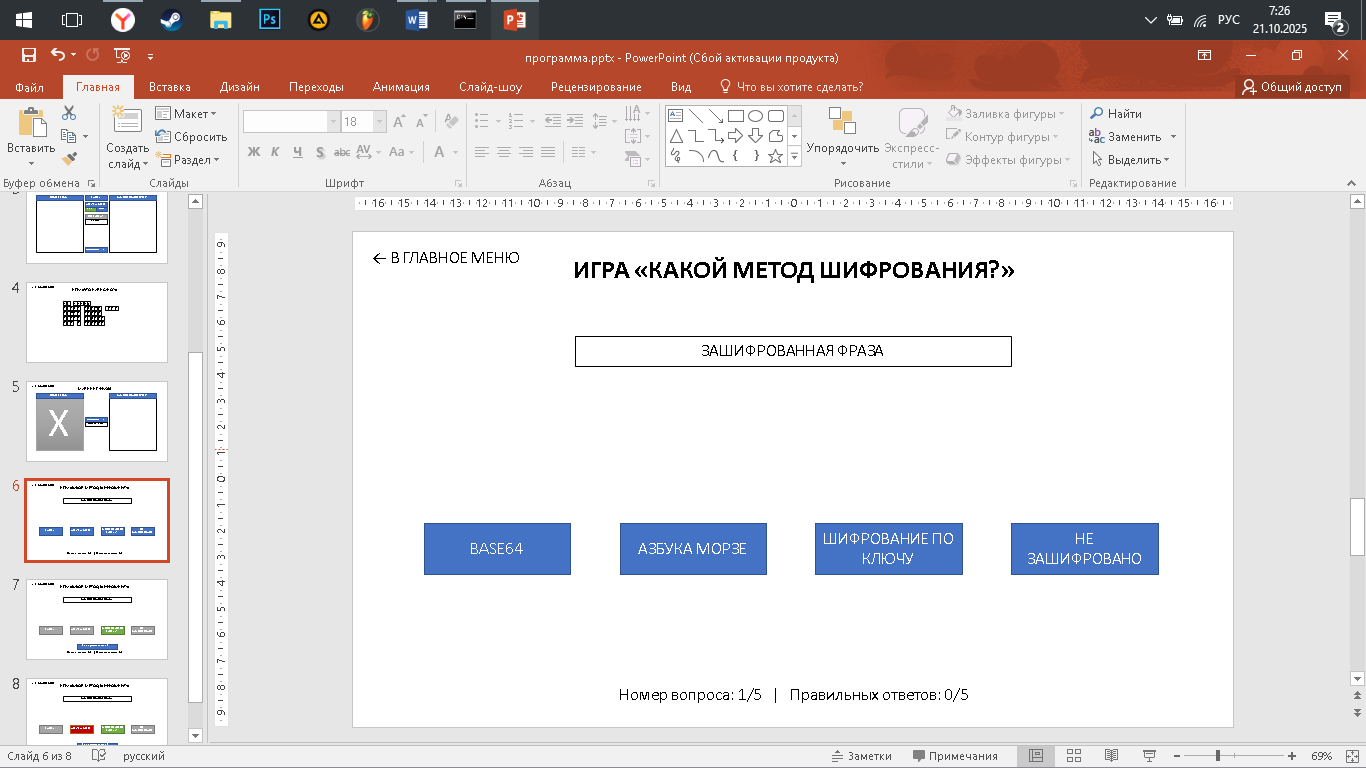


Рисунок 7. Игра «Какой метод шифрования?»

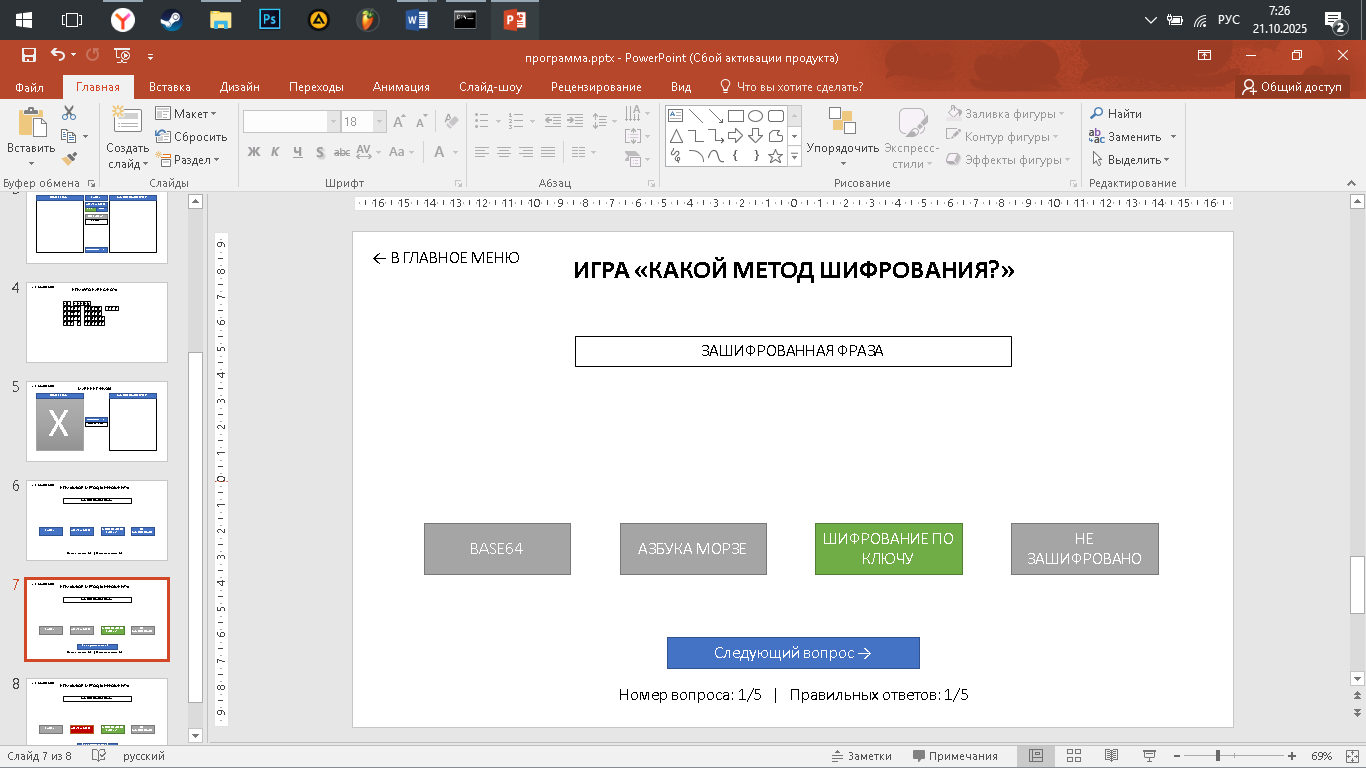


Рисунок 8. Пользователь правильно ответил на вопрос

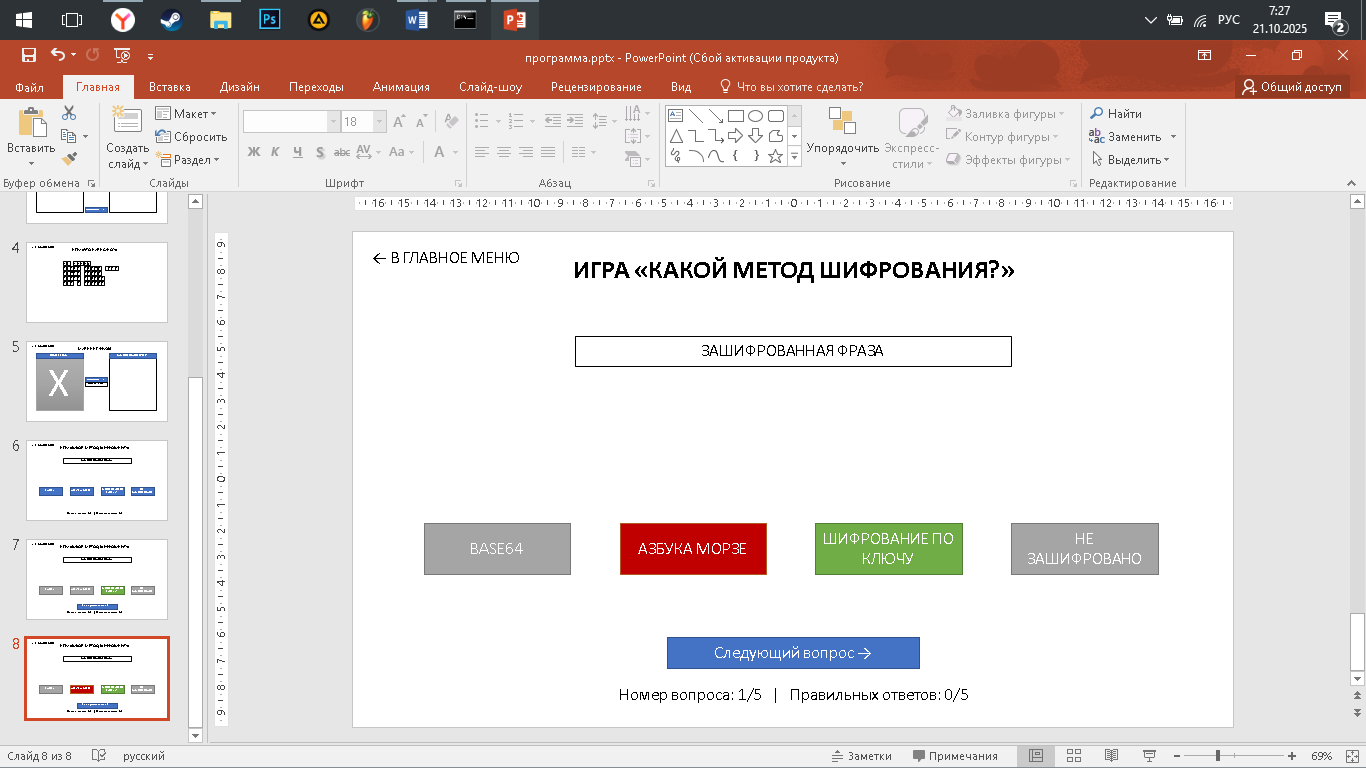


Рисунок 9. Пользователь неправильно ответил на вопрос

Таким образом, в разделе 1 был определен концепт шифратора «CRYPTOSFER», были изучены строгие нормативно-правовые аспекты разработки криптографического ПО и определены технические стандарты, а также разработана архитектура приложения, выбраны технологии и методы шифрования, что создало прочный фундамент для последующей реализации проекта.

# 2. СОЗДАНИЕ ОСНОВНОГО ПРИЛОЖЕНИЯ

Для реализации основного приложения необходимо создать класс CryptoApp, который наследуется от CTk и представляет главное окно программы. Данный класс изображён на рисунке 10.

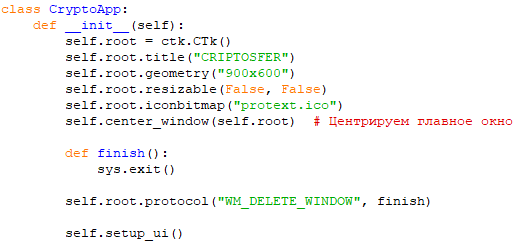


Рисунок 10. Класс главного приложения

Для центрирования окна на экране нужно реализовать метод center\_window, показанный на рисунке 11.

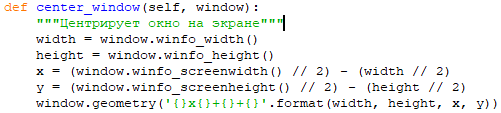


Рисунок 11. Метод, центрирующий окно на экране

Нужно создать метод setup\_ui, показанный на рисунке 12, в котором создаётся пользовательский интерфейс, показанный на рисунке 13 с заголовком программы и тремя основными кнопками: «ЗАШИФРОВАТЬ», «РАСШИФРОВАТЬ», «ИГРА «КАКОЙ МЕТД ШИФРОВАНИЯ?»».

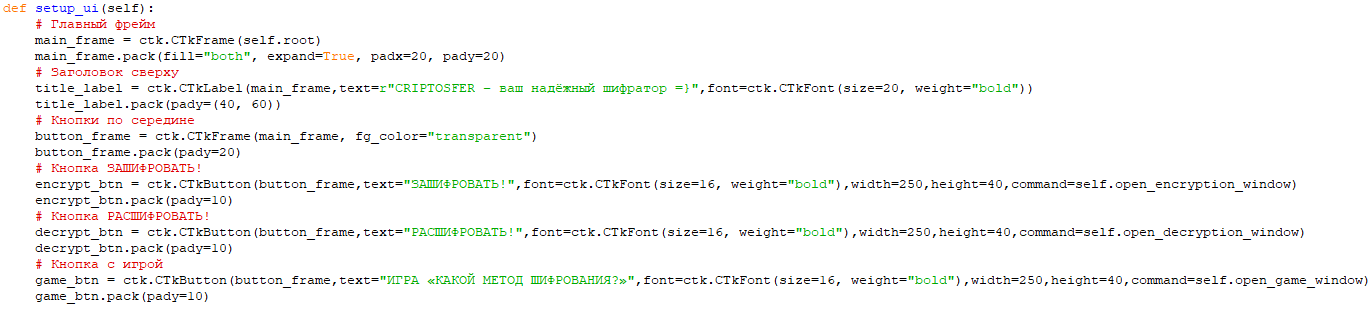


Рисунок 12. Метод создания интерфейса главного меню

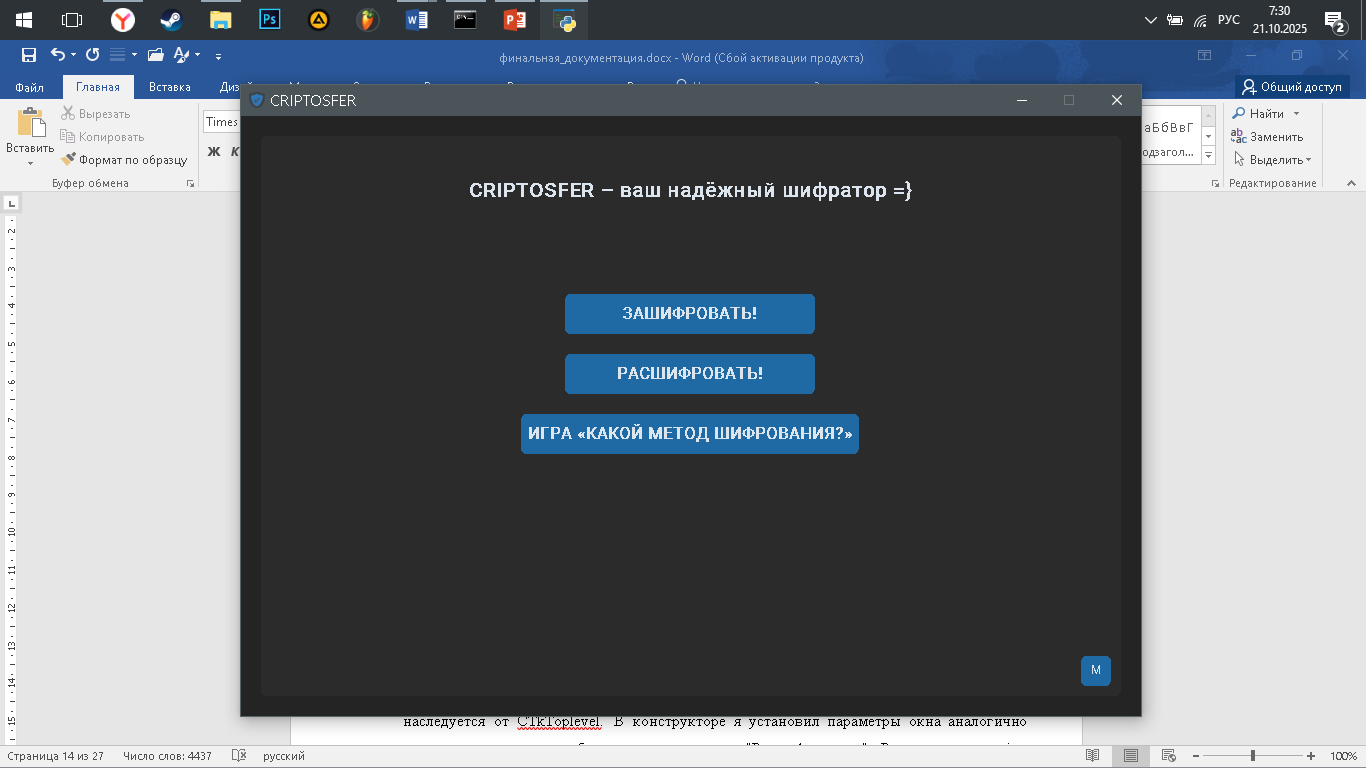


Рисунок 13. Интерфейс главного меню

Для реализации окна шифрования нужно создать класс EncryptionWindow, который наследуется от CTkToplevel. Данный класс показан на рисунке 14.

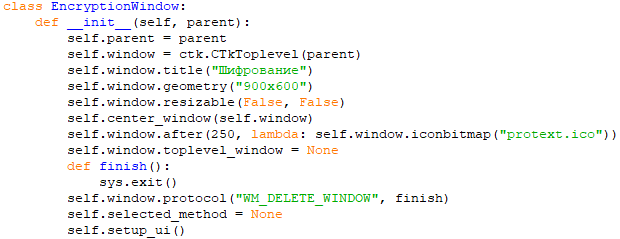


Рисунок 14. Класс с окном шифрования

Нужно создать метод setup\_ui, в котором создаётся интерфейс с тремя основными областями, как показано на рисунке 15.

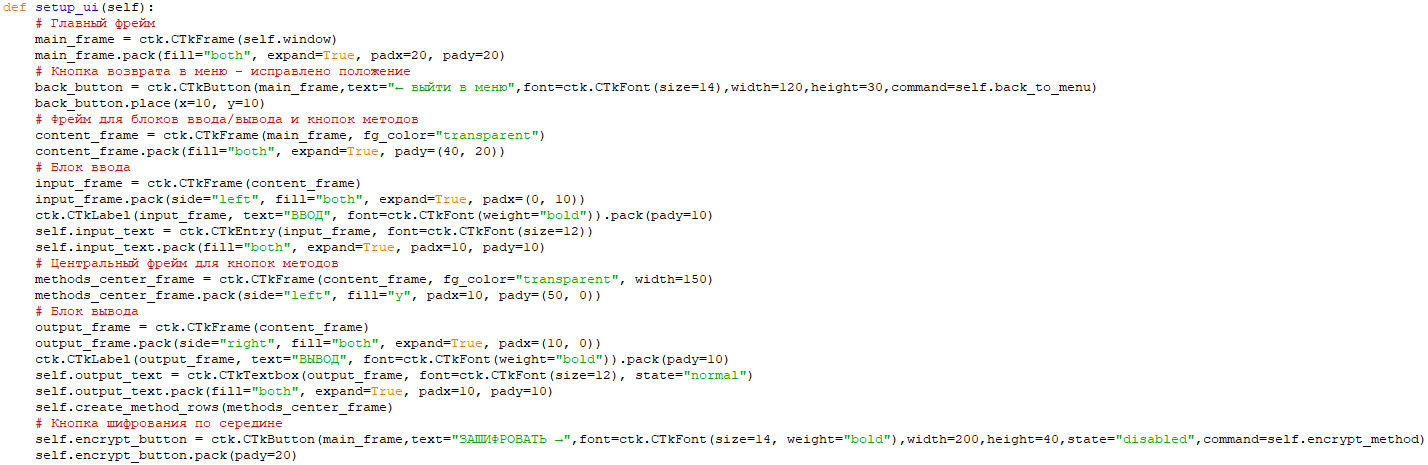


Рисунок 15. Создание интерфейса с 3 областями

Для каждого метода шифрования необходимо создать отдельные кнопки с обработчиком события select\_method, который изменяет цвет выбранной кнопки и активирует кнопку шифрования. Данное окно показано на рисунке 16.

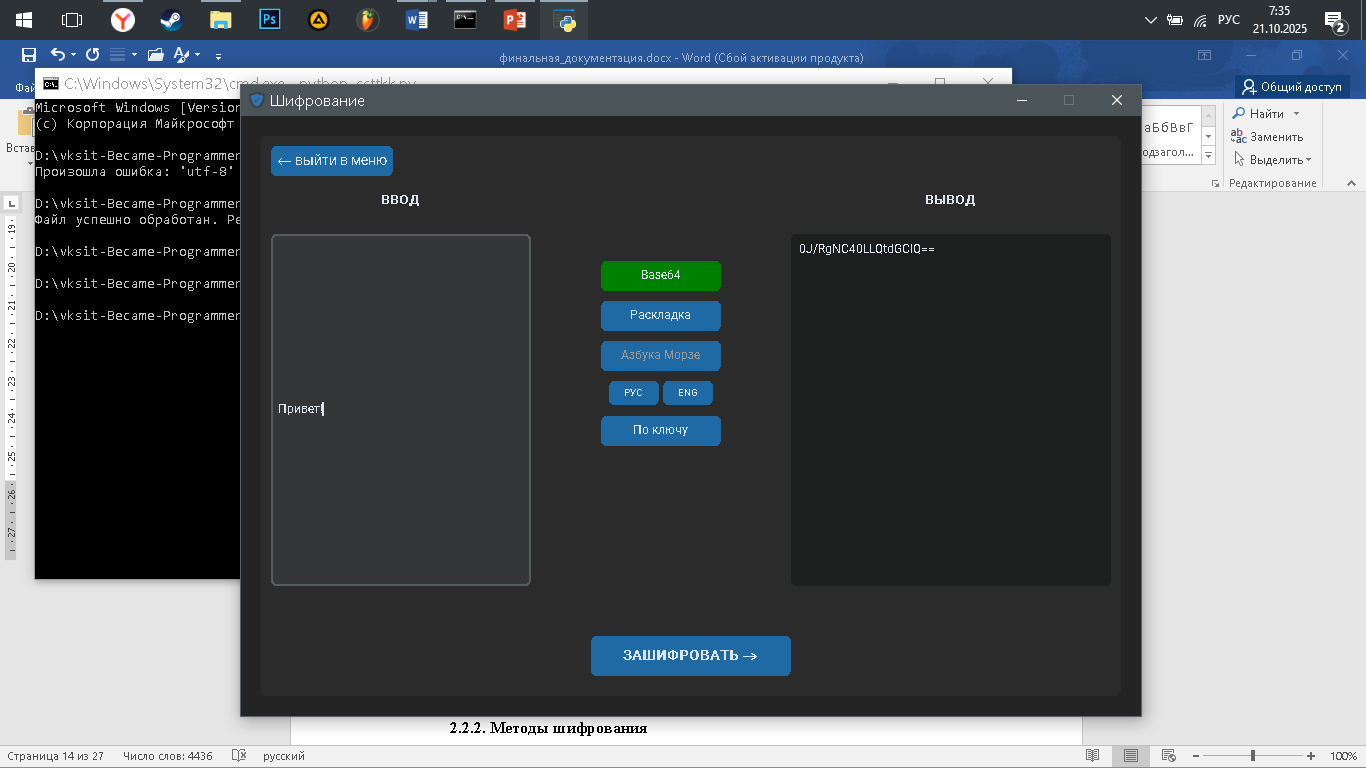


Рисунок 16. Окно шифрования

Необходимо реализовать четыре основных метода шифрования. Код их реализации представлен на рисунке 17.

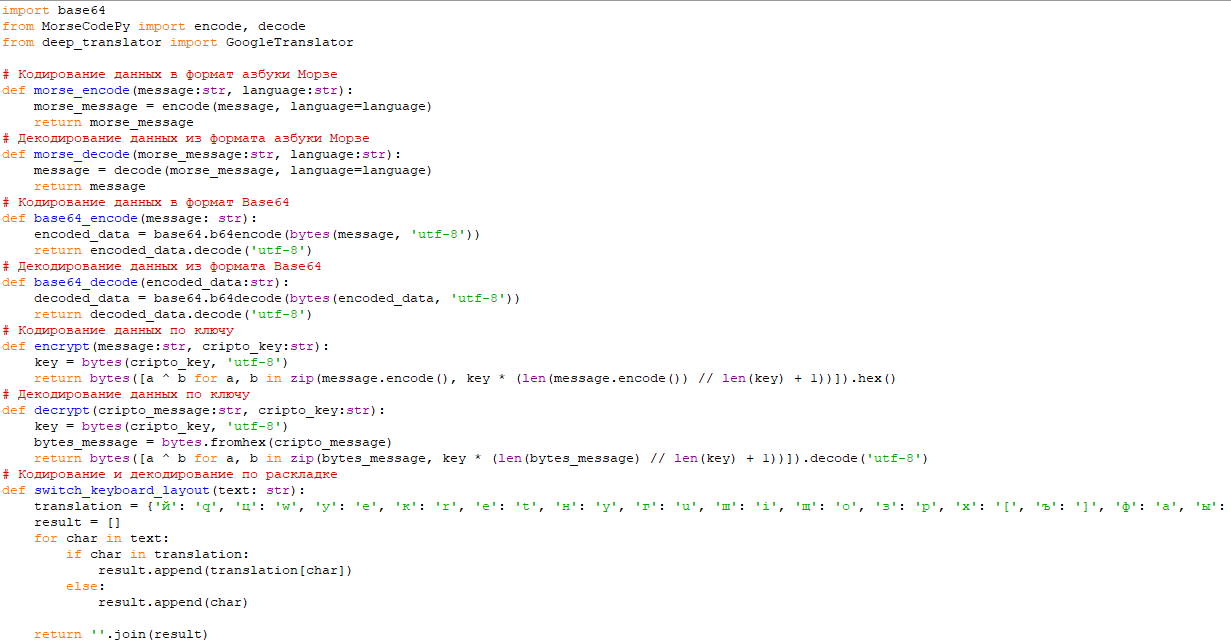


Рисунок 17. Код реализации методов шифрования

Класс DecryptionWindow необходимо реализовать по аналогии с EncryptionWindow. В интерфейсе нужно сохранить ту же структуру, но функциональность кнопок изменить для выполнения операций расшифрования. Данное окно показано на рисунке 18, а методы расшифровывания представлены на рисунке 19.

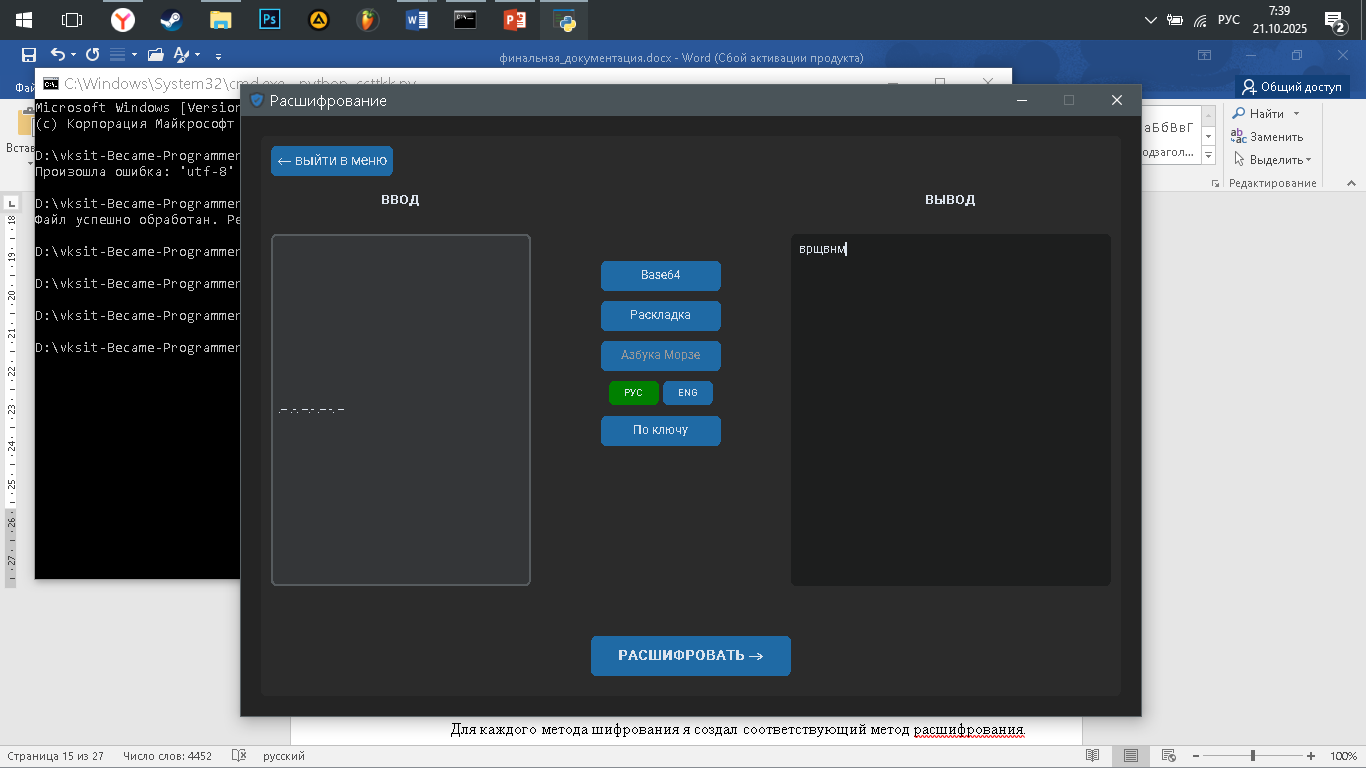


Рисунок 18. Окно расшифровки

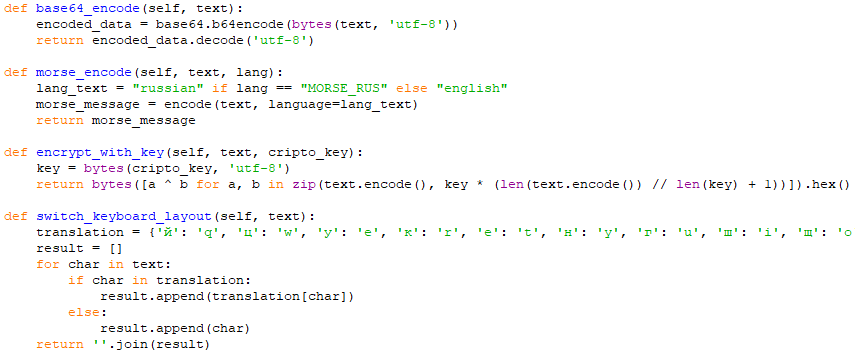


Рисунок 19. Методы расшифровывания

Реализация интерактивной игры.

Для создания образовательной интерактивной игры «Угадай метод шифрования» нужно разработать класс GameWindow. Игровую механику нужно построить на последовательности из пяти вопросов, в каждом из которых пользователю показывается зашифрованное слово и четыре варианта методов шифрования. Окно с игрой показано на рисунке 20.

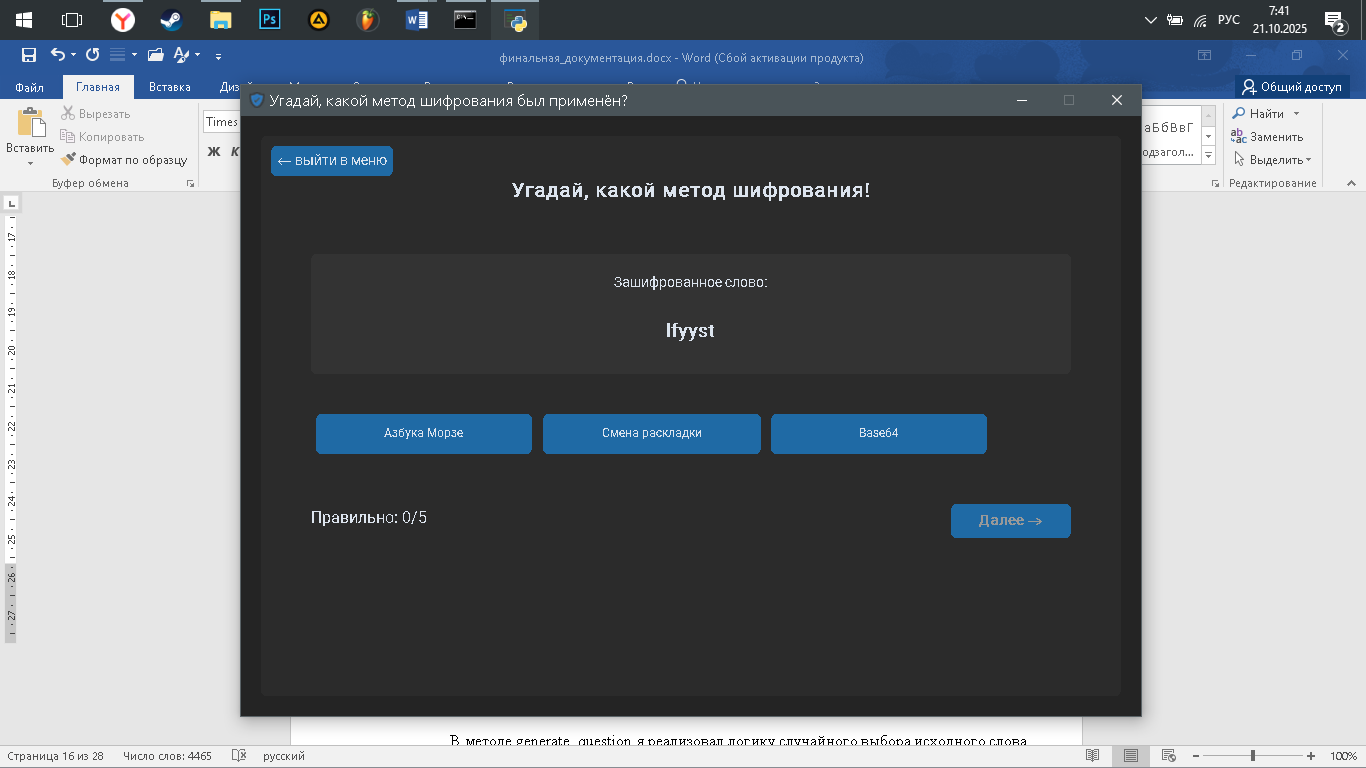


Рисунок 20. Игра «Угадай метод шифрования»

В методе generate\_question необходимо реализовать логику случайного выбора исходного слова из предопределенного списка и случайного выбора метода шифрования из трех доступных, показанную на рисунке 21.



Рисунок 21. Метод случайной зашифровки текста

Далее необходимо реализовать единую систему навигации между всеми окнами приложения. В каждое дочернее окно необходимо добавить кнопку возврата в главное меню, которая уничтожает текущее окно и снова показывает главное окно с помощью метода back\_to\_menu, показанного на рисунке 22.

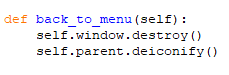


Рисунок 22. Метод возврата в главное меню

При закрытии любого из окон через системную кнопку закрытия необходимо предусмотреть корректное завершение работы всего приложения через команду «sys.exit()». Метод продемонстрирован на рисунке 23.

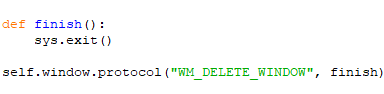


Рисунок 23. Метод закрытия шифратора

Во всех модулях шифрования и расшифрования нужно добавить блоки try-except для обработки потенциальных ошибок. В игре нужно предусмотреть обработку ошибок при генерации вопросов, чтобы гарантировать стабильную работу игры даже в случае непредвиденных ситуаций.

Чтобы любой пользователь смог запустить шифратора, необходимо скомпилировать код программы. Для этого необходимо установить библиотеку PyInstaller и с помощью специальной команды, изображённой на рисунке 24, скомпилировать наш код.

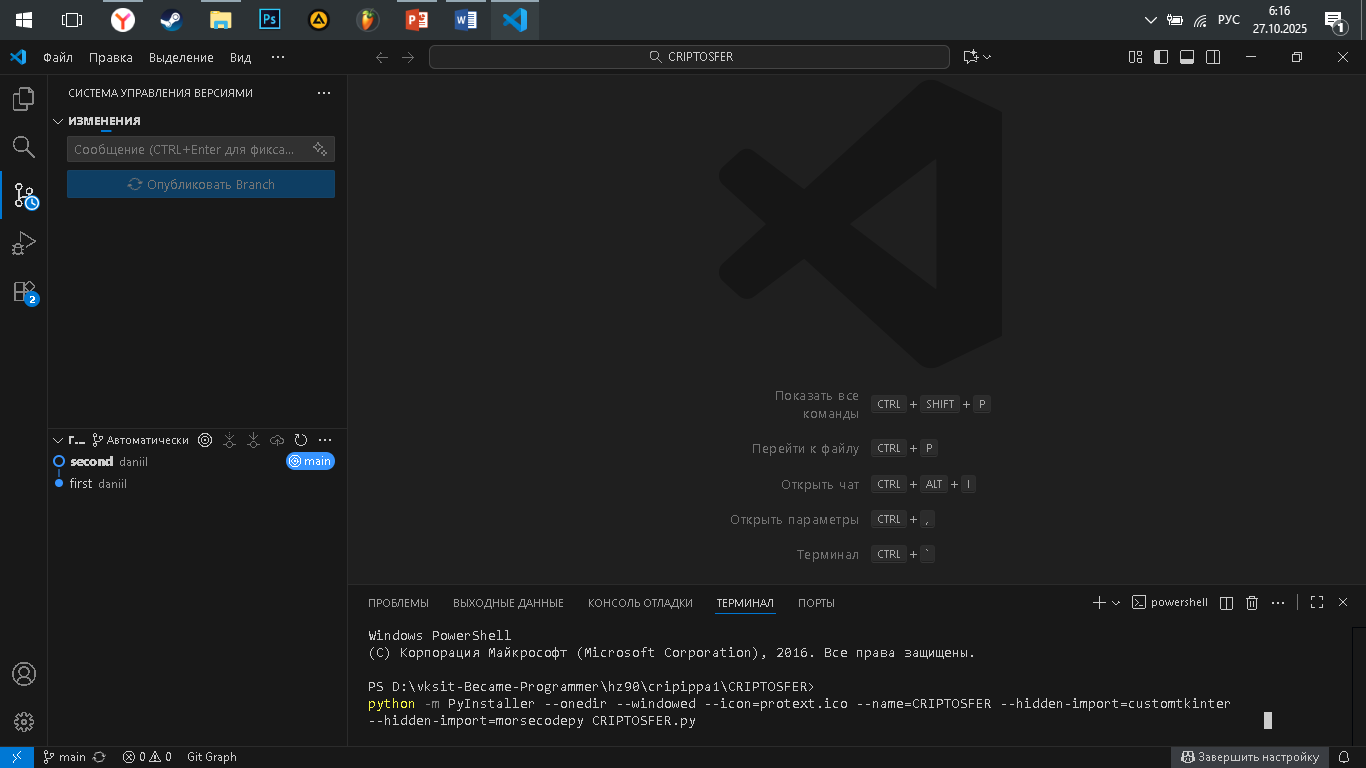


Рисунок 24. Команда для компиляции

Таким образом, в разделе 2 был успешно реализован шифратор в соответствии с проектом. Были созданы интуитивно понятный графический интерфейс на CustomTkinter, надежные модули шифрования и дешифрования для четырех методов, а также интерактивная игра. Шифратор был скомпилирован в исполняемую программу.

# 3. ЭКОНОМИЧЕСКАЯ ЧАСТЬ

Важный фактор, влияющий на величину выручки от реализации продукта – процесс ценообразования.

В конечном итоге цена продукта определяется рынком, она представляет собой компромисс между желанием продавца и возможностями покупателя. Исходным пунктом формирования цены продукта является калькуляция.

В настоящее время калькуляционный метод формирования цен остаётся основным, так как цена должна обеспечивать покрытие всех затрат и сверх того – получение прибыли.

Если рассчитанная калькуляционным методом цена окажется выше сложившейся на рынке, следует изыскать пути снижения затрат или отказаться от разработки данного продукта.

Наряду с калькуляционным методом применяются и другие методы формирования цен на вновь разработанные продукты: параметрические, зависящие от определённых параметров; статистический, основанный на анализе динамического ряда цен на аналогичные продукты.

Но при всех условиях цена должна возмещать затраты изготовителя (разработчика) продукта, поэтому использование калькуляций необходимо.

В Российских условиях проектируемая цена продукта при применении калькуляционного способа может рассчитываться способом, показанным на таблице 3.

Таблица 3.

Расчет стоимости продукта

|  |  |
| --- | --- |
| Статья затрат и элементы цены | Сумма, руб. |
| Затраты на электроэнергию | 401,7 |
| Заработная плата разработчика | 35280,08 |
| Отчисления с заработной платы | 10341,03 |
| Амортизация основных средств | 833,49 |
| Прочие расходы | 2342,81 |
| Общая сумма затрат | 49199,08 |
| Прибыль | 7379,86 |
| Цена продукта: | 56578,95 |

Затраты на электроэнергию.

Затраты на электроэнергию складываются из расходов на освещение помещения и расходов на производственное потребление. Исходные данные для расчётов отражены в таблице 4.

Таблица 4.

Затраты на электроэнергию

|  |  |
| --- | --- |
| Характеристика | Значение |
| Усредненный расход энергии, необходимой для освещения одного квадратного метра площади помещения в год, кВт | 50 |
| Площадь помещения, м2 | 25 |
| Расход энергии за год, кВт | 1250 |
| Количество дней для разработки продукта | 9 |
| Количество потребленной энергии за период разработки продукта, кВт | 31 |
| Тариф за 1 кВт/час, руб. | 8,71 |
| Стоимость электроэнергии для освещения помещения, руб. | 270,01 |
| Количество компьютеров, шт. | 1 |
| Потребление энергии одним компьютером, кВт | 0,2 |
| Коэффициент, учитывающий потери в сети | 1,05 |
| Количество часов работы компьютера за период разработки, час. | 72 |
| Стоимость электроэнергии для производственного потребления, руб. | 131,69 |
| Итого затраты на электроэнергию: | 401,7 |

Заработная плата разработчика.

Поскольку среднемесячная заработная плата составляет 86240,2 рублей, то затраты на оплату труда разработчика могут составить: 86240,2 рублей разделить на количество рабочих дней в месяце (22) и умножить на количество дней разработки.

Отчисления от заработной платы.

В настоящее время размер отчислений составляет 1,5 умножить на минимальный размер оплаты труда, умножить на 30%, прибавить 15%, умноженные на доход, уменьшенный на минимальный размер оплаты труда, умноженный на 1,5 рублей от фонда заработной платы.

Амортизация основных средств.

Средняя стоимость компьютера (ноутбука) составляет 69457,37 рублей. Норма амортизации 4% в мес.

Срок эксплуатации составляет 25 месяцев, значит, норма амортизации рассчитывается следующим образом: 100% разделить на 25 мес. (= 4%). Значит, амортизация за период разработки продукта составляет: 69457 рублей умножить на 4%, разделить на 30 дней и умножить на количество дней разработки.

Прочие расходы.

Прочие расходы в размере 5% от суммы предыдущих расходов.

Общая сумма затрат.

Общая сумма затрат складывается из суммы всех вышеперечисленных расходов.

Прибыль.

Экономический интерес любого предприятия заключается в получении прибыли, которая необходима для дальнейшего развития. В цену продукта заложим получение прибыли в размере 15% от общей суммы затрат.

Цена продукта.

В результате расчётов формируется цена продукта, которая складывается из общих затрат и прибыли.

Таким образом, в разделе 3 расчет экономической составляющей проекта показал, что полная себестоимость разработки шифратора «CRYPTOSFER» составляет 56 578,95 рублей.

# ЗАКЛЮЧЕНИЕ

Шифраторы являются ключевым звеном в обеспечении безопасности, передаче и хранении информации. В мире, где данные стали ценным активом, шифраторы защищают конфиденциальность, целостность и доступность этих данных от несанкционированного доступа и краж. Таким образом, шифраторы остаются актуальными, поскольку лежат в основе безопасной, эффективной и связанной цифровой среды.

В ходе работы был спроектирован, реализован и оценен с экономической точки зрения шифратор «CRYPTOSFER». Программа успешно сочетает в себе прикладные функции шифрования текста с помощью нескольких алгоритмов шифрования с элементами интерактивной игры для обучения.

Таким образом, все задачи по разработке шифратора выполнены в полном объёме. Цель работы – достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ **ИСТОЧНИКОВ**

I. Нормативно-правовые акты

1. Российская Федерация. Законы. О лицензировании отдельных видов деятельности : Федеральный закон № 99-ФЗ : [принят Государственной Думой 22 апреля 2011 года : одобрен Советом Федерации 27 апреля 2011 года]. – Текст : электронный // СПС «КонсультантПлюс» : [сайт] / ЗАО «КонсультантПлюс». – Ежедневное обновление. – URL: http://www.consultant.ru/document/.
2. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : [принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года]. – Текст : электронный // СПС «КонсультантПлюс» : [сайт] / ЗАО «КонсультантПлюс». – Ежедневное обновление. – URL: http://www.consultant.ru/document/cons\_doc\_LAW\_61798/.
3. Российская Федерация. Законы. О коммерческой тайне : Федеральный закон № 98-ФЗ : [принят Государственной Думой 9 июля 2004 года : одобрен Советом Федерации 15 июля 2004 года]. – Текст : электронный // СПС «КонсультантПлюс» : [сайт] / ЗАО «КонсультантПлюс». – Ежедневное обновление. – URL: http://www.consultant.ru/document/.
4. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем... : Постановление Правительства РФ от 16 апреля 2012 г. № 313. – Текст : электронный // СПС «КонсультантПлюс» : [сайт] / ЗАО «КонсультантПлюс». – Ежедневное обновление. – URL: http://www.consultant.ru/document/.
5. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке с использованием средств криптографической защиты информации : Приказ ФСБ России от 10 июля 2014 г. № 378. – Текст : электронный // СПС «КонсультантПлюс» : [сайт] / ЗАО «КонсультантПлюс». – Ежедневное обновление. – URL: http://www.consultant.ru/document/.
6. Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) : Приказ ФСБ России от 9 февраля 2005 г. № 66. – Текст : электронный // СПС «КонсультантПлюс» : [сайт] / ЗАО «КонсультантПлюс». – Ежедневное обновление. – URL: http://www.consultant.ru/document/.
7. Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну : Приказ ФАПСИ от 13 июня 2001 г. № 152. – Текст : электронный // СПС «КонсультантПлюс» : [сайт] / ЗАО «КонсультантПлюс». – Ежедневное обновление. – URL: http://www.consultant.ru/document/.
8. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования : межгосударственный стандарт : издание официальное : утверждён и введён в действие Постановлением Госстандарта СССР от 27.06.89 № 2182 : дата введения 1990-07-01. – Москва : Стандартинформ, 2007. – 21 с. – Текст : непосредственный.
9. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи : национальный стандарт Российской Федерации : издание официальное : утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2012 г. № 2151-ст : дата введения 2014-01-01. – Москва : Стандартинформ, 2013. – 54 с. – Текст : непосредственный.
10. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования : национальный стандарт Российской Федерации : издание официальное : утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2012 г. № 2150-ст : дата введения 2014-01-01. – Москва : Стандартинформ, 2013. – 16 с. – Текст : непосредственный.
11. ГОСТ Р 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры : национальный стандарт Российской Федерации : издание официальное : утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 7 декабря 2018 г. № 1143-ст : дата введения 2019-06-01. – Москва : Стандартинформ, 2019. – 38 с. – Текст : непосредственный.
12. ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров : межгосударственный стандарт : издание официальное : утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 5 декабря 2018 г. № 1096-ст : дата введения 2019-06-01. – Москва : Стандартинформ, 2019. – 24 с. – Текст : непосредственный.
13. Единая система программной документации (ЕСПД). Общие требования к программным документам : ГОСТ 19.XXX-XX : межгосударственный стандарт : издание официальное; введ. 1979-01-01. – Москва : ИПК Издательство стандартов, 2002. – 10 с. – Текст : непосредственный.

II. Основные источники

1. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/.
2. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2025. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/.

III. Интернет источники

1. Welcome to Python.org : [сайт]. – URL: https://www.python.org/.
2. Python — Википедия : [сайт]. – URL: https://ru.wikipedia.org/wiki/Python.
3. base64 — Base16, Base32, Base64, Base85 Data Encodings — документация Python : [сайт]. – URL: https://docs.python.org/3/library/base64.html.
4. MorseCodePy : [сайт]. – URL: https://pypi.org/project/MorseCodePy/.
5. Official Documentation And Tutorial | CustomTkinter : [сайт]. – URL: https://customtkinter.tomschimansky.com/.
6. byte operations (XOR) in python - Stack Overflow : [сайт]. – URL: https://stackoverflow.com/questions/29408173/byte-operations-xor-in-python.
7. PyInstaller Manual — PyInstaller 6.16.0 documentation : [сайт]. – URL: https://pyinstaller.org/en/stable/index.html.
8. VeraCrypt - Бесплатное надёжное шифрование дисков с открытым исходным кодом : [сайт]. – URL: https://veracrypt.io/ru/Home.html.
9. The GNU Privacy Guard : [сайт]. – URL: https://www.gnupg.org/.
10. Обзор BitLocker | Microsoft Learn : [сайт]. – URL: https://learn.microsoft.com/ru-ru/windows/security/operating-system-security/data-protection/bitlocker/.
11. Зарплаты в IT по всем IT-специализациям — Хабр Карьера : [сайт]. – URL: https://career.habr.com/salaries.