|  |
| --- |
| **МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ** |
| **ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»**  **(ФГБОУ ВО «МГУТУ ИМ. К.Г. РАЗУМОВСКОГО (ПКУ)»)** |
|  |
| **УНИВЕРСИТЕТСКИЙ КОЛЛЕДЖ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ** |

|  |
| --- |
| **КУРСОВОЙ ПРОЕКТ** |
|  |
| по междисциплинарному курсу: МДК.01.02. Технология разработки программного обеспечения |
|  |
| на тему: Разработка обучающей программы по теме «Криптография данных» |
|  |
| студентки группы 090203-9o-20/1  специальности 09.02.03 Программирование в компьютерных системах |
| Смирнова Константина Вадимовича |

|  |  |  |
| --- | --- | --- |
| Студент |  | К.В Смирнов |
| Руководитель курсового проекта |  | С.Ю. Кузьменко |
| Председатель ПЦК специальности 09.02.03 Программирование в компьютерных системах |  | А.И. Глускер |

|  |  |  |
| --- | --- | --- |
| Дата защиты «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2023 г. | | |
| Оценка:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Заведующий отделением № 1 |  | И.А. Миланова | |

Москва

2023

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 2](#_Toc146040566)

[1 ОБЩАЯ ЧАСТЬ 5](#_Toc146040567)

[1.1 Обзор и анализ предметной области 5](#_Toc146040568)

[1.2 Обзор существующих аналогов приложения 6](#_Toc146040569)

[1.3 Жизненный цикл базы данных 7](#_Toc146040570)

[1.4 Выбор и характеристика СУБД 8](#_Toc146040571)

[1.5 Выбор и характеристика среды разработки приложения 9](#_Toc146040572)

# ВВЕДЕНИЕ

Современность сложно представить без использования компьютеров и интернета. Информационные технологии развивались с середины прошлого века вплоть до сегодняшних дней. Распространение персональных компьютеров и смартфонов достигло того, что люди используют устройства не только во время работы, но и в обычной жизни для отдыха, развлечений, общения на расстоянии и обучения.

В следствие взаимодействия людей как с компьютерами, так и между собой по средству соцсетей, данные пользователей, которые используются приложениями, сохраняются в базах данных для дальнейшего использования. Но с ростом объема передаваемой информации возрастает угроза утечки или взлома.

В мире, где информация является одним из самых ценных ресурсов, шифрование данных становится все более актуальной темой. Криптография – это наука, которая занимается защитой информации путем шифрования и дешифрования. К методам криптографии относятся: обеспечение [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C), [целостности данных](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8), [аутентификации](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F), [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Криптография используется в сферах начиная от финансовых транзакций до военных коммуникаций.

Основная цель проекта - Разработка обучающей программы по теме «Криптография данных», представляющей из себя ознакомление с основными принципами криптографии данных, методами шифрования и дешифрования информации и приложение на основе переносной шифровальной машины «Эни́гма» (от [нем.](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BC%D0%B5%D1%86%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Änigma — загадка) для реализации данного материала.

В этапы разработки проекта входят:

* Анализ предметной области
* Выбор средств разработки
* Создание и заполнение базы данных
* Разработка приложения
* Разработка документации

В ходе анализа предметной области были изучены основные алгоритмы шифрования, такие как симметричное и асимметричное шифрование. Рассмотрены основные аспекты шифрования. Проведен обзор существующих программ по данной теме для реализации собственного приложения.

В результате прохождения обучения, в приложении можно будет получить знания и навыки, необходимые для защиты своих данных и данных клиентов. Это поможет повысить уровень безопасности бизнеса и укрепить доверие со стороны клиентов.

# ОБЩАЯ ЧАСТЬ

## Обзор и анализ предметной области

Обучающая программы по теме «Криптография данных» будет полезна для компаний, которые планируют начать обучение сотрудников/клиентов методам шифрования/дешифрования и их практической реализации. В связи с этим программа должна быть простой, интуитивно понятной, с актуальной логической моделью и базой данных для взаимодействия с пользователем.

База данных создаётся для хранения информации о теоретической части и для хранения данных о приложении в практической части. База данных должна содержать данные о ключах, методах шифрования/дешифрования алфавита.

В соответствии с предметной областью система строится с учётом следующих особенностей:

* Пользователи могут просматривать алфавит,
* Пользователи могут просматривать ключи шифрования/дешифрования,
* Пользователи могут просматривать результат шифрования/дешифрования,

Базовые сущности предметной области:

**Теория**. Атрибуты – идентификатор, текст, номер страницы

**Пользователи** – идентификатор, имя, пароль

**Энигма (приложение практической части)**. Атрибуты Энигмы – идентификатор, название, конфигурация роторов (ключа шифрования). Названия связаны с **Сообщениями.**

**Сообщения** – идентификатор, номер машины, текст сообщения для шифрования, зашифрованное сообщение

**Аудит** - таблица предназначена для отслеживания и регистрации действий, связанных с использованием машины Энигма, включая операции шифрования и дешифрования.

Идентификатор, номер пользователя, номер машины, тип операции, время выполнения операции

На основе имеющейсся информации можно сделать вывод, что программа предназначена для компаний, которые хотят обучить своих сотрудников или клиентов методам шифрования и дешифрования. Программа включает логическую модель и базу данных, которые содержат информацию о теоретических и практических аспектах криптографии, включая ключи и методы шифрования.

## Обзор существующих аналогов приложения

Возможности приложения определялись исходя из рассмотрения уже существующих вариантов.

Рассмотренные приложения:



Рисунок 1.1. Логотип сайта edX

1. edX: Introduction to Cryptography – курсы.

В функции входят курсы по криптографии данных.



Рисунок 1.2. Логотип сайта Codecademy

Codecademy – сайт.

интерактивный курс, который позволяет студентам изучать криптографию через практические упражнения и программирование.



Рисунок 1.3. Логотип приложения Crypto101

DataDex – Онлайн-Книга.

бесплатная книга доступна онлайн и предоставляет введение в современную криптографию, включая примеры кода



Рисунок 1.3. Логотип приложения Coursera

Coursera – Онлайн-курсы.

Несколько курсов, охватывающих основы криптографии и современные методы шифрования данных.

Анализ существующих систем показал, что основными функциями приложений в данной предметной области являются просмотр информации, манипулирование с ключами и алфавитом. Исходя из полученных данных, приложение будет разрабатываться с учётом перечисленных функций и дополнительных, отсутствующих в рассмотренных приложениях, сайтах, книгах.

Вывод: Программа будет сделана исходя из имеющихся аналогов, совмещая их положительные аспекты и собственные наработки.

## Жизненный цикл базы данных

Жизненный цикл базы данных состоит из шести этапов:

1. Предварительное планирование

На этом этапе были определены цели и задачи, которые база данных должна решать, а также ресурсы, которые необходимы для ее создания и поддержания.

1. Проверка осуществимости

На этом этапе была проведена оценка возможности создания базы данных с учетом ресурсов, которые будут задействованы.

1. Определение требований

На этом этапе был произведён сбор информации о том, какую информацию необходимо хранить в базе данных, как она будет использоваться, кто будет работать с базой данных и какие функции должна включать разрабатываемая система.

1. Концептуальное проектирование

На этом этапе были созданы основные модели данных, для организации информации в базе данных. Также были разработаны схемы, отношения между данными и функции, которые должна включать база данных.

1. Реализация

На этом этапе было произведено создание структуры базы данных, написание кода для реализации функций, создание пользовательского интерфейса и тестирование системы.

1. Оценка работы и поддержка базы данных.

На этом этапе была произведена оценка работы базы данных, были выявлены проблемы и их решение. Этот этап также включает в себя поддержание базы данных в актуальном состоянии и обучение пользователей ее использованию.

1. На основе вышеперечисленного можно сделать вывод, что Жизненный цикл базы данных состоит из шести этапов: Предварительное планирование, Проверка осуществимости, Определение требований, Концептуальное проектирование, Реализация, Оценка работы и поддержка базы данных.

Выбор и характеристика СУБД

Для разработки информационной системы применялась концепция клиент-серверного взаимодействия, которая предусматривает существование серверов и клиентов, использующих определенные сервисы.

Архитектура клиент-сервер была выбрана потому, что клиенты и серверы могут работать на разных компьютерах в сети, что позволяет распределять нагрузку и обеспечивать более высокую доступность и производительность приложений.

Клиент-серверная архитектура позволяет масштабировать приложения по мере необходимости, добавляя дополнительные серверы или клиенты.

Разделение приложения на клиентскую и серверную части позволяет изменять или обновлять каждую часть независимо от другой.

Серверная часть приложения может обеспечивать более высокий уровень безопасности с помощью механизмов аутентификации, авторизации и шифрования данных.

Клиент-серверная архитектура позволяет централизованно управлять хранилищами данных, приложениями и доступом к ним.

Клиент-серверная архитектура позволяет оптимизировать производительность приложения, разделяя задачи между клиентом и сервером.

Клиент-серверная архитектура обеспечивает возможность добавления новых функций и модулей без необходимости изменения всего приложения.

Для реализации клиент-серверной архитектуры была выбрана СУБД MS SQL Server, предоставляющая бесплатный доступ. Также ПО MS SQL Server Management Studio для работы с MS SQL Server упрощает разработку, предоставляющий удобный интерфейс и встроенный компилятор для кода на SQL языке.

Вывод: для разработки программы выбрана концепция клиент-серверного взаимодействия. Для реализации клиент-серверной архитектуры была выбрана СУБД MS SQL Server

Выбор и характеристика среды разработки приложения

Для создания приложения была применена технология C# WPF Entity Framework, Предоставляет возможность взаимодействия с объектами как посредством [LINQ](https://ru.wikipedia.org/wiki/LINQ) в виде LINQ to Entities, так и с использованием Entity SQL. озволяющая строить многоуровневые приложения, реализуя один из шаблонов проектирования [MVC](https://ru.wikipedia.org/wiki/Model-View-Controller), [MVP](https://ru.wikipedia.org/wiki/Model-View-Presenter) или [MVVM](https://ru.wikipedia.org/wiki/Model-View-ViewModel).

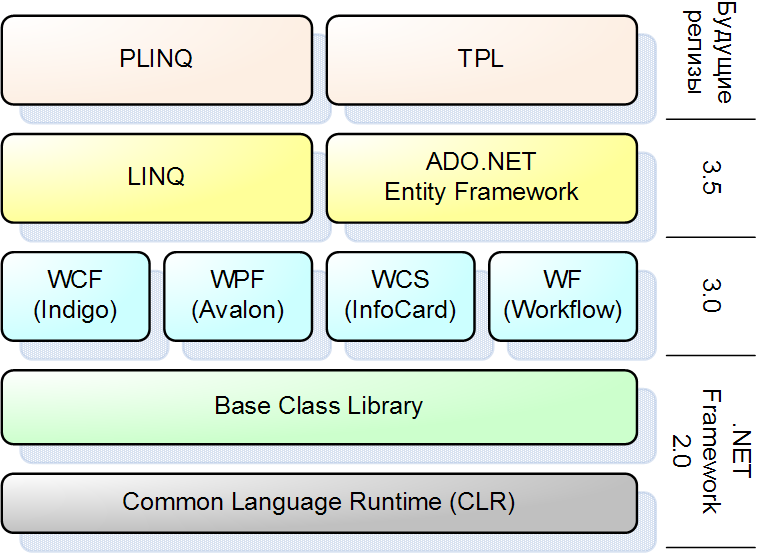


Рисунок 1.4. Схема работы Entity Framework

Плюсами ADO.NET являются:

1. Основной нужный функционал включен в ядро .NET Framework
2. Простота в использовании, для работы достаточно хорошо знать SQL язык
3. Стабильность и быстрота работы

Минусами ADO.NET являются:

1. Неудобство работы с объектами
2. Много повторяющихся блоков кода
3. Необходимость написания SQL-запросов

Entity Framework - инструмент ORM (Object-Relational Mapping), позволяющий взаимодействовать с базами данных, используя объектно-ориентированный подход.

Плюсами Entity Framework являются:

1. Простота в использовании и повышение уровня абстракции
2. Генерация SQL-запросов: EF автоматически генерирует SQL-запросы на основе LINQ-запросов, что уменьшает вероятность ошибок и повышает производительность. Минусами Entity Framework являются:

Минусы Entity Framework:

В некоторых случаях, при работе с большими объемами данных, Entity Framework может быть не так быстрым, как написание хранимых процедур или ручное написание SQL-запросов.

Исходя из вышеперечисленного, выбор был сделан в пользу Entity Framework.

В качестве среды разработки была выбрана Microsoft Visual Studio, так как она предоставляет множество удобств для разработчика:

* 1. Понятный интерфейс. Интерфейс Visual Studio был разработан, чтобы сделать работу программиста простой и удобной. Все инструменты и функции легко доступны благодаря простой структуре меню и панелей инструментов.
  2. Visual Studio содержит все необходимые инструменты и функции, такие как редактор кода, отладчик, компилятор и многие другие.
  3. Visual Studio имеет мощный отладчик, который позволяет находить и исправлять ошибки в коде. Он также поддерживает множество отладочных функций, таких как точки остановок, просмотр переменных и значения, трассировка стека вызовов и др.

Исходя из текста выше следует вывод:

Для создания приложения была применена технология C# WPF Entity Framework, а средой разработки - Microsoft Visual Studio.