**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кафедра \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Допустить к защите*

Заведующий кафедрой

\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(подпись)*  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(тема ВКР)*

Направление/специальность подготовки

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(код и наименование направления/специальности)*

Направленность (профиль)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(наименование)*

Квалификация \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(наименование квалификации в соответствии с ФГОС ВО)*

Студент:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Научный руководитель:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_

*(учёная степень, учёное звание, Ф.И.О.)(подпись)*

Санкт-Петербург, 20\_\_

*Оборотная сторона титульного листа*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*работа написана мною самостоятельно*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*работа не содержит неправомерных заимствований*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*работа может быть размещена в электронно-библиотечной системе университета*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(дата) (подпись) (ФИО студента)*

Текст ВКР размещен в электронно-библиотечной системе университета.

Руководитель отдела комплектования библиотеки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(Ф.И.О.)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(дата) (подпись)*

Коэффициент оригинальности ВКР \_\_\_\_\_\_\_\_ % .

Проверил: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(Должность, Ф.И.О.)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(дата) (подпись)*

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Кафедра\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Направление (специальность) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(код и наименование)

**Утверждаю:**

Зав. кафедрой\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О., подпись)

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г.

**ЗАДАНИЕ**

**на выполнение выпускной квалификационной работы (ВКР)**

1. Студент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № группы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество)

2. Руководитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество, должность, уч. степень и звание)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Квалификация\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование в соответствии с ФГОС ВО)

4. Тема ВКР \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_утверждена приказом ректора университета от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_\_\_\_\_\_

5. Исходные данные (технические требования):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Содержание работы (анализ состояния проблемы, проведение исследований, разработка, расчеты параметров, экономическое обоснование и др.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Вид отчетных материалов, представляемых в ГЭК (пояснительная записка, перечень, графического материала, отчет о НИР, технический проект, образцы и др.): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Консультанты по ВКР с указанием относящихся к ним разделов

|  |  |  |  |
| --- | --- | --- | --- |
| Раздел | Консультант | Подпись дата | |
| Задание  выдал | Задание  принял |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |

Дата выдачи задания «\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

Дата представления ВКР к защите «\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

*Руководитель* *ВКР\_*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

*Студент*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

Оглавление

[ВВЕДЕНИЕ 8](#_Toc135483321)

[1 ОБЗОР ЛИТЕРАТУРЫ 9](#_Toc135483322)

[1.1 Современные тенденции в использовании мгновенных сообщений в коммерческих организациях 9](#_Toc135483323)

[1.2 Основные угрозы безопасности при обмене мгновенными сообщениями 11](#_Toc135483324)

[1.3 Анализ существующих платформ мгновенного обмена сообщениями и их уязвимостей 13](#_Toc135483325)

[1.4 Основные подходы к защите информации в мгновенных сообщениях 15](#_Toc135483326)

[2 ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ К ЗАЩИЩЕННОЙ ПЛАТФОРМЕ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ ДЛЯ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ 17](#_Toc135483327)

[2.1 Определение потребностей и требований организации к платформе 17](#_Toc135483328)

[2.2 Формулирование функциональных и нефункциональных требований к платформе 19](#_Toc135483329)

[2.3 Разработка требований к уровню защиты информации на платформе 21](#_Toc135483330)

[3 РАЗРАБОТКА АРХИТЕКТУРЫ ПЛАТФОРМЫ ЗАЩИЩЕННОГО ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ 24](#_Toc135483331)

[3.1 Определение основных модулей и компонентов платформы 24](#_Toc135483332)

[3.2 Разработка архитектуры системы, учитывающей требования к безопасности 25](#_Toc135483333)

[3.3 Описание протоколов и механизмов защиты информации на платформе 25](#_Toc135483334)

[4 РЕАЛИЗАЦИЯ ПЛАТФОРМЫ ЗАЩИЩЕННОГО ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ 26](#_Toc135483335)

[4.1 Выбор технологического стека и инструментов разработки 26](#_Toc135483336)

[4.2 Модельные представления объекта разработки 30](#_Toc135483337)

[**4.2.1** **IDEF0 диаграмма** 30](#_Toc135483338)

[4.3 Разработка программного обеспечения для платформы 38](#_Toc135483339)

[4.4 Тестирование и отладка платформы 38](#_Toc135483340)

[5 АНАЛИЗ БЕЗОПАСНОСТИ И ЭФФЕКТИВНОСТИ ПЛАТФОРМЫ ЗАЩИЩЕННОГО ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ 39](#_Toc135483341)

[5.1 Проведение тестирования на безопасность и оценка соответствия требованиям к защите информации 39](#_Toc135483342)

[5.2 Оценка эффективности платформы с точки зрения использования организацией 39](#_Toc135483343)

[5.3 Сравнение разработанной платформы с существующими аналогами 39](#_Toc135483344)

[6 ЗАКЛЮЧЕНИЕ 39](#_Toc135483345)

[6.1 Основные результаты исследования 39](#_Toc135483346)

[6.2 Выводы и рекомендации по дальнейшей разработке и использованию платформы 39](#_Toc135483347)

[6.3 Ограничения и ограничивающие факторы 39](#_Toc135483348)

[6.4 Направления дальнейших исследований в области защищенного обмена мгновенными сообщениями 40](#_Toc135483349)

[7 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 41](#_Toc135483350)

[8 ПРИЛОЖЕНИЕ 41](#_Toc135483351)

ВВЕДЕНИЕ

В настоящее время мгновенные сообщения стали неотъемлемой частью коммуникации в коммерческих организациях. Они используются для обмена информацией между сотрудниками, партнерами и клиентами, что значительно ускоряет процессы коммуникации и повышает эффективность работы.

Однако при использовании мгновенных сообщений возникают проблемы безопасности, связанные с возможностью несанкционированного доступа к информации, передачей конфиденциальных данных, угрозой вредоносного кода и многими другими рисками.

**Цель:** разработка платформы защищенного обмена мгновенными сообщениями для коммерческой организации.

**Задачи:**

* Обзор литературы по современным тенденциям в использовании мгновенных сообщений в коммерческих организациях, анализ существующих платформ мгновенного обмена сообщениями и их уязвимостей.
* Определение требований к платформе защищенного обмена мгновенными сообщениями на основе результатов обзора литературы и анализа существующих платформ.
* Разработка архитектуры платформы защищенного обмена мгновенными сообщениями, удовлетворяющей определенным требованиям.
* Реализация программного обеспечения для платформы защищенного обмена мгновенными сообщениями на основе разработанной архитектуры.
* Проведение анализа безопасности и эффективности разработанной платформы, оценка ее соответствия требованиям безопасности и эффективности использования в коммерческой организации.

Ожидаемым результатом данной работы будет создание защищенной платформы мгновенного обмена сообщениями, соответствующей требованиям безопасности и функциональности для использования в коммерческой организации.

# ОБЗОР ЛИТЕРАТУРЫ

## Современные тенденции в использовании мгновенных сообщений в коммерческих организациях

В настоящее время, использование мгновенных сообщений становится все более популярным средством коммуникации между компаниями и их клиентами, а также внутри самой компании. Это связано с рядом преимуществ, таких как быстрая доставка сообщений, возможность обмена мультимедийными файлами и удобство использования на мобильных устройствах.

Ниже приведены некоторые из современных тенденций в использовании мгновенных сообщений в коммерческих организациях:

1. Использование чат-ботов для автоматизации обслуживания клиентов

Компании начинают использовать чат-ботов для автоматизации обслуживания клиентов через мгновенные сообщения. Чат-боты могут быстро и эффективно отвечать на вопросы клиентов, помогать им сделать заказы и решать проблемы без необходимости связываться с оператором контакт-центра. Это позволяет сократить расходы на обслуживание клиентов и улучшить качество обслуживания.

1. Использование мгновенных сообщений для внутренней коммуникации

Компании также начинают использовать мгновенные сообщения для внутренней коммуникации. Это позволяет улучшить коммуникацию между сотрудниками, сократить время на решение проблем и повысить эффективность работы. Кроме того, мгновенные сообщения могут быть использованы для проведения внутренних опросов, что позволяет получить мнение сотрудников по различным вопросам.

1. Использование мгновенных сообщений для продаж и маркетинга

Многие компании начинают использовать мгновенные сообщения для продаж и маркетинга. Они могут использовать мгновенные сообщения для отправки рекламных сообщений, уведомлений о распродажах и специальных предложений, а также для отправки купонов и промо-кодов. Это помогает увеличить количество продаж и улучшить отношения с клиентами.

1. Использование мгновенных сообщений для улучшения сервиса и удовлетворенности клиентов

Многие компании начинают использовать мгновенные сообщения для улучшения сервиса и удовлетворенности клиентов. Они могут использовать мгновенные сообщения для получения обратной связи от клиентов, а также для решения возникших проблем и вопросов быстро и эффективно. Кроме того, мгновенные сообщения могут использоваться для уведомления клиентов о статусе их заказов или доставки товаров.

1. Использование мгновенных сообщений для развития бизнеса

Мгновенные сообщения могут использоваться для развития бизнеса, например, для общения с потенциальными партнерами или клиентами, проведения онлайн-конференций и вебинаров, а также для организации встреч и совещаний. Это позволяет расширить сферу бизнеса и увеличить его прибыльность.

Однако, использование мгновенных сообщений также сопряжено с рядом угроз безопасности, которые необходимо учитывать при использовании данного средства коммуникации. В дипломной работе будут рассмотрены эти угрозы и способы их минимизации, чтобы компании могли использовать мгновенные сообщения безопасно и эффективно.

Начало формы

Конец формы

## Основные угрозы безопасности при обмене мгновенными сообщениями

В этом разделе мы рассмотрим основные угрозы безопасности, связанные с обменом мгновенными сообщениями.

Перехват сообщений

Перехват сообщений является одной из наиболее распространенных угроз при обмене мгновенными сообщениями. Конфиденциальные данные, такие как пароли, личные данные, банковские данные и т.д. могут быть перехвачены злоумышленниками, если сообщения не защищены надлежащим образом. Например, если сообщения передаются по нешифрованным каналам связи, злоумышленник может перехватить сообщения и получить доступ к конфиденциальной информации.

Вредоносное ПО

Вредоносное ПО - это программа, которая может быть установлена на устройстве пользователя без его ведома и использоваться для перехвата сообщений и другой конфиденциальной информации. Некоторые платформы обмена мгновенными сообщениями могут быть более подвержены атакам вредоносного ПО, чем другие. Например, приложения, которые не имеют механизмов защиты от вредоносных атак, могут стать уязвимыми.

Социальная инженерия

Социальная инженерия - это метод атаки, который использует психологические методы воздействия на пользователя для получения доступа к конфиденциальной информации. Некоторые злоумышленники могут использовать социальную инженерию для получения доступа к аккаунтам обмена мгновенными сообщениями. Например, злоумышленник может отправить пользователю ложное сообщение, попросив его предоставить свои учетные данные для решения вымышленной проблемы.

Фишинг-атаки

Фишинг-атаки - это тип атаки, при котором злоумышленник пытается получить доступ к конфиденциальной информации путем отправки ложных сообщений, которые кажутся легитимными. Например, злоумышленник может отправить сообщение, которое выглядит так, как будто оно было отправлено от банка, с просьбой предоставить учетные данные для проверки или обновления аккаунта. Если пользователь предоставляет свои данные, они могут быть использованы злоумышленником для доступа к аккаунту и получения конфиденциальной информации.

Несанкционированный доступ к устройству

Несанкционированный доступ к устройству, на котором выполняется обмен мгновенными сообщениями, также может представлять угрозу безопасности. Если злоумышленник получит физический доступ к устройству, он может получить доступ к конфиденциальной информации, сохраненной в приложениях обмена мгновенными сообщениями. Кроме того, если устройство не защищено паролем, злоумышленник может получить доступ к приложениям без предварительной авторизации.

Для защиты конфиденциальности и безопасности пользователей при обмене мгновенными сообщениями необходимо принимать меры предосторожности. Важно использовать приложения, которые имеют механизмы защиты от вредоносных атак и шифруют сообщения. Кроме того, пользователи должны быть внимательны при общении в мессенджерах и не разглашать конфиденциальную информацию. Наконец, устройства должны быть защищены паролем и физически защищены от несанкционированного доступа.

## Анализ существующих платформ мгновенного обмена сообщениями и их уязвимостей

При разработке собственного мессенджера необходимо проанализировать существующие платформы мгновенного обмена сообщениями и выявить их уязвимости, чтобы учесть их при проектировании своего продукта.

Одна из самых популярных платформ мгновенного обмена сообщениями является WhatsApp. Несмотря на то, что этот мессенджер использует шифрование end-to-end, были обнаружены уязвимости в его защите. Например, в 2019 году была обнаружена уязвимость, которая позволяла злоумышленникам установить вредоносное ПО на устройствах пользователей, даже если они не совершали никаких действий.

Еще одной популярной платформой мгновенного обмена сообщениями является Telegram. В отличие от WhatsApp, Telegram использует протокол MTProto для шифрования сообщений, который не подвергался такому широкому аудиту, как, например, протокол Signal. Тем не менее, Telegram не является полностью безопасной платформой, и у него есть свои уязвимости. Например, в 2019 году была обнаружена уязвимость, которая позволяла злоумышленникам получить доступ к сообщениям пользователей, используя атаку типа "человек по середине".

Протокол Signal является одним из самых безопасных протоколов мгновенного обмена сообщениями. Signal использует шифрование end-to-end и открытый исходный код, что позволяет специалистам по безопасности проанализировать его на уязвимости. Тем не менее, у Signal также есть свои недостатки, такие как отсутствие возможности отправки сообщений с большими файлами.

Помимо перечисленных выше платформ, существуют и другие мессенджеры, такие как Viber, Facebook Messenger, Skype и другие. Каждый из них имеет свои особенности и уязвимости.

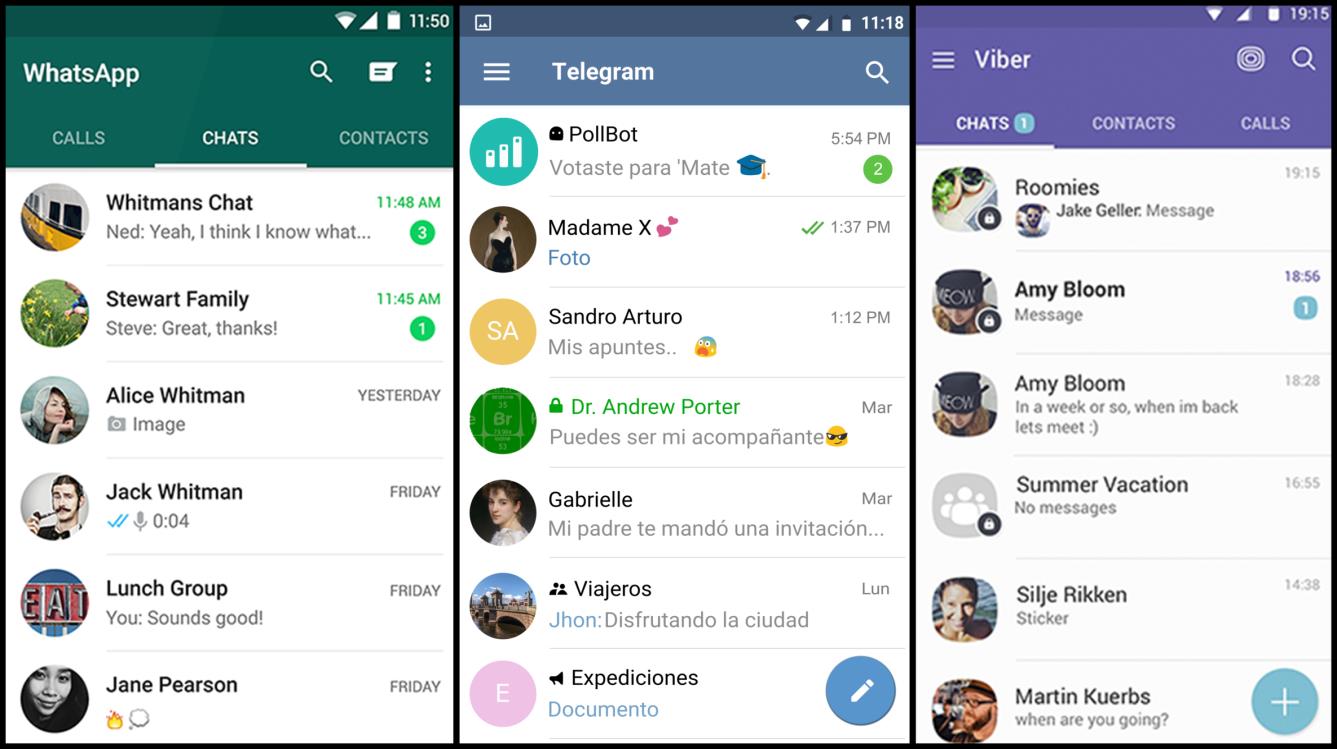


Рис. 1. Пользовательский интерфейс WhatsApp, Telegram, Viber для платформы Android

При разработке своей собственной платформы мгновенного обмена сообщениями необходимо учитывать уязвимости, выявленные в существующих платформах, и принимать меры для обеспечения максимальной защиты пользователей.

## Основные подходы к защите информации в мгновенных сообщениях

При использовании мгновенных сообщений возникает ряд проблем с защитой информации, таких как утечки данных, хакерские атаки и другие угрозы. Чтобы обеспечить безопасность и защиту информации в мгновенных сообщениях, существуют различные подходы и методы.

Основные подходы к защите информации в мгновенных сообщениях включают следующее:

1. Шифрование сообщений

Шифрование сообщений - это метод защиты информации, который заключается в преобразовании сообщения в зашифрованный вид с помощью специальных алгоритмов. Такой подход позволяет обеспечить конфиденциальность передачи сообщений, т.е. только получатель может расшифровать сообщение. Для реализации шифрования сообщений можно использовать различные алгоритмы, такие как AES, RSA и др.

1. Аутентификация и авторизация пользователей

Аутентификация и авторизация пользователей - это методы, которые позволяют определить легитимность пользователей и их доступ к ресурсам. Эти методы могут быть использованы для предотвращения несанкционированного доступа к мгновенным сообщениям и другим конфиденциальным данным. Для аутентификации и авторизации пользователей могут использоваться различные методы, такие как пароли, биометрические данные и т.д.

1. Проверка на вредоносное ПО

Проверка на вредоносное ПО - это метод, который позволяет обнаруживать и предотвращать атаки на мгновенные сообщения и другие системы. Для этого используются специальные антивирусные программы, которые могут сканировать сообщения на наличие вирусов и других вредоносных программ. Это помогает предотвратить атаки на мгновенные сообщения и защитить данные пользователей.

1. Проверка на уязвимости

Проверка на уязвимости - это метод, который позволяет обнаруживать уязвимости в системе и устранять их до того, как они будут использованы злоумышленниками. Для этого проводится анализ системы на наличие уязвимостей и применяются соответствующие меры по их устранению. Это помогает увеличить уровень безопасности мгновенных сообщений и защитить данные пользователей.

# ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ К ЗАЩИЩЕННОЙ ПЛАТФОРМЕ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ ДЛЯ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

## Определение потребностей и требований организации к платформе

Первая потребность, которую необходимо учитывать, это конфиденциальность передачи сообщений. Организации могут иметь конфиденциальную информацию, которую необходимо защитить от несанкционированного доступа. Платформа для защищенного обмена мгновенными сообщениями должна обеспечивать шифрование сообщений, чтобы защитить конфиденциальную информацию.

Вторая потребность - безопасность передачи сообщений. Организации могут столкнуться с различными угрозами безопасности, такими как вирусы, хакерские атаки и другие виды вредоносных действий. Платформа для защищенного обмена мгновенными сообщениями должна обеспечивать высокий уровень защиты от таких угроз.

Третья потребность - гибкость. Платформа должна быть гибкой и настраиваемой, чтобы она могла быть адаптирована к специфическим потребностям организации. Например, возможность настройки прав доступа пользователей, групповая работа и другие функции могут быть необходимы в зависимости от потребностей организации.

Четвертая потребность - доступность. Платформа должна быть доступна для использования с любого устройства и в любом месте, где есть доступ к Интернету. Это позволит сотрудникам организации обмениваться сообщениями в любое время и из любой точки мира.

Пятая потребность - удобство использования. Платформа должна быть удобной в использовании и иметь простой интерфейс, который не требует специальной подготовки. Это поможет упростить работу.

Кроме того, при выборе платформы для защищенного обмена мгновенными сообщениями, организации должны учитывать и требования, связанные с техническими характеристиками платформы. Она должна иметь высокую скорость передачи данных, высокую производительность, чтобы обеспечить быструю обработку большого объема данных, и высокую надежность, чтобы гарантировать доступность платформы в любое время.

Также важно, чтобы платформа была совместима с другими программными продуктами, которые используются в организации. Например, если организация использует программное обеспечение для управления проектами, то платформа для защищенного обмена сообщениями должна быть совместима с этим программным обеспечением, чтобы обеспечить эффективную коммуникацию между участниками проекта.

Еще одним важным требованием является возможность интеграции платформы с другими системами безопасности, такими как системы контроля доступа и мониторинга сети. Это позволит организации обеспечить комплексную безопасность своих данных и максимально защитить их от угроз.

При выборе платформы для защищенного обмена мгновенными сообщениями, организации также должны учитывать вопросы стоимости и доступности поддержки. Платформа должна быть доступна по разумной цене, чтобы организации могли себе позволить ее использовать, и должна иметь высококачественную техническую поддержку, чтобы гарантировать бесперебойную работу платформы и быстрое реагирование на возникающие проблемы.

Таким образом, выбор платформы для защищенного обмена мгновенными сообщениями является критически важным для организаций, которые имеют дело с конфиденциальной информацией. При выборе платформы необходимо учитывать множество факторов, включая конфиденциальность, безопасность, гибкость, доступность, удобство использования и технические характеристики.

## Формулирование функциональных и нефункциональных требований к платформе

Одним из ключевых шагов при разработке платформы защищенного обмена мгновенными сообщениями является определение функциональных и нефункциональных требований. Функциональные требования определяют, какие функции должна выполнять платформа, а нефункциональные требования определяют, каким образом эти функции должны быть реализованы.

Ниже приведены функциональные и нефункциональные требования к платформе защищенного обмена мгновенными сообщениями.

Функциональные требования:

1. Регистрация пользователей: платформа должна предоставлять возможность регистрации новых пользователей и хранить информацию об аккаунтах пользователей.
2. Отправка сообщений: платформа должна позволять пользователям отправлять мгновенные сообщения другим пользователям.
3. Шифрование сообщений: платформа должна обеспечивать шифрование всех сообщений, передаваемых через систему, чтобы обеспечить конфиденциальность и целостность передаваемой информации.
4. Управление контактами: платформа должна предоставлять функциональность управления контактами, чтобы пользователи могли добавлять, удалять и изменять информацию о своих контактах.
5. Управление группами: платформа должна предоставлять возможность создания групповых чатов и управления членами групп.
6. Уведомления: платформа должна предоставлять уведомления о получении новых сообщений и других важных событий, связанных с пользовательским аккаунтом.
7. Интеграция с другими приложениями: платформа должна позволять интеграцию с другими приложениями, такими как электронная почта, календарь и другие инструменты, используемые в рабочих процессах организации.

Нефункциональные требования:

1. Безопасность: платформа должна обеспечивать высокий уровень безопасности и защиты от внешних угроз, таких как хакерские атаки, вирусы и другие виды вредоносных действий.
2. Доступность: платформа должна быть доступна для использования в любое время и из любой точки мира, где есть доступ к Интернету.
3. Надежность: платформа должна быть надежной и стабильной, чтобы пользователи могли полагаться на ее работу в любое время.
4. Производительность: платформа должна иметь высокую производительность и быстро обрабатывать запросы пользователей, даже при большом количестве активных пользователей.
5. Масштабируемость: платформа должна быть масштабируемой и способной поддерживать большое количество пользователей и сообщений без существенного ухудшения производительности.
6. Совместимость: платформа должна быть совместима с различными устройствами и операционными системами, используемыми пользователями. Удобство использования: платформа должна быть легкой в использовании и иметь простой и понятный интерфейс для пользователей всех уровней технической грамотности.
7. Поддержка: платформа должна предоставлять круглосуточную техническую поддержку для пользователей, чтобы решать возникающие проблемы и отвечать на вопросы.
8. Соответствие требованиям законодательства: платформа должна соответствовать требованиям законодательства, регулирующего обмен информацией, а также обеспечивать соблюдение приватности и конфиденциальности пользовательских данных.

В целом, функциональные и нефункциональные требования к платформе защищенного обмена мгновенными сообщениями должны быть четко определены и учитывать потребности пользователей, а также требования безопасности и надежности системы.

## Разработка требований к уровню защиты информации на платформе

Одним из ключевых аспектов разработки требований к уровню защиты информации на платформе является определение уровня угроз и уязвимостей, которые могут возникнуть в процессе использования платформы. На этом этапе необходимо проанализировать все возможные угрозы, которые могут поставить под угрозу конфиденциальность, целостность и доступность информации на платформе.

Важно учитывать, что угрозы могут появляться не только из-за внешних факторов, таких как кибератаки или вирусы, но и из-за внутренних проблем, таких как ошибки в программном обеспечении или неправильные настройки безопасности.

После анализа угроз и уязвимостей необходимо определить требования к уровню защиты информации, которые должна обеспечивать платформа. Эти требования могут включать в себя следующее:

1. Контроль доступа: платформа должна обеспечивать строгий контроль доступа, чтобы только авторизованные пользователи имели доступ к конфиденциальной информации. Это может включать в себя механизмы аутентификации, авторизации и управления доступом.
2. Шифрование данных: платформа должна обеспечивать шифрование всех данных, которые передаются через систему, чтобы обеспечить конфиденциальность и целостность информации. Шифрование может включать в себя различные методы, такие как шифрование на уровне приложения или шифрование на уровне сети.
3. Резервное копирование: платформа должна обеспечивать резервное копирование данных, чтобы обеспечить доступность информации в случае непредвиденных сбоев или катастрофических событий.
4. Мониторинг и аудит: платформа должна обеспечивать мониторинг и аудит всех действий пользователей, чтобы обеспечить защиту от внутренних угроз и выявлять любые несанкционированные действия.
5. Обновление и патчи: платформа должна регулярно обновляться и устанавливать необходимые патчи, чтобы защитить от новых угроз и уязвимостей.
6. Физическая защита: платформа должна быть защищена физически, чтобы предотвращать несанкционированный доступ к серверам и оборудованию, которые обеспечивают работу платформы.
7. Разграничение доступа: платформа должна обеспечивать разграничение доступа между различными пользователями и ролями, чтобы минимизировать риски от внутренних угроз.
8. Защита от DDoS-атак: платформа должна быть защищена от DDoS-атак, чтобы обеспечить доступность информации и предотвратить отказ в обслуживании.
9. Соблюдение нормативных требований: платформа должна соответствовать всем применимым нормативным требованиям и стандартам безопасности, таким как GDPR, HIPAA и т.д.
10. Обучение и обеспечение безопасности пользователей: платформа должна предоставлять обучение и обеспечение безопасности для пользователей, чтобы минимизировать риски от внутренних угроз и несанкционированного доступа.

После того, как были определены требования к уровню защиты информации, необходимо разработать соответствующие меры безопасности и процедуры для обеспечения их выполнения. Это может включать в себя регулярное обновление программного обеспечения, резервное копирование данных, мониторинг и аудит действий пользователей, управление ролями и доступом, а также обучение и обеспечение безопасности пользователей.

Для обеспечения эффективной защиты информации на платформе необходимо учитывать, что безопасность является процессом, а не одноразовым мероприятием. Поэтому, необходимо регулярно анализировать угрозы и уязвимости, обновлять меры безопасности и процедуры, и обеспечивать обучение и обеспечение безопасности для пользователей.

# РАЗРАБОТКА АРХИТЕКТУРЫ ПЛАТФОРМЫ ЗАЩИЩЕННОГО ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ

## Определение основных модулей и компонентов платформы

Ниже представлен структурированный перечень основных модулей и компонентов платформы защищенного обмена мгновенными сообщениями для коммерческой организации. Каждый модуль состоит из набора компонентов, которые взаимодействуют между собой для обеспечения надежной и безопасной работы платформы:

Первым модулем является серверная часть, которая обеспечивает обработку и хранение сообщений. Она состоит из базы данных, сервера приложений и систем безопасности. База данных хранит все сообщения и данные пользователей, сервер приложений обеспечивает обработку запросов и управление работой всех компонентов серверной части, а системы безопасности контролируют доступ, шифруют данные и мониторят активность пользователей.

Второй модуль - клиентская часть, которая представляет собой набор приложений и интерфейсов, используемых пользователями для общения и работы с платформой. Она может включать в себя мобильное приложение, веб-интерфейс и клиент для ПК.

Третий модуль - дополнительные компоненты, которые могут включать в себя интеграцию с другими приложениями, API и системы аналитики. Их наличие зависит от потребностей конкретной коммерческой организации.

Четвертый модуль - модуль управления сообщениями, отвечающий за обработку и хранение сообщений, а также управление их доступом. Он может включать в себя базу данных сообщений, механизмы поиска и фильтрации сообщений, а также механизмы управления правами доступа к сообщениям.

Пятый модуль - модуль уведомлений и оповещений, отвечающий за механизмы уведомления пользователей о новых сообщениях, событиях и изменениях на платформе. Он может включать в себя электронную почту, SMS-уведомления, пуш-уведомления и другие средства коммуникации.

Шестой модуль - модуль управления архивом сообщений, отвечающий за хранение старых сообщений и возможность их поиска и извлечения при необходимости. Он может включать в себя системы архивации сообщений, механизмы резервного копирования данных и механизмы управления жизненным циклом сообщений

Все эти модули и компоненты платформы защищенного обмена мгновенными сообщениями должны работать в интеграции друг с другом, обеспечивая надежную и безопасную работу платформы и защиту конфиденциальности и целостности информации.

## Разработка архитектуры системы, учитывающей требования к безопасности

## Описание протоколов и механизмов защиты информации на платформе

Существует множество протоколов и механизмов, которые могут обеспечить безопасность обмена сообщениями в коммерческой организации. Один из таких протоколов - SSL/TLS, который используется для шифрования трафика и обеспечения аутентификации сервера. Это достигается путем использования цифровых сертификатов, которые подтверждают легитимность сервера.

Другим протоколом, который может быть использован для обеспечения безопасности сообщений, является S/MIME. Этот протокол использует асимметричное шифрование, чтобы зашифровать сообщения, и электронную подпись, чтобы обеспечить аутентификацию отправителя. Это делает невозможным подделку сообщений или подмену отправителя.

Для защиты от атак типа "человек посередине" (Man-in-the-Middle), может использоваться протокол IPsec, который создает зашифрованный туннель для обмена сообщениями. Это гарантирует, что только конечные узлы могут прочитать сообщения, а злоумышленники не смогут перехватывать их по пути.

Кроме того, существует ряд механизмов, которые можно использовать для обеспечения безопасности на платформе обмена сообщениями. Например, может быть введена политика сильных паролей, которая потребует от пользователей использовать сложные пароли и периодически их менять. Также можно использовать механизмы многофакторной аутентификации, такие как SMS-коды или аутентификация по отпечатку пальца, чтобы обеспечить дополнительный уровень защиты.

Наконец, можно использовать систему мониторинга, которая будет отслеживать необычную активность на платформе, такую как неудачные попытки входа, необычный трафик или подозрительные действия пользователей. Это поможет быстро выявлять и реагировать на потенциальные угрозы безопасности.

# РЕАЛИЗАЦИЯ ПЛАТФОРМЫ ЗАЩИЩЕННОГО ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ

## Выбор технологического стека и инструментов разработки

HTML (Hypertext Markup Language) и CSS (Cascading Style Sheets) являются стандартными языками разметки и стилей для веб-страниц. Они позволяют разработчикам создавать красивые и удобные интерфейсы для пользователей.HTML используется для создания структуры веб-страниц, определяя содержание страницы, такое как текст, изображения, ссылки и другие элементы.

CSS используется для определения визуального стиля веб-страниц, таких как цвета, шрифты, размеры и расположение элементов. Использование HTML и CSS для разработки мессенджера позволяет создавать красивый и удобный пользовательский интерфейс, что важно для успешной работы приложения. Кроме того, HTML и CSS являются широко распространенными и хорошо поддерживаемыми технологиями, что обеспечивает стабильность и надежность разработанного приложения.

Использование фреймворка Vue.js и связанных с ним библиотек (Vuex, Vue Router, Axios) имеет ряд преимуществ для разработки мессенджера. Во-первых, Vue.js обладает высокой производительностью и быстрым откликом на пользовательские действия. Это особенно важно для мессенджеров, которые работают в режиме реального времени и требуют мгновенного обновления интерфейса при появлении новых сообщений. Во-вторых, Vuex позволяет управлять состоянием приложения и обеспечивает однонаправленный поток данных. Это облегчает разработку и поддержку приложения, так как упрощает отслеживание изменений состояния и их влияния на другие части приложения. Vue Router предоставляет возможность создания навигации в приложении и обеспечивает удобный механизм для перехода между страницами. Это важно для мессенджеров, которые имеют множество разных страниц и диалоговых окон для обеспечения удобной навигации и пользовательского опыта. Axios обеспечивает возможность выполнения HTTP-запросов и упрощает обмен данными между клиентом и сервером. Это необходимо для мессенджеров, которые требуют постоянного обновления данных и отправки сообщений на сервер. Таким образом, использование фреймворка Vue.js и связанных с ним библиотек для разработки мессенджера является правильным выбором, который позволяет обеспечить высокую производительность, удобную навигацию и обмен данными, а также упрощает управление состоянием приложения.

Django является одним из самых популярных фреймворков для разработки веб-приложений на языке Python. Он предоставляет мощные инструменты для создания серверной части приложения, включая встроенную ORM, автоматическую генерацию форм, поддержку административной панели и многое другое. Djoser является пакетом для аутентификации и регистрации в Django-приложениях, который обеспечивает стандартные REST API эндпоинты для регистрации, входа и выхода пользователя, а также восстановления пароля. DRF является популярным пакетом для создания RESTful API на основе Django, который обеспечивает множество удобных инструментов для работы с сериализацией данных, валидацией, аутентификацией и авторизацией. Django Channels представляет собой библиотеку для создания асинхронных WebSocket-серверов на основе Django, позволяя создавать более интерактивные приложения, например, мессенджеры. Использование всех этих инструментов позволяет значительно упростить и ускорить процесс разработки мессенджера. Django обеспечивает каркас для серверной части приложения, а Djoser и DRF обеспечивают безопасность и удобство работы с API. Использование Django Channels позволяет создавать асинхронные WebSocket-серверы, обеспечивая более быструю и эффективную передачу данных между клиентом и сервером.

Кроме того, все эти инструменты широко используются в сообществе разработчиков, что обеспечивает множество готовых решений и интеграций для проекта. Большое сообщество также обеспечивает поддержку и обновления инструментов, что является важным фактором для продолжения развития и поддержания мессенджера в будущем.

Таким образом, использование Django, Djoser, DRF и Django Channels является правильным выбором для разработки мессенджера, обеспечивая быстрое, безопасное и эффективное создание серверной части приложения с множеством готовых решений и поддержкой сообщества разработчиков.

Далее рассмотрим выбранную систему управления базами данных (СУБД). В данной работе таковой является СУБД MySQL. Выбранная ситема будет являться идеальной совокупность программных и лингвистических средств общего или специального назначения, и даст возможность полномассшабно обеспечивать управление созданием и использованием таблиц данных, справочников и отчетов.  
Система управления базами данных MySQL является бесплатной, непосредственно свободно распространяемой СУБД. Данная система имеет значительно функциональную клиент-серверную архитектуру: к серверу MySQL имеют возможность обращаться разнообразные клиентские приложения, в том числе и с возможностью доступа с удаленных компьютеров. Существует визуальный интерфейс для облегчения работы с базами данных MySQL — PhpMyAdmin. СУБД MySQL версий 5.0 и выше соответствуют стандарту структурированного языка запросов SQL, поэтому она совместима с другими базами данных. Основными языками разработки являются C/C++.

Рассмотрим функциональные особенности системы управления базами данных MySQL:

- реляционная СУБД;  
- имеет открытый код;  
- система имеет кроссплатформенное строение;  
- обладает большим числом программных интерфейсов (API), с помощью которых непосредственно к базе данных MySQL имеют возможность подключения разнообразные приложения, созданные на следующих языках программирования: C/C++, Eiffel, Java, Perl, PHP, Python, Tcl, ODBC, NET и Visual Studio.

- обладает значительными техническими характеристиками, такими как многопользовательский доступ, многопоточность, масштабируемость быстродействие;

- располагает развитой системой обеспечения безопасности функционирования и разграничения доступа к информационным ресурсам на основе системы привилегий.

## Модельные представления объекта разработки

Для создания программной реализации приложения, необходимо его спро- ектировать, сформулировать главную функцию и расписать ее. Результат пред- ставляет IDEF0 диаграмма.

### **IDEF0 диаграмма**

IDEF0 - методология функционального моделирования и графическое представление, предназначенное для описания и формализации бизнес-процессов. Отличительной особенностью IDEF0 является её акцент на соподчинённость объектов. Описание модели выглядит как черный ящик с входами, выходами, управлением и механизмом, постепенно детализирующиеся до необходимого уровня.

На схеме представляет собой набор модулей, со следующим правилом сторон:

1) стрелка входа всегда приходит в левую грань активности; 2) стрелка выхода - правая грань;  
3) стрелка управления - верхняя грань;  
4) стрелка механизма - нижняя грань.

Главные задачи мессенджера – отправка и получение сообщений. Далее представлены IDEF0 диаграммы этих задач.



Рис. 3. Отправка зашифрованного сообщения получателю

На рисунке 3 представлена диаграмма отправки зашифрованного сообще- ния получателю. Диаграмма имеет следующие данные:

1)  Входящие данные – информация профиля пользователя, информа- ция профиля получателя, текст сообщения;

2)  Исходящие данные – информация о доставке сообщения;

3)  Управление – алгоритмы шифрования, требования к содержанию сообщения, протокол передачи данных;

4)  Механизмы – приложение, сервер приложения.

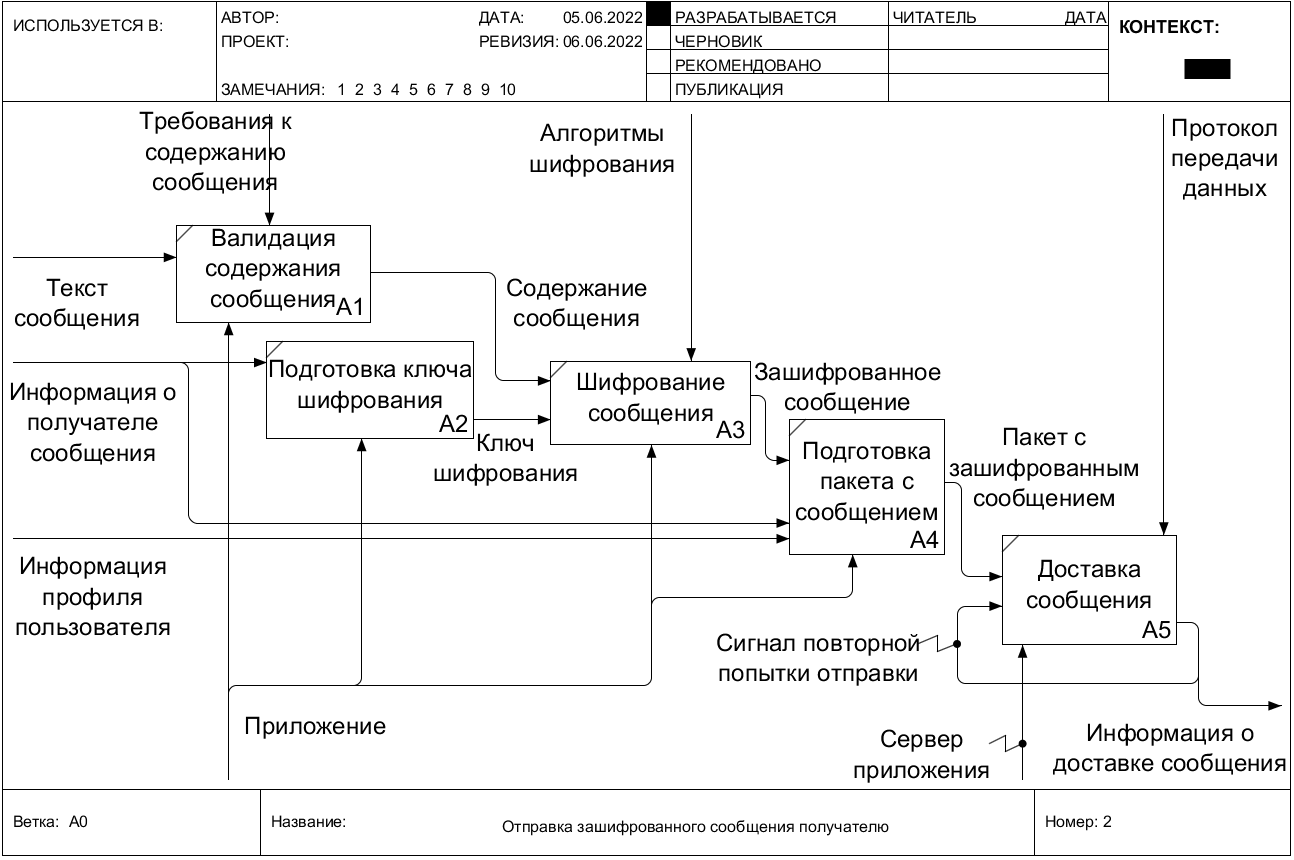


Рис. 4. Процессы отправки зашифрованного сообщения получателю

Далее проиллюстрирован процесс отправки зашифрованного сообщения получателю.

В процессе отправки, сообщение проходит проверку на не пустоту, после чего с помощью открытого ключа получателя шифруется использую криптографический алгоритм RSA. Затем формируется пакет сообщения, состоящий из зашифрованного сообщения, времени отправки, id пользователя и id получателя и отправляется на сервер.

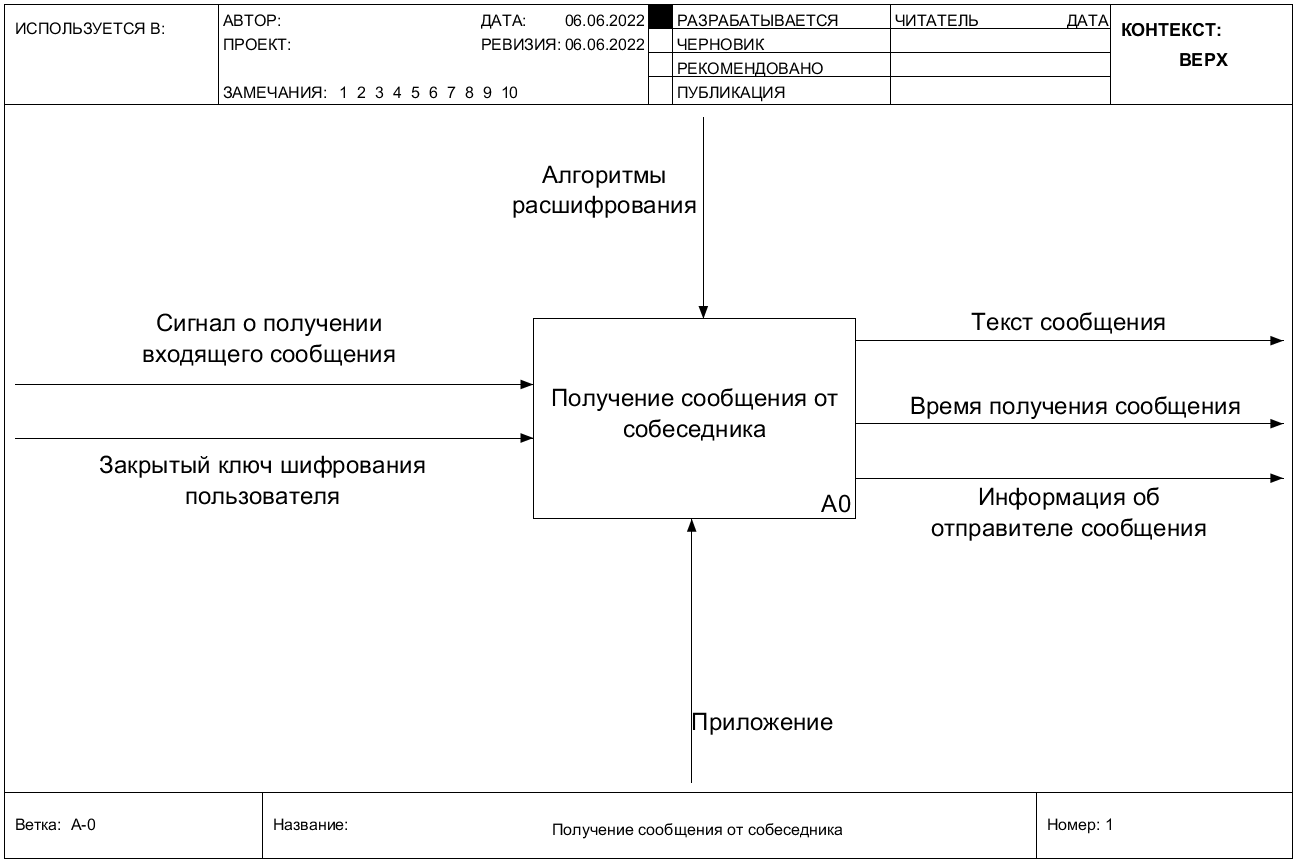


Рис. 5. Получение сообщения от собеседника

На рисунке 5 представлена диаграмма получения сообщения от собесед- ника. Диаграмма имеет следующие данные:

1)  Входящие данные – сигнал о получении входящего сообщения, за- крытый ключ шифрования пользователя;

2)  Исходящие данные – текст сообщения, время сообщения, информа- ция об отправителе сообщения;

3)  Управление – алгоритмы расшифрования;

4)  Механизмы – приложение.

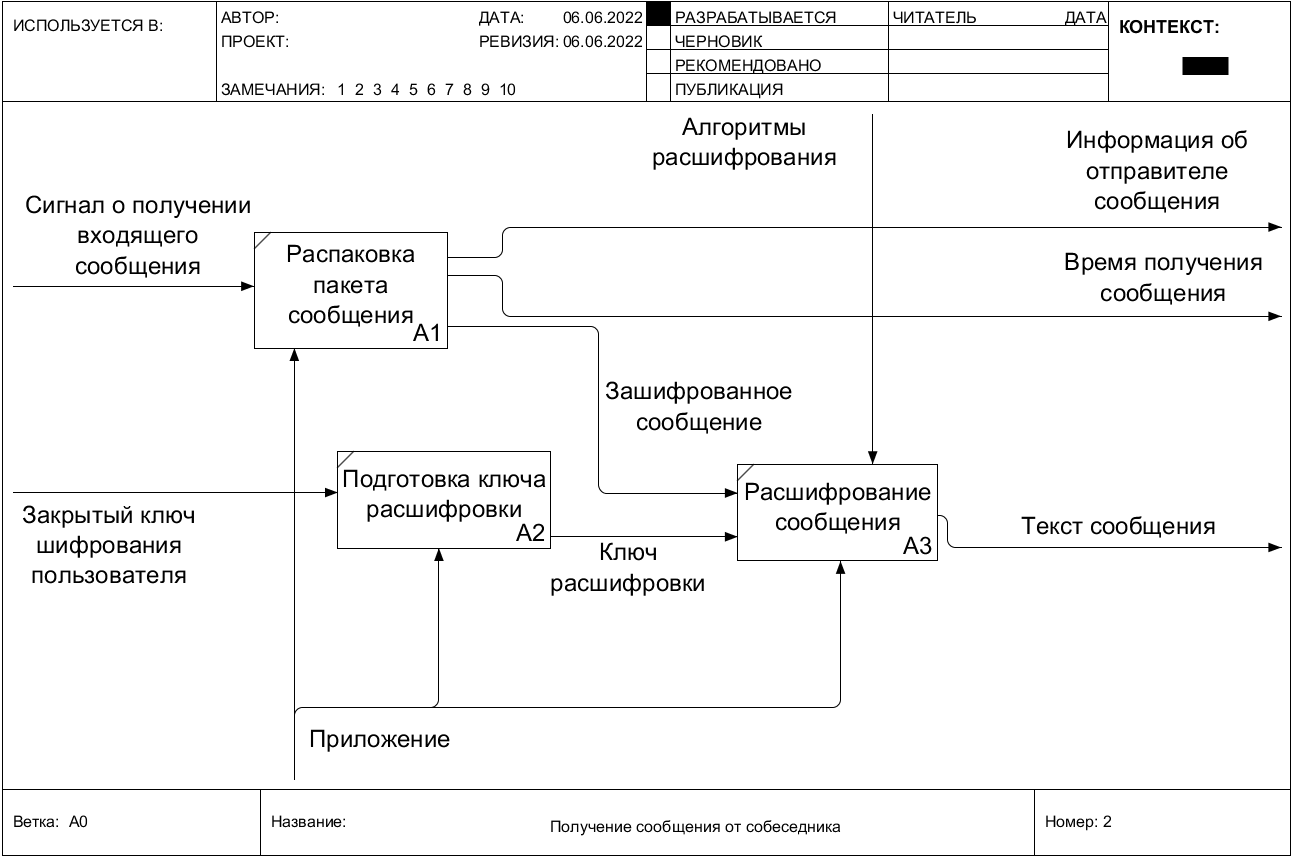


Рис. 6. Процессы получения сообщения от собеседника

В процессе получения сообщения у приложения запущен метод получения сигнала о получении входящего пакета сообщения, после получения которого происходит распаковка данного пакета на: зашифрованное сообщение, время по- лучения сообщения и id отправителя сообщения. Для расшифровки из внутрен- него хранилища подготавливается закрытый ключ для расшифровки и дальней- шего получения текста сообщения.

Но для отправки и получения сообщений, следует также описать процесс регистрации и входа пользователя приложение.

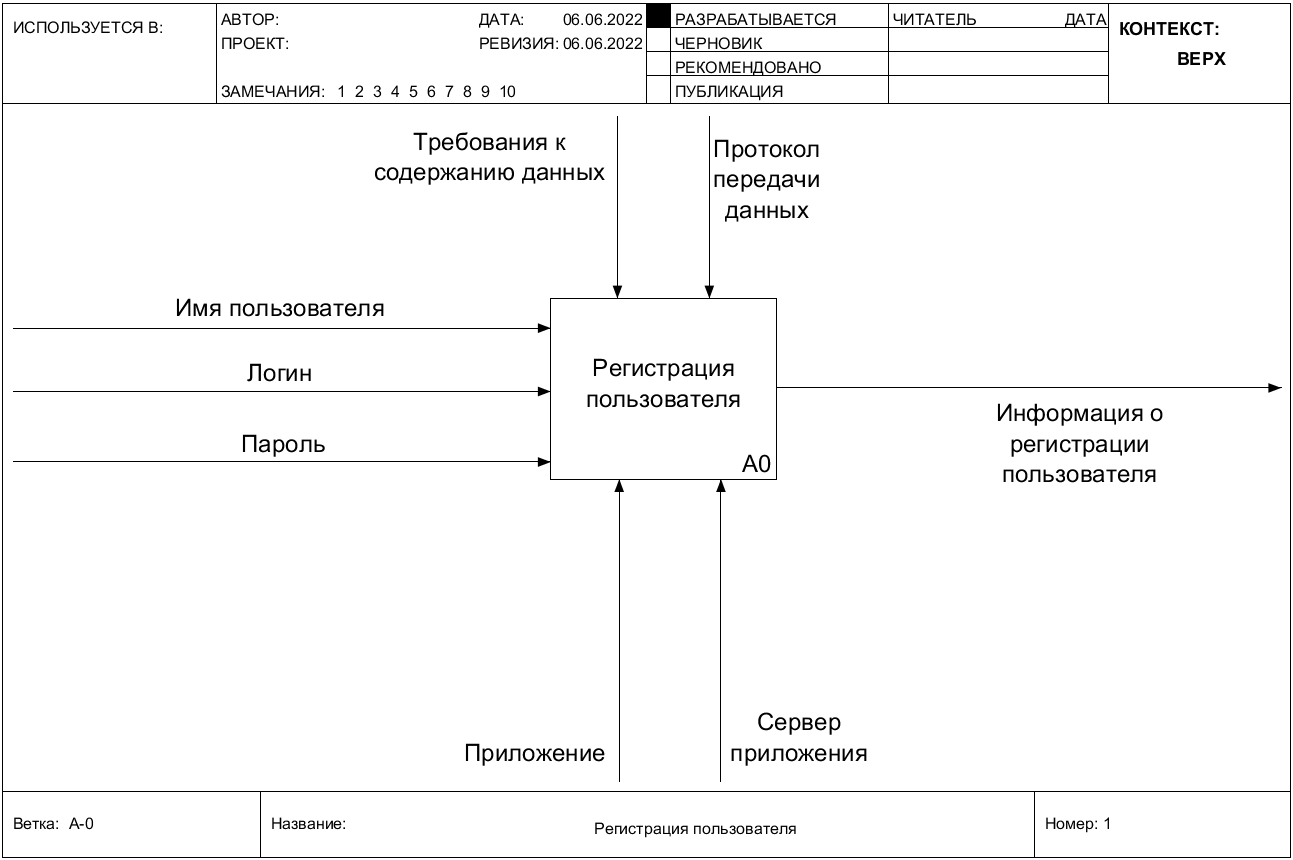


Рис. 7. Регистрация пользователя

На рисунке 7 представлена диаграмма регистрации пользователя. Диаграмма имеет следующие данные:

1)  Входящие данные – имя пользователя, логин, пароль;

2)  Исходящие данные – информация о регистрации пользователя;

3)  Управление – требования к содержанию данных, протокол передачи данных;

4)  Механизмы – приложение, сервер приложения.

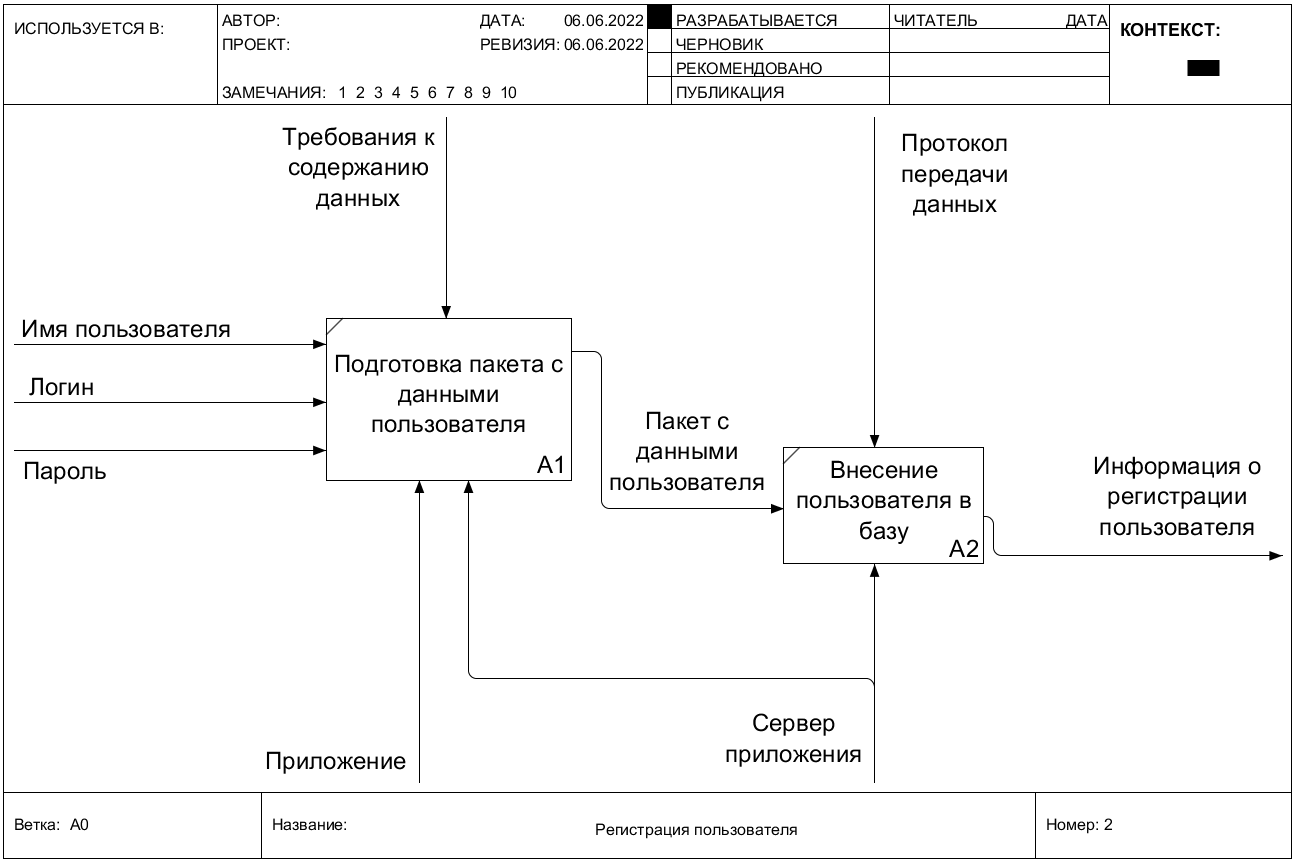


Рис. 8. Процессы регистрации пользователя

Процесс регистрации проверяет корректность введенных данных (все поля проверяются на не пустоту, логин проверяется на уникальность, пароль на длину), после чего формируется пакет с данными пользователя, который вно- сится в базу пользователей.

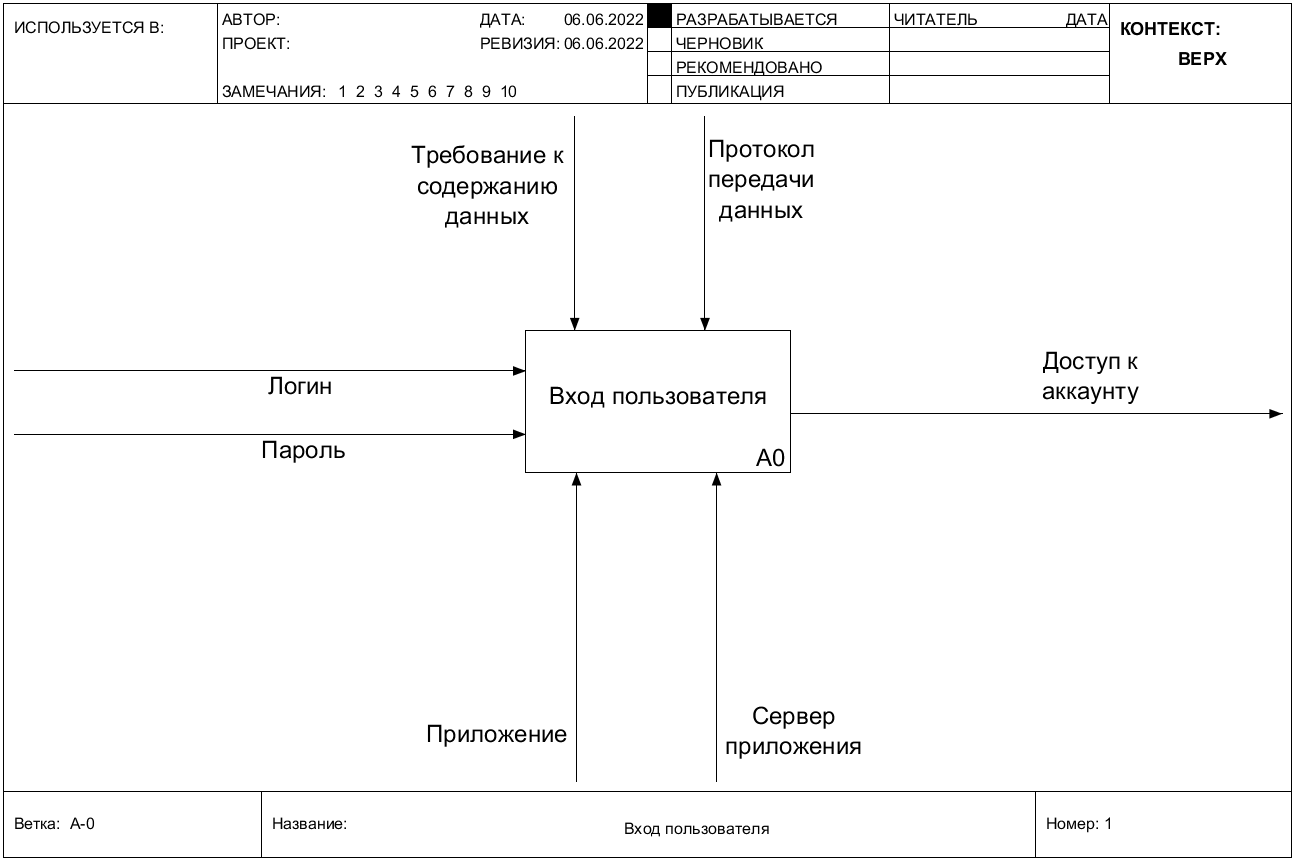


Рис. 9. Вход пользователя

На рисунке 9 представлена диаграмма входа пользователя. Диаграмма имеет следующие данные:

1)  Входящие данные – логин и пароль;

2)  Исходящие данные – доступ к аккаунту;

3)  Управление – требования к содержанию данных, протокол передачи

данных;

4)  Механизмы – приложение, сервер приложения.

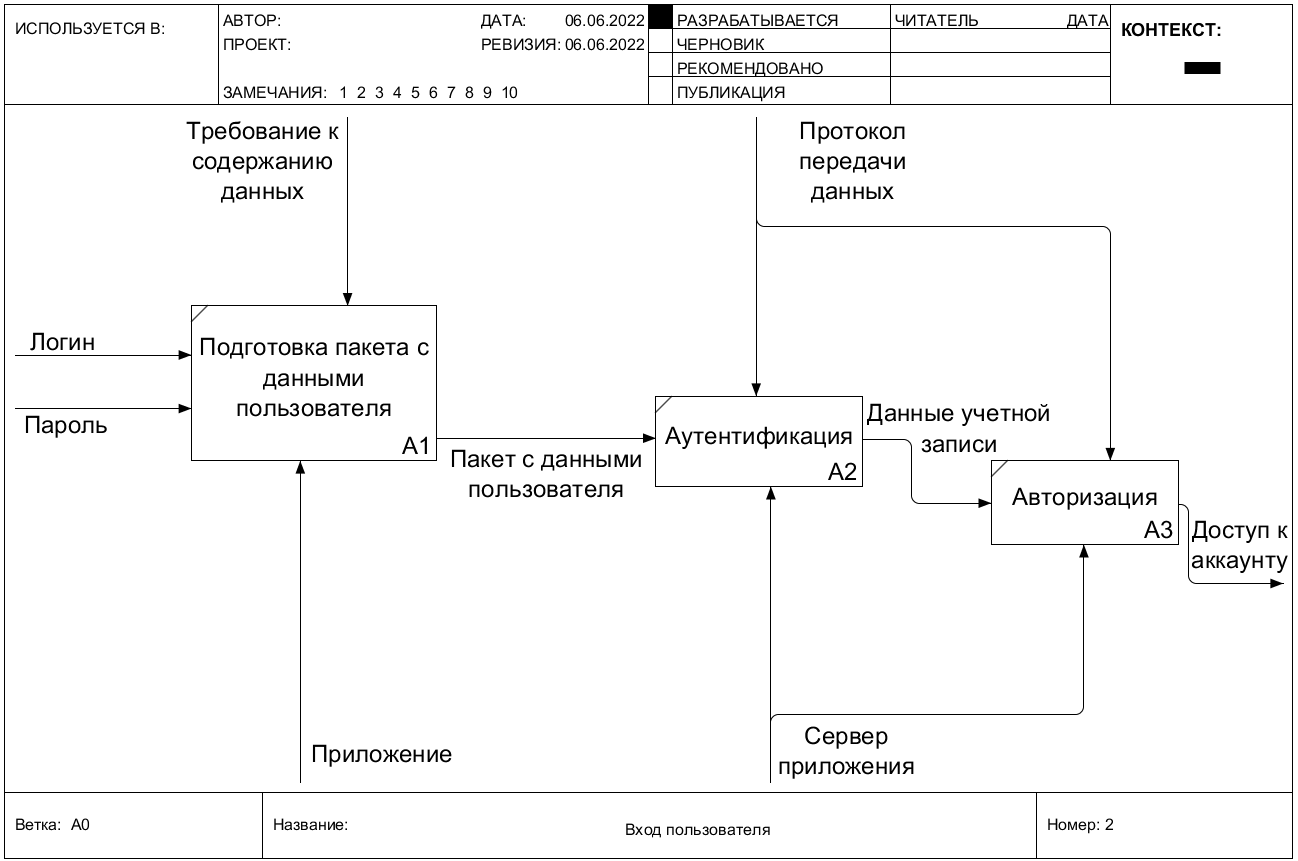


Рис. 10. Процессы входа пользователя

Процесс входа пользователя в приложение похож с процессом регистра- ции. При входе осуществляется проверка введенных данный на отсутствие пу- стых полей, формируется пакет с данными пользователя и происходит аутенти- фикация. В случае удачной аутентификации пользователя происходит его авто- ризация в приложении.

## Разработка программного обеспечения для платформы

## Тестирование и отладка платформы

# АНАЛИЗ БЕЗОПАСНОСТИ И ЭФФЕКТИВНОСТИ ПЛАТФОРМЫ ЗАЩИЩЕННОГО ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ

## Проведение тестирования на безопасность и оценка соответствия требованиям к защите информации

## Оценка эффективности платформы с точки зрения использования организацией

## Сравнение разработанной платформы с существующими аналогами

# ЗАКЛЮЧЕНИЕ

## Основные результаты исследования

## Выводы и рекомендации по дальнейшей разработке и использованию платформы

## Ограничения и ограничивающие факторы

Бюджет. Один из основных ограничивающих факторов - бюджет. Разработка безопасной и надежной платформы для обмена мгновенными сообщениями может быть дорогой. Организации должны выделить достаточно средств, чтобы обеспечить разработку и поддержку платформы на должном уровне.

Соответствие нормам и правилам. Другим ограничивающим фактором является соответствие нормам и правилам, которые регулируют обработку и хранение персональных данных пользователей. Необходимо убедиться, что платформа соответствует соответствующим нормам и правилам, таким как GDPR, HIPAA и т.д.

## Направления дальнейших исследований в области защищенного обмена мгновенными сообщениями

В области защищенного обмена мгновенными сообщениями возможны следующие направления дальнейших исследований:

* Разработка новых методов шифрования и аутентификации данных, которые обеспечат более высокий уровень безопасности.
* Исследование возможностей использования искусственного интеллекта для обнаружения и предотвращения угроз безопасности в реальном времени.
* Развитие методов анализа данных для выявления паттернов и трендов в активности пользователей, что может помочь в обнаружении аномальной активности и в предотвращении угроз безопасности.
* Разработка новых методов обнаружения атак и угроз на ранних этапах, чтобы можно было предотвратить их до того, как они станут серьезным проблемой для пользователей.
* Исследование возможностей использования технологии блокчейн для обеспечения безопасности обмена мгновенными сообщениями.
* Разработка новых методов аудита и мониторинга безопасности, которые позволят администраторам платформы быстро обнаруживать и реагировать на любые угрозы.
* Исследование новых методов анонимизации данных, чтобы пользователи могли общаться с максимальной степенью конфиденциальности и анонимности.
* Развитие новых методов защиты от социальной инженерии и фишинга, которые могут быть использованы злоумышленниками для получения доступа к конфиденциальной информации.
* Разработка новых методов автоматического определения и обработки пользовательских жалоб на нарушения безопасности.
* Разработка новых методов автоматической классификации сообщений на основе их содержания и контекста, что может помочь в предотвращении распространения нежелательной информации и контента.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

# ПРИЛОЖЕНИЕ