ГУАП

КАФЕДРА № 43

ОТЧЁТ  
ЗАЩИЩЁН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент |  |  |  | Г.С. Армашова-Тельник |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЁТ О ПРАКТИЧЕСКОЙ РАБОТЕ №4 |
| Данные проекта в различных форматах |
| по курсу: Экономическое обоснование программных проектов |

РАБОТУ ВЫПОЛНИЛИ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТЫ ГР.№ | 4136 |  |  |  | Н.С. Бобрович, Т.С. Колесникова, П.В. Иноземцева |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2025

1. **Цель работы:**

Представить данные проекта в различных форматах.

1. **Задание на практическую работу:**

1. представить данные проекта (пр 1, 2, 3) в форматах:

- диаграмма Ганта (табличный формат), диаграмма Исикавы (схематично) – п. 5

- графическая модель (сетевой график) проекта - п. 6

- жизненный цикл программного проекта (схематично в системе координат с

выделением и характеристикой этапов) - п. 7

- сформировать матрицу рисков, в табличном формате (наименование риска, методы

предотвращения, методы минимизации наступившего риска) - п. 8

- выполнение расчетной части (соблюдать последовательность выполнения расчетов,

представить формульный ряд с экспликацией, произвести расчеты в рамках проекта,

свести данные в итоговую таблицу) - п. 9

- представить презентационный лист данных – п. 10

1. **Выполнение практической работы:**

**Диаграмма Ганта:**

Для построения диаграммы Ганта нужно разбить проект на этапы и определить сроки выполнения каждой задачи.

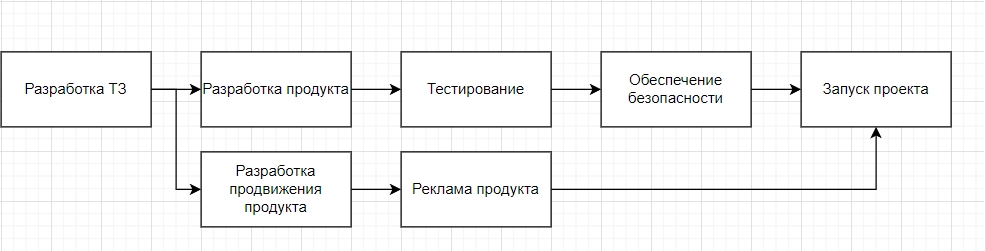
|  |  |  |
| --- | --- | --- |
| Название этапа | Дата начала работы над этапом (месяц/год) | Дата окончанию работы над этапом (месяц/год) |
| Создание ТЗ | 01.07.2025 | 01.08.2025 |
| Разработка | 01.08.2025 | 01.02.2026 |
| Тестирование | 01.02.2026 | 01.04.2026 |
| Запуск | 01.04.2026 | 01.05.2026 |

**Диаграмма Исикавы (причинно-следственная диаграмма):**



**Графическая модель (сетевой график) проекта:**

Сетевой график строится на основе зависимостей между задачами.



**Жизненный цикл программного проекта:**

1. Определение потребностей бизнеса. На этом шаге идея становится более оформленной: появляется аналитика, конкретные требования к продукту, потенциальная выгода и так далее.
2. Инициация. С этого шага начинаются этапы, в которых принимает участие непосредственно команда разработки. Команда получает ТЗ, анализирует его и называет +/- точные сроки и стоимость разработки. Если заказчика это не устраивает – начинаются обсуждения, если заказчика все устроило – ПО уходит в разработку.
3. Проектирование/инженерный дизайн. Команда выбирает методологию разработки, делит ТЗ на изолированные части, выбирают технологии и так далее, готовят ПО к процессу разработки.
4. Имплементация. Непосредственно разработка: написание кода, создание инфраструктуры для приложение, разработка интерфейса и внешнего вида в целом.
5. Тестирование. Когда все задачи выполнены – ПО уходит на тестирование, в процессе которого то, что получилось, сравнивают с тем, что задумывалось. Тестирование может проводиться параллельно с имплементацией, может проводиться после неё.
6. Внедрение. Продукт выпускают на рынок. Основные задачи здесь лежат на отделе маркетинга, от команды разработчиков требуется поддерживать инфраструктуру (сервера, например).
7. Сопровождение. Этап, который может длиться бесконечно. На этом этапе нужно отлавливать баги информационных продуктов, закрывать дыры в безопасности, и тд.
8. Смерть. Если продукт оказался нежизнеспособным или потерял актуальность – его закрывают: перестают поддерживать, закрывают сервера, перестают выделять финансирование на сопровождение.

3-7. Маркетинг. Реклама и продвижение продукта.

**Матрица рисков:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Существенность (верт.)  Вероятность (гор.) | Очень низкий | Низкий | Средний | Высокий | Очень высокий |
| Очень низкий |  | Избыточная сложность системы  (12) | Несоответствие требованиям законодательства  (8) | Неблагоприятные изменения внешней среды  (13) | Утечка данных  (1) |
| Низкий |  | Проблемы с интеграцией существующих систем  (9) |  |  | Недоступность необходимых ресурсов  (11) |
| Средний |  | Зависимость от сторонних поставщиков  (10) | Низкое качество разработки  (2) | Низкая производительность при росте нагрузки  (7) |  |
| Высокий |  | Недовольство клиентов качеством обслуживания  (5) | Недостаток финансирования  (6) | Несоответствие ТЗ  (3) |  |
| Очень высокий | Атака типа DDoS  (4) |  |  |  |  |

1. Утечка данных : Методы предотвращения - Шифрование данных, контроль доступа. Методы минимизации наступившего риска - Резервное копирование и восстановление данных.
2. Низкое качество разработки : Методы предотвращения - Code review. Методы минимизации наступившего риска - Повторное тестирование и исправление ошибок.
3. Несоответствие ТЗ : Методы предотвращения - Валидация требований. Методы минимизации наступившего риска - Пересмотр архитектуры и рефакторинг.
4. Атака типа DDoS : Методы предотвращения - Фильтрация трафика, распределённые серверы. Методы минимизации наступившего риска - Ограничение доступа, перенаправление трафика.
5. Недовольство клиентов качеством обслуживания : Методы предотвращения - Постоянное улучшение UX/UI, техподдержка 24/7. Методы минимизации наступившего риска -Компенсации, персональные предложения, улучшения в сервисе .
6. Недостаток финансирования : Методы предотвращения - Бюджетное планирование, привлечение инвесторов. Методы минимизации наступившего риска - Сокращение расходов, пересмотр приоритетов.
7. Низкая производительность при росте нагрузки : Методы предотвращения - Оптимизация кода, кластеризация серверов. Методы минимизации наступившего риска - Горизонтальное масштабирование, временное ограничение функциональности.
8. Несоответствие требованиям законодательства : Методы предотвращения - Регулярный юридический аудит. Методы минимизации наступившего риска - Внешний консалтинг для соблюдения правовых норм.
9. Проблемы с интеграцией существующих систем : Методы предотвращения - Использование стандартных интерфейсов и протоколов. Методы минимизации наступившего риска - Проведение пилотных проектов для проверки совместимости.
10. Зависимость от сторонних поставщиков : Методы предотвращения - Диверсификация поставщиков. Методы минимизации наступившего риска - Активное взаимодействие с альтернативными поставщиками.
11. Недоступность необходимых ресурсов : Методы предотвращения - Планирование ресурсов заранее. Методы минимизации наступившего риска - Аренда дополнительных мощностей.
12. Избыточная сложность системы : Методы предотвращения - Модульный дизайн и декомпозиция задач. Методы минимизации наступившего риска - Рефакторинг и упрощение сложных модулей.
13. Неблагоприятные изменения внешней среды : Методы предотвращения - Стратегическое планирование. Методы минимизации наступившего риска - Гибкость и адаптивность процесса.

**Выполнение расчётной части:**

Последовательность выполнения расчётов:

1. Оценка бюджета проекта.

Формула:

Бюджет проекта = Зарплаты сотрудников + Закупка оборудования + Прочие расходы, где:

Зарплаты сотрудников = Количество сотрудников × Средняя зарплата сотрудника × Время работы

Закупка оборудования = Стоимость сервера × Количество серверов + Стоимость ПО × Количество лицензий

Прочие расходы = Административные расходы + Маркетинговые расходы + Резервы на непредвиденные обстоятельства

Предположим, что:

Зарплата одного разработчика — 100 000 рублей в месяц.

В команде 10 человек, работающих полный рабочий день.

Продолжительность проекта — около 10 месяцев.

Закупается 5 серверов стоимостью 300 000 рублей каждый.

Стоимость лицензии на ПО — 200 000 рублей за каждую лицензию, всего приобретено 50 лицензий.

Прочие расходы составляют 25% от суммы зарплат и закупок.

Расчёт:

Зарплаты сотрудников:

10 × 100 000 рублей/мес. × 12 мес. = 120 000 000 рублей

Закупка оборудования:

5 × 300 000 рублей/серв. + 50 × 200 000 рублей/лицензию = 10 000 000 + 10 000 000 = 20 000 000 рублей

Прочие расходы:

0.25 × (120 000 000 + 20 000 000) = 35 000 000 рублей

Итоговый бюджет:

140 000 000 + 20 000 000 + 35 000 000 = 195 000 000 рублей

2. Оценка сроков проекта.

Методология оценки сроков:

Используем метод PERT (Program Evaluation and Review Technique) для оценки временных рамок проекта. Формулы:

PERT = (Оптимистичный срок + 4 × Наиболее вероятный срок + Пессимистичный срок) / 6

У нас есть следующие данные для временных рамок проекта:

Оптимистический срок — 8 месяца.

Наиболее вероятный срок — 10 месяца.

Пессимистический срок — 12 месяцев.

PERT = (8 + 10 × 4 + 12) / 6 = ~10 месяцев

Это означает, что наиболее реалистичным сроком завершения этапа разработки является примерно ~10 месяцев.

3. Оценка рентабельности проекта.

Формула:

ROI = ((Доход от проекта − Инвестиции) / Инвестиции) × 100%

Предположим, что доход от проекта ожидается в размере 400 миллионов рублей, а общие затраты (инвестиции) составляют около ~200 миллионов рублей.

ROI = ((400 000 000 − 200 000 000) / 200 000 000) × 100% = ~100%

Рентабельность инвестиций (ROI) составляет 100%, что свидетельствует о хорошей окупаемости проекта.

1. Итоговая таблица.

Теперь сведём все рассчитанные показатели в единую таблицу:

|  |  |
| --- | --- |
| Показатель | Значение |
| Общий бюджет проекта | 195 000 000 рублей |
| Срок разработки | ~10 месяцев |
| ROI проекта | ~100% |

1. Заключение.

Выполненная расчётная часть показывает, что проект имеет хороший потенциал для успешной реализации. Прогнозируемый бюджет находится в пределах разумного диапазона, сроки соответствуют ожиданиям, а рентабельность достаточно высока для привлечения инвесторов.

**Презентационный лист данных:**

Этот документ предназначен для представления основных аспектов проекта руководству, инвесторам или другим заинтересованным сторонам. Его задача — кратко и наглядно изложить ключевые характеристики и ожидаемые результаты проекта.

1. Название проекта

Название проекта: «Облачная платформа для безопасного хранения и обработки данных».

2. Общая информация

Цели проекта:

Обеспечение безопасности данных, масштабируемости и отказоустойчивости облачной платформы.

Создание эффективного решения для корпоративных клиентов и государственных учреждений.

Срок реализации:

Начало: 01.07.2025

Завершение: 01.05.2026

Продолжительность: ~10 месяцев

Бюджет:

Общий бюджет: 195 000 000 рублей

Включает зарплаты, закупку оборудования, программное обеспечение и прочие расходы.

3. Ключевые характеристики

Функционал:

Защита данных от утечек и кибератак.

Масштабируемость для обработки растущего числа пользователей и данных.

Отказоустойчивость и быстрое восстановление после сбоев.

Совместимость с различными платформами и технологиями.

Преимущества:

Соответствие международным стандартам безопасности.

Высокая производительность при увеличении нагрузки.

Круглосуточная техническая поддержка.

Лёгкая интеграция с существующими системами.

4. Этапы реализации

Анализ требований: Определение потребностей клиентов и формирование технического задания.

Разработка : Создание базовой архитектуры и написание кода.

Тестирование: Проверка безопасности, производительности и отказоустойчивости.

Запуск: Полноценное развёртывание платформы и начало эксплуатации.

Поддержка и развитие: Обновления, исправления багов и добавление новых функций.

5. Риски и пути их минимизации

|  |  |  |
| --- | --- | --- |
| Риск | Меры предотвращения | Меры минимизации |
| Утечка данных | Шифрование данных | Резервное копирование и восстановление |
| Несанкционированный доступ | Многофакторная аутентификация | Ограничение доступа и аудит логов |
| Недостаточное финансирование | Бюджетное планирование | Пересмотр приоритетов и сокращение расходов |
| Снижение производительности | Оптимизация кода | Горизонтальное масштабирование |
| Неправильная совместимость с системами | Предварительное тестирование | Использование промежуточных решений |

6. Финансовые показатели

Общая сумма инвестиций: 195 000 000 рублей

Ожидаемый доход: 400 000 000 рублей

Рентабельность инвестиций (ROI): ~100%

8. Заключение

Проект представляет собой высокотехнологичное решение, которое способно удовлетворить растущие потребности рынка в безопасных и масштабируемых облачных услугах. Он сочетает в себе передовые технологии и профессиональные компетенции команды, что гарантирует успех и стабильность в долгосрочной перспективе.

Этот презентационный лист данных содержит всю необходимую информацию для принятия взвешенных решений по проекту.

1. **Выводы:**

Проект разработки облачного сервиса, направленного на обеспечение высокого уровня безопасности, масштабируемости и отказоустойчивости, представляет собой значимое решение для удовлетворения потребностей современного цифрового мира. Основное внимание уделяется защите данных, устойчивости к возрастающим нагрузкам и минимизации последствий кибератак и сбоев. Эти аспекты являются ключевыми для успешного функционирования облачных систем в условиях роста числа пользователей и увеличения объёмов обрабатываемой информации.

Анализ основных проблемных зон выявил необходимость концентрации усилий на предотвращении утечек данных, улучшении масштабируемости и обеспечении отказоустойчивости. Эти направления были обоснованы статистическими данными, подтверждающими значимость проблемы и рост соответствующих рынков. Комплексный подход к решению указанных задач предполагает использование передовых технологий, строгих мер безопасности и стратегического планирования.

Таким образом, успешная реализация данного проекта внесёт значительный вклад в развитие индустрии облачных технологий, повысит уровень кибербезопасности и обеспечит стабильное функционирование цифровых экосистем в условиях постоянно растущих требований к безопасности и производительности.

1. **Предыдущие выполненные задания:**

Практическое задание 1:

1. Направление:

Разработка программного обеспечения для облачных сервисов требует высокой степени безопасности и способности к масштабированию. С ростом числа пользователей и объёма обрабатываемых данных возникает необходимость в создании эффективных решений, обеспечивающих надёжность, производительность и безопасность приложений.

1. Основные проблемные зоны:

Безопасность данных: Облачные сервисы хранят огромные объёмы конфиденциальной информации, что делает их привлекательными целями для кибератак. Проблемы включают утечки данных, несанкционированный доступ и атаки типа DDoS.

Масштабируемость: Приложения должны легко адаптироваться к увеличению нагрузки без снижения производительности. Недостаточная масштабируемость ведёт к задержкам в обработке запросов и ухудшению качества обслуживания клиентов.

Совместимость и интероперабельность: В условиях гетерогенных сред (различные платформы, языки программирования, базы данных) важно обеспечить совместную работу всех компонентов системы.

Обеспечение отказоустойчивости: Программное обеспечение должно быть устойчивым к сбоям и аварийным ситуациям, чтобы минимизировать время простоя и потери данных.

1. Обоснование п.2:

Угрозы безопасности:

По данным компании McAfee, глобальные убытки от киберпреступности составили около $600 млрд в год (по состоянию на 2018 год).

Согласно отчету IBM Security, средняя стоимость утечки данных составляет $3,86 млн (данные за 2019 год).

Рост рынка облачных технологий:

Аналитическая компания IDC прогнозирует, что мировой рынок публичных облаков вырастет до $500 млрд к 2023 году.

Более 90% организаций используют хотя бы один облачный сервис (исследование RightScale, 2019).

Проблемы масштабируемости:

Около 60% IT-руководителей считают масштабируемость одним из ключевых факторов успеха для бизнеса (опрос Forrester Research, 2018).

Исследования показывают, что недостаточная масштабируемость может привести к потерям до 20% потенциальной прибыли компаний.

Эти данные подчеркивают важность разработки безопасного и масштабируемого программного обеспечения для облачных вычислений, способного справляться с растущими угрозами и требованиями современного цифрового мира.

Практическое задание 2:

Модель А. Остервальдера и И. Пинье:

1. Целевое предложение:

Предоставляем компаниям и организациям безопасный, масштабируемый и отказоустойчивый облачный сервис, который позволяет хранить и обрабатывать большие объёмы данных, обеспечивая высокий уровень защиты от кибератак и минимизируя риски потерь данных и производительности.

2. Целевые сегменты:

Крупные предприятия: Нуждаются в высоконадёжных решениях для хранения и обработки больших массивов данных, а также защиты корпоративной информации.

Государственные учреждения: Требуют максимальной безопасности и соответствия законодательным требованиям по защите персональных данных.

Небольшие и средние бизнесы: Стремятся к экономии ресурсов и ищут гибкие решения для быстрого роста и адаптации к меняющимся условиям.

Разработчики ПО: Используют платформу для создания и тестирования новых продуктов в безопасной среде.

3. Ключевые активности:

Разработка и поддержка защищённой инфраструктуры облачной платформы.

Создание инструментов для мониторинга и анализа безопасности.

Автоматизация процессов масштабирования и восстановления после сбоев.

Интеграция с популярными инструментами разработки и управления данными.

4. Ключевые ресурсы:

Команда высококвалифицированных специалистов в области информационной безопасности и облачных технологий.

Современная инфраструктура дата-центров с высоким уровнем защиты.

Лицензии и сертификаты соответствия международным стандартам безопасности.

Партнёрские отношения с ведущими поставщиками технологий безопасности.

5. Ключевые партнёры:

Поставщики оборудования и ПО для дата-центров.

Компании, предоставляющие услуги кибербезопасности.

Консалтинговые фирмы, специализирующиеся на интеграции ИТ-решений.

Разработчики специализированных инструментов для работы с облаками.

6. Каналы сбыта:

Прямая продажа через сайт компании.

Партнерская сеть реселлеров и интеграторов.

Участие в отраслевых выставках и конференциях.

Проведение вебинаров и онлайн-курсов для потенциальных клиентов.

7. Взаимоотношения с клиентами:

Круглосуточная техническая поддержка.

Персонализированные консультации по вопросам безопасности и масштабирования.

Постоянное обновление и улучшение функционала платформы.

Регулярные отчёты о состоянии безопасности и производительности.

8. Потоки доходов:

Подписка на использование платформы.

Дополнительные услуги по настройке и интеграции.

Плата за повышенный уровень безопасности и резервирование данных.

Комиссия за использование сторонних инструментов и API.

9. Структура затрат:

Затраты на разработку и поддержку платформы.

Оплата труда команды разработчиков и экспертов по безопасности.

Расходы на аренду и обслуживание дата-центров.

Инвестиции в маркетинг и продвижение продукта.

Проблема, которую решает проект

Проект направлен на решение проблемы обеспечения безопасности данных, масштабируемости и устойчивости к сбоям в облачных системах. Реализованная платформа позволит пользователям избежать утечек данных, несанкционированного доступа и атак, а также обеспечит плавное увеличение производительности при росте числа пользователей и объёма данных.

**Кто выиграет от реализации проекта?**

Основные стейкхолдеры:

Компании-клиенты:

1. Получат надежный и безопасный инструмент для хранения и обработки данных.
2. Смогут быстрее реагировать на изменения в бизнесе благодаря легкому масштабированию.
3. Минимизируют риски финансовых и репутационных потерь от кибератак.
4. Пользователи конечных продуктов:
5. Будут защищены от утечек личных данных.
6. Пользуются услугами с минимальным временем отклика и стабильностью.

Партнёры и поставщики:

1. Увеличение спроса на их продукты и услуги в сфере кибербезопасности и облачных технологий.
2. Возможность расширения партнерских сетей и повышения своей экспертизы.
3. Государство и регуляторы:
4. Повышение уровня национальной кибербезопасности.
5. Соответствие законодательству в области защиты данных.

Инвесторы:

1. Выгодные инвестиции в быстрорастущий сектор облачных технологий.
2. Рост стоимости акций компании-разработчика.

Практическое задание 3:

**1. Цель проекта в формате SMART и дерево целей:**

**SMART-цель:**

Specific:Создать облачную платформу, обеспечивающую высокий уровень безопасности, масштабируемость и отказоустойчивость для корпоративных клиентов и государственных учреждений.

Measurable:Доля клиентов, использующих платформу, достигнет 10% от общего числа целевого сегмента в течение первых двух лет после запуска. Уровень удовлетворённости клиентов составит не менее 85%.

Achievable:Использование проверенных технологий кибербезопасности и партнёрства с ведущими игроками рынка позволяют достичь поставленных целей.

Relevant:Платформа соответствует актуальным потребностям рынка и способствует решению критически важных проблем в области кибербезопасности и облачных технологий.

Time-bound:Запуск основной версии платформы запланирован на конец первого года реализации проекта, полная функциональность — через два года.

**Дерево целей:**

Главная цель:Создание надёжной и масштабируемой облачной платформы.

Подцели:

Безопасность данных:

Разработать систему защиты от кибератак.

Обеспечить соответствие международным стандартам безопасности.

Масштабируемость:

Создать инфраструктуру, поддерживающую автоматическое масштабирование.

Оптимизировать производительность при увеличении нагрузки.

Отказоустойчивость:

Внедрить механизмы резервного копирования и восстановления данных.

Уменьшить время простоя до минимума.

Интероперабельность:

Поддержка интеграции с различными платформами и базами данных.

Совместимость с популярными языками программирования и фреймворками.

Клиентский опыт:

Предоставлять круглосуточную техподдержку.

Проводить регулярные обновления и улучшения функционала.

**2. PEST-анализ внешних факторов:**

Политические факторы (P):

Законодательные требования к защите данных (например, GDPR, ФЗ-152 в РФ).

Государственная политика поддержки инноваций в сфере кибербезопасности.

Риски санкционного давления и ограничений на импорт технологий.

Экономические факторы (E):

Рост мирового рынка облачных технологий ($500 млрд к 2023 году).

Высокий спрос на безопасные и масштабируемые решения среди крупных предприятий и госучреждений.

Конкуренция со стороны международных игроков на рынке облачных услуг.

Социальные факторы (S):

Повышенное внимание общества к вопросам конфиденциальности и безопасности данных.

Тенденция к цифровизации бизнес-процессов и переходу на удалённую работу.

Рост осведомлённости о рисках кибератак среди потребителей.

Технологические факторы (T):

Быстрая эволюция технологий кибербезопасности и облачных вычислений.

Доступность передовых инструментов для автоматизации и мониторинга безопасности.

Необходимость постоянного обновления и модернизации инфраструктуры.

Выводы:

Внешние условия благоприятствуют развитию проекта. Растущие потребности в кибербезопасности и масштабируемых облачных решениях создают значительный рыночный потенциал. Однако важно учитывать регуляторные ограничения и конкуренцию на международном уровне.

**3. SWOT-анализ внутренних факторов**

Strengths (сильные стороны):

Высокая квалификация команды в области кибербезопасности и облачных технологий.

Наличие лицензий и сертификатов соответствия международным стандартам.

Партнёрские отношения с ведущими поставщиками технологий безопасности.

Weaknesses (слабые стороны):

Ограниченный бюджет на первоначальном этапе.

Отсутствие готовой клиентской базы и опыта продвижения на рынке.

Зависимость от сторонних поставщиков оборудования и ПО.

Opportunities (возможности):

Растущий спрос на безопасные облачные решения.

Возможность выхода на международные рынки.

Привлечение инвестиций и партнёрских соглашений.

Threats (угрозы):

Жёсткая конкуренция с крупными международными игроками.

Изменения в законодательстве, влияющие на требования к безопасности данных.

Кибератаки и другие внешние угрозы, способные подорвать доверие к платформе.