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 №2 |
| Идея проекта |
| 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:**

Определить идею проекта.

1. **Задание на практическую работу:**

1. При формировании отчёта приложить выполненное задание 1. **(пункт 5)**   
2. Сформировать идею проекта в формате модели А. Остервальдера и И. Пинье.   
3. Обозначить - какую проблему решит реализованный проект - кому поможет (охарактеризовать всех стейкхолдеров проекта).

1. **Выполнение практической работы:**

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.
3. **Выводы:**

Определили идею проекта.

1. **Выполненное задание 1:**
2. 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.