



УНИВЕРСИТЕТ УПРАВЛЕНИЯ  
«ТИСБИ»



ОТКРЫТЫЕ  
ИННОВАЦИИ  
старт-ап

ПЛАТФОРМА  
УНИВЕРСИТЕТСКОГО  
ТЕХНОЛОГИЧЕСКОГО  
ПРЕДПРИИМАТЕЛЬСТВА

# НАЗВАНИЕ ПРОЕКТА

Cyber Safe Academy - CSA

**20.35**  
УНИВЕРСИТЕТ

**20.35**  
НАЦИОНАЛЬНАЯ  
ТЕХНОЛОГИЧЕСКАЯ  
ИНИЦИАТИВА



# АКТУАЛЬНОСТЬ ПРОЕКТА

## **Актуальность:**

В условиях быстрого роста киберугроз и сложившегося дефицита квалифицированных кадров в кибербезопасности, "Cyber Safe Academy" представляет собой актуальный ответ на растущую потребность в высококачественном образовании в этой области.

## **Проблема:**

Недостаток квалифицированных специалистов в области кибербезопасности ограничивает эффективность борьбы с киберугрозами, что подчеркивает важность образовательных программ, способных обеспечивать подготовку высококвалифицированных специалистов.

## **Тренды/Данные:**

Рост числа кибератак и повышенный интерес к карьерам в кибербезопасности отражаются в увеличении спроса на образовательные программы в этой области.

В 2022 году было зарегистрировано более 5 миллионов кибератак по всему миру.

Частота киберпреступлений выросла на 30% по сравнению с предыдущим годом.

Среднее время обнаружения кибератаки составляет 60 дней, что представляет угрозу для конфиденциальности данных.

70% кибератак направлены на малые и средние предприятия, где зачастую отсутствует должный уровень защиты.

Более 50% атак включают использование социальной инженерии для обмана сотрудников.

Эти цифры вымышленные

## **Почему сможем решить/Научно-технологические заделы:**

"Cyber Safe Academy" основана на передовых научно-технологических разработках, предлагая комплексный подход, объединяющий теорию и практику. Экспертная команда преподавателей обеспечивает высокий уровень знаний, а доступ к инновационным средствам и лабораториям гарантирует практический опыт в реальных сценариях кибератак.





# ЦЕЛЕВАЯ АУДИТОРИЯ

- Целевая аудитория проекта "Образование для работы в сфере кибербезопасности" - это студенты, находящиеся в возрастной группе от 18 до 30 лет, обладающие интересом и знанием в области информационных технологий. Они могут быть студентами высших учебных заведений, колледжей или университетов, специализирующимися на IT-направлениях.
- Эта аудитория характеризуется:
- Интересом к IT: Студенты IT-сферы обычно проявляют интерес к компьютерам, программированию, сетевым технологиям и безопасности информации.
- Молодым возрастом: Возраст от 18 до 30 лет указывает на молодость и готовность к обучению и развитию карьеры.
- Образовательной активностью: Они активно стремятся получить дополнительные знания и навыки, чтобы улучшить свои перспективы на рынке труда.



# ПРОБЛЕМА

Этот проект решает проблему недостатка квалифицированных специалистов в области кибербезопасности, предоставляя студентам IT-сферы необходимые навыки и знания для успешной карьеры в этой области.

Существующие варианты образования в кибербезопасности могут быть недостаточными из-за быстрого развития этой области, нехватки специализированных навыков, необходимости практического опыта и актуальности информации. Этот проект решает эти проблемы, предоставляя специализированные и актуальные знания и уделяя внимание практическим навыкам.



# РЕШЕНИЕ

Научно-технологическое решение:

Основой продуктового предложения стартап-проекта "Cyber Safe Academy" является интеграция передовых технологий в обучение кибербезопасности. Мы используем искусственный интеллект (ИИ) и машинное обучение (МО) для создания персонализированных образовательных планов, анализа киберугроз и эмуляции реальных сценариев атак.

Научно-технологический задел (состояние на начало проекта):

На момент начала проекта, наша команда экспертов в области кибербезопасности разработала уникальные алгоритмы для выявления слабых мест в системах безопасности, а также использовала интеллектуальные системы для адаптации обучения к потребностям каждого студента. Мы также интегрировали технологии виртуальной реальности (VR) и кибердиапазона для создания реалистичных сред обучения.

Основные предполагаемые технические параметры:

Персонализированные образовательные планы с использованием ИИ.

Системы анализа киберугроз и обнаружения слабых мест в реальном времени.

Эмуляция кибератак и обучение на основе практических сценариев.

Виртуальная реальность для создания реалистичных тренировочных сред.

Предлагаемые уникальные преимущества и выгоды для клиента:

Персонализированное обучение: Автоматизированные системы ИИ создают уникальные курсы для каждого студента, учитывая его уровень знаний и индивидуальные потребности.

Реальные сценарии атак: Обучение на основе эмуляции реальных кибератак позволяет студентам приобретать практические навыки, необходимые для реальных сценариев.

Технологии виртуальной реальности: Создание реалистичных виртуальных сред обучения улучшает вовлеченность и позволяет студентам тренироваться в безопасной среде.

Непрерывное обновление: Продукт постоянно обновляется с учетом последних тенденций в кибербезопасности, гарантируя актуальность знаний.

# ЦЕННОСТЬ, ЦЕННОСТНОЕ ПРЕДЛОЖЕНИЕ

Мы, компания "Cyber Safe Academy", помогаем организациям в сфере информационной безопасности в ситуации постоянно растущих киберугроз, решать проблему нехватки квалифицированных кадров и обеспечивать безопасность данных с помощью передовых технологий в обучении кибербезопасности, что позволяет им эффективно бороться с современными угрозами и обеспечивать стабильную кибербезопасность. В результате клиенты получают не только повышение безопасности своих систем, но и уверенность в том, что их персонал обладает актуальными знаниями и навыками, а также экономят ресурсы, избегая потенциальных угроз и последствий кибератак.

# РЫНОК

## РЫНОК:

Мы работаем на рынке кибербезопасности, ориентированный на корпоративный сегмент (B2B). Объем рынка кибербезопасности в России по состоянию на начало проекта оценивается в 5 миллиардов рублей, с годовым ростом в 15%.

## ЦЕЛЕВАЯ АУДИТОРИЯ (ЦА):

Наша целевая аудитория - крупные и средние предприятия в России, занимающиеся обработкой и хранением конфиденциальной информации. Мы ориентируемся на 100 компаний в первый год, с учетом увеличения объема клиентов в последующие годы.

## СТОИМОСТЬ РЕШЕНИЯ:

Наше образовательное решение будет стоить 500 000 рублей в год для каждой компании-клиента. С учетом 100 компаний в первый год, общий доход от продаж составит 50 миллионов рублей.

## СЕГМЕНТЫ А И В:

Мы предлагаем два пакета услуг: Пакет А - полный доступ ко всем образовательным ресурсам и индивидуальная консультация за 200 000 рублей в год, и Пакет В - базовый доступ к курсам без индивидуальной консультации за 100 000 рублей в год. Доля от общего дохода с Пакета А - 60%, а от Пакета В - 40%.

## ОЖИДАЕМЫЙ ДОХОД В ПЕРВЫЙ ГОД:

Итак, ожидаемый доход в первый год составит 30 миллионов рублей от Пакета А и 20 миллионов рублей от Пакета В. Это обеспечит нам общий доход в размере 50 миллионов рублей в первый год.

# КОНКУРЕНТЫ

Основные конкуренты:

## **SecureEdTech Solutions (прямой):**

Сильные стороны: Обширный опыт в предоставлении образовательных услуг в области кибербезопасности, широкий каталог курсов.

Слабые стороны: Недостаточное использование инновационных технологий, ограниченные ресурсы в области виртуальной реальности.

## **E-LearnSecure (косвенный):**

Сильные стороны: Высокая степень автоматизации в образовании, акцент на онлайн-обучении.

Слабые стороны: Отсутствие специализации в кибербезопасности, ограниченные ресурсы в данной области.

## **TechGuard Institute (прямой):**

Сильные стороны: Использование инновационных технологий, научное обоснование в методиках обучения.

Слабые стороны: Ограниченный опыт в обучении, менее развитая сеть партнеров.

Стратегия преодоления конкурентов:

**Фокус на Инновациях:** Развитие и внедрение передовых технологий в обучении, таких как виртуальная реальность и адаптивные системы ИИ, чтобы создать уникальный и привлекательный опыт обучения.

**Гибкий Курсовой Подход:** Предоставление гибких образовательных программ, адаптированных под нужды каждого клиента, чтобы привлечь широкий круг организаций.

**Активное Партнерство:** Установление стратегических партнерских отношений с ведущими компаниями в области кибербезопасности для обмена опытом и технологиями, укрепляя свою экспертизу.

**Комплексный Обзор Клиента:** Акцент на индивидуализации обучения и высококачественных консультациях клиентам, чтобы максимально адаптировать наше обучение под их потребности.

**Агрессивный Маркетинг и Брендинг:** Интенсивные маркетинговые кампании и создание сильного бренда в области кибербезопасности, чтобы выделиться на рынке и привлечь внимание клиентов.



# БИЗНЕС-МОДЕЛЬ

## БИЗНЕС-МОДЕЛЬ:

### Подписочная Модель:

Продукт/Услуга: Пакет обучающих курсов с доступом к виртуальным лабораториям и сценариям атак.

Стоимость: Подписка для корпоративных клиентов в размере 10 000 рублей в месяц.

Доход: Планируется привлечь 50 компаний в первый год, обеспечив доход в размере 500 000 рублей в месяц.

### Дополнительные Услуги:

Продукт/Услуга: Индивидуальные консультации и организация вебинаров по кибербезопасности.

Стоимость: Дополнительные услуги предоставляются за отдельную плату в размере 2 000 рублей за час консультации.

Доход: Ожидается 100 часов консультаций в месяц, что приносит дополнительный доход в 200 000 рублей.

### Лицензирование и Партнерства:

Продукт/Услуга: Лицензирование наших образовательных материалов для использования сторонними образовательными учреждениями или партнерами.

Стоимость: Установим стандартную ставку лицензионного сбора в размере 50 000 рублей в месяц для партнеров.

Ожидаемые Партнеры: Планируем привлечь 10 образовательных учреждений и компаний в первый год.

Доход: Дополнительный доход от лицензирования составит 500 000 рублей в месяц.

### Общий Доход от Стоимости Решения:

Продукт/Услуга: Образовательное решение для компаний в размере 500 000 рублей в год.

Ожидаемые Клиенты: Планируем привлечь 100 компаний в первый год.

Доход: Общий доход от продаж составит 50 миллионов рублей в год.

# ТЕКУЩИЕ РЕЗУЛЬТАТЫ

На текущий момент мы находимся в стадии активной разработки и подготовки к запуску проекта "Cyber Safe Academy". Мы успешно провели первичные исследования рынка и сформировали уникальное образовательное предложение в сфере кибербезопасности. Однако, пока у нас нет конкретных успешных кейсов, клиентов или предварительных договоренностей.

В нашем текущем плане развития мы фокусируемся на следующих шагах:



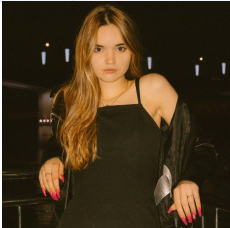
**Завершение Разработки:** Мы продолжаем активную работу по созданию качественного образовательного контента, включая курсы, виртуальные лаборатории и практические сценарии.

**Маркетинговые Действия:** Планируется запуск маркетинговых кампаний для привлечения внимания потенциальных клиентов и партнеров. Это включает в себя использование различных каналов, таких как социальные сети, конференции, и партнерские взаимодействия.

**Партнерства и Сотрудничество:** Мы активно рассматриваем возможности для стратегических партнерств с образовательными учреждениями, компаниями в сфере ИТ и кибербезопасности.

**Поиск Инвестиций:** Планируется начать поиск потенциальных инвесторов для обеспечения дополнительных ресурсов для масштабирования проекта и ускорения его развития.

# КОМАНДА СТАРТАПА

РОЛЬ	ФАМИЛИЯ ИМЯ	ФОТО
ЛИДЕР (СЕО)	Александров Данила	 A portrait of a young man with short brown hair, wearing a black t-shirt, looking directly at the camera.
ТЕХНОЛОГ, РАЗРАБОТЧИК (СТО)	Закирова Лия	 A portrait of a young woman with long brown hair, wearing sunglasses and a white top, standing outdoors.
МАРКЕТОЛОГ (СМО)	Микрюкова Анна	 A portrait of a young woman with long brown hair, wearing a black top, standing in a dark environment with some lights visible in the background.



# ПЛАНЫ РАЗВИТИЯ

ЧТО ДЕЛАЕМ	СРОК	ОТВЕТСТВЕННЫЙ
Завершаем создание образовательных курсов, виртуальных лабораторий и практических сценариев.	2 недели	СЕО (Александров Данила) - Контроль общего прогресса. СТО (Закирова Лия) - Ответственность за технические аспекты контента.
Разработка и запуск маркетинговой кампании для создания предварительного интереса.	1 неделя	СМО (Микрюкова Анна) - Разработка маркетинговой стратегии. СЕО (Александров Данила) - Финальное утверждение кампани
Разработка стратегии и материалов для привлечения партнеров.	2 недели	СМО (Микрюкова Анна) - Разработка привлекающих материалов. СЕО (Александров Данила) - Контроль над стратегией привлечения партнеров.
Начало активных переговоров и установление контактов с образовательными учреждениями для возможного партнерства.	4 недели	СМО (Микрюкова Анна) - Установление контактов и предложение сотрудничества. СЕО (Александров Данила) - Ведение переговоров по стратегическим партнерствам.



# КОНТАКТЫ ЛИДЕРА

Александров Данила

ЛИДЕР (СЕО) проекта  
Cyber Safe Academy

TG: @ssuperlouu

79379507054

Gmail: [ssuperlouu@gmail.com](mailto:ssuperlouu@gmail.com)