ПАСПОРТ СОЦИАЛЬНОГО ПРОЕКТА

_____*(ссылка на проект)* *(дата выгрузки)*

Наименование образовательной организации высшего образования (Получателя гранта)	Чебоксарский институт (филиал) федерального государственного автономного образовательного учреждения высшего образования «Московский политехнический университет»
Регион Получателя гранта	Чувашская республика
Наименование акселерационной программы	«Мосполитех-Чебоксары 3.0»
Дата заключения и номер Договора	

	КРАТКАЯ ИНФОРМАЦИЯ О СОЦИАЛЬНОМ ПРОЕКТЕ	
1	**Название стартап-проекта**	Рука помощи детям
2	**Тема социального проекта** *Указывается тема социального проекта в рамках темы акселерационной программы.*	[illegible]
	ИНФОРМАЦИЯ О ЛИДЕРЕ И УЧАСТНИКАХ СОЦИАЛЬНОГО ПРОЕКТА	
6	**Лидер социального проекта***	- Unti ID 1079509 - Leader ID 3704381 - ФИО Лысенко Степан Игоревич - Телефон 89519993450 - Почта 987987at@gmail.com
7	**Команда стартап-проекта (участники стартап-проекта, которые работают в рамках акселерационной программы)**	

№	Unti ID	Leader ID	ФИО	Роль в проекте	Телефон, почта	Должность (при наличии)	Опыт и квалификация (краткое описание)

	1	1919397	6254506	Столбов Иван Юрьевич	Маркетолог-монтажер	+7(927)861-88-37, stolboa/vanya@yandex.ru		

ПЛАН РЕАЛИЗАЦИИ СТАРТАП-ПРОЕКТА

8	**Аннотация проекта*** *Указывается краткая информация (не более 1000 знаков, без пробелов) о стартап-проекте (краткий реферат проекта, детализация отдельных блоков предусмотрена другими разделами Паспорта): цели и задачи проекта, ожидаемые результаты.*	**Цели и задачи:** • Повышение осведомленности детей и подростков о мошенничестве: Обучение детей и подростков основам интернет-безопасности и распознаванию мошеннических схем. • Развитие навыков самозащиты от мошенничества: Предоставление практических рекомендаций по защите от мошенников, формирование навыков критического мышления и умения отличать правду от лжи. • Создание безопасной онлайн-среды: Совместная работа с родителями, педагогами, правоохранительными органами для создания безопасной онлайн-среды для детей и подростков. **Ожидаемые результаты:** • Уменьшилось мошеннических действий по отношению к детям и их родителям что привело к сохранению финансовых ресурсов, психологическому состоянию и более бдительному пользованию интернетом

	Характеристика будущего продукта	
9	**Основные технические параметры, включая обоснование соответствия идеи/задела тематическому направлению (лоту)*** *Необходимо привести основные технические параметры продукта, которые обеспечивают их конкурентоспособность и соответствуют выбранному тематическому направлению*	**1.Система мониторинга подозрительной активности:** **Параметр:** Алгоритмы машинного обучения (например, на основе нейронных сетей или деревьев решений) для анализа поведения пользователей в сети (частота сообщений, типы сайтов, взаимодействие с неизвестными контактами, финансовые операции). **Обоснование:** выявление аномалий в поведении, характерных для фишинга, вымогательства, онлайн-мошенничества (например, внезапное увеличение трафика на сомнительных сайтах, запросы на перевод денег неизвестным лицам). Это помогает выявлять риски на ранних стадиях и предотвращать потери. **Дополнительные параметры:** интеграция с базами данных известных фишинговых сайтов и вредоносных программ. Анализ эмоционального состояния пользователя по текстам сообщений (NLP). **2. Система фильтрации контента:** **Параметр:** Многоуровневый подход к фильтрации контента, включая ключевые слова, анализ изображений и видео, распознавание речи. **Обоснование:** Блокировка доступа к сайтам с неприемлемым контентом (насилие, порнография, экстремизм), предотвращение контактов с потенциальными преступниками, распространяющими вредоносный контент. **Дополнительные параметры:** возможность персонализации фильтров в зависимости от возраста и настроек пользователя (с контролем со стороны родителей). Использование технологий блокировки рекламы и вредоносных ссылок. **3. Система обучения безопасного поведения в интернете:** **Параметр:** интерактивные обучающие игры и модули, система обратной связи и тестирования знаний. **Обоснование:** Повышение цифровой грамотности детей и подростков, развитие навыков критического мышления и умения распознавать мошеннические схемы. **Дополнительные параметры:** интеграция с учебными программами школ, доступность материалов на разных платформах (мобильные приложения, веб-сайты). **4. Система уведомлений и оповещений:** **Параметр:** Система push-уведомлений, SMS-сообщения или рассылка по электронной почте о потенциальных угрозах, подозрительной активности и новом мошенническом ПО. **Обоснование:** Своевременное информирование детей и родителей о потенциальных угрозах, помощь в принятии решений о необходимых действиях. **Дополнительные параметры:** интеграция с социальными сетями и мессенджерами, возможность отключения уведомлений. **5. Система защиты финансовых операций:** **Параметр:** двухфакторная аутентификация, ограничения на денежные переводы, мониторинг необычной активности на банковских счетах. **Обоснование:** защита от несанкционированного доступа к финансовым ресурсам, предотвращение кражи денег.

		Дополнительные параметры: интеграция с банковскими системами, блокировка подозрительных транзакций.

	Характеристика проблемы, на решение которой направлен стартап-проект	
25	**Какая часть проблемы решается (может быть решена)***	**1.Прямые угрозы:** финансовые потери из-за мошенничества, кражи личных данных, угроза безопасности, связанная с кибербуллингом, угрозами, шантажом, участием в противозаконных онлайн-группах. **2.Психологическое благополучие:** потеря самооценки, тревожность, депрессия, вызванные кибербуллингом, демонстрацией неприемлемого контента, манипуляциями и давлением со стороны интернет-знакомых. **3.Социальное развитие:** возможные проблемы с социализацией, формирование неадекватного поведения в реальной жизни, нездоровой зависимости от цифровых коммуникаций, негативный опыт. **Не решается полностью проблема:** **4.Общие проблемы цифрового пространства:** например, вопросы информационного шума, информационной перегрузки, проблем с использованием цифровых инструментов в образовании и самообразовании. **5.Всех аспектов проблем:** остаются вопросы, связанные с подростковым кризисом, психическим здоровьем, созависимостью в семье и другими социальными и психологическими проблемами, которые могут усугубляться использованием цифровых технологий. **6.Технологических рисков:** хотя эта тема посвящена мошенничеству, она не охватывает такие проблемы, как недостаточная кибербезопасность в системах, проблемы с обеспечением конфиденциальности и злоупотребление технологиями. **7.Глобальный контекст проблем**: эта область фокусируется на локальных пользователях, но не всегда охватывает глобальные проблемы, связанные с тем, что мошенники могут действовать на международном уровне, а также с проблемами обеспечения защиты данных, которые затрагивают пользователей в разных странах. В итоге, тема фокусируется на **уязвимости конкретной группы (детей и подростков)** и **их взаимодействии с цифровым пространством**, но не охватывает все аспекты цифровых проблем. Это важный и актуальный фрагмент, но не единственный для решения проблем в цифровом мире.

	Необходимо детально раскрыть вопрос, поставленный в пункте 10, описав, какая часть проблемы или вся проблема решается с помощью стартап-проекта	
26	**«Держатель» проблемы, его мотивации и возможности решения проблемы с использованием продукции*** *Необходимо детально описать взаимосвязь между выявленной проблемой и потенциальным потребителем (см. пункты 9, 10 и 11)*	**1. Технические проблемы:** **Разработка эффективных алгоритмов:** создание алгоритмов, способных распознавать различные виды мошенничества и вредоносный контент, требует больших вычислительных ресурсов и постоянного совершенствования в связи с постоянным развитием мошеннических схем. Нейтрализация обхода фильтров мошенниками является постоянной гонкой вооружений. **Масштабируемость системы:** система должна быть способна обрабатывать огромное количество данных и запросов от пользователей, что требует значительных вычислительных мощностей и оптимизации архитектуры. **Интеграция с различными платформами:** необходимость интеграции с различными социальными сетями, мессенджерами, банковскими системами и другими платформами может создавать технические сложности и требовать согласования с владельцами этих платформ. **Защита от атак:** система должна быть защищена от хакерских атак и попыток взлома, что требует применения сложных механизмов защиты информации. **Обеспечение конфиденциальности данных:** сбор и обработка персональных данных пользователей требуют соблюдения строгих требований по защите конфиденциальности и соответствия законодательству о защите данных (например, GDPR). **2. Психолого-педагогические проблемы:** **Разработка эффективных обучающих материалов:** создание понятных и интересных материалов для обучения детей и подростков безопасному поведению в интернете требует специальных знаний в области психологии и педагогики. **Мотивация пользователей:** заставить детей и подростков использовать систему и следовать рекомендациям по безопасности может быть непросто. Система должна быть удобной и не вызывать отторжения. **Индивидуальный подход:** учитывать индивидуальные особенности детей и подростков разных возрастов и с разным уровнем цифрового развития. **Работа с родителями:** необходимость вовлечения родителей в процесс обучения и контроля за безопасностью детей в интернете. **3. Юридические и этические проблемы:** **Соблюдение законодательства:** необходимо строго соблюдать законодательство о защите персональных данных, авторских правах и других областях права. **Ответственность за ошибки системы:** вопросы ответственности за возможные ошибки системы и причиненный ими ущерб. **Доступ к информации:** сбалансировать необходимость защиты детей от нежелательного контента с правом на доступ к информации. **Проблема цензуры:** установление границ между безопасностью и свободой слова.

		4. Проблемы финансирования и ресурсного обеспечения: **Привлечение инвестиций:** поиск источников финансирования для разработки, внедрения и поддержки проекта. **Кадровые ресурсы:** необходимость привлечения квалифицированных специалистов в области информационной безопасности, психологии, педагогики, юриспруденции. **5. Проблемы распространения и внедрения:** **Доступность для всех пользователей:** обеспечение доступности системы для детей и подростков из разных социальных групп и регионов. **Создание партнерских отношений:** необходимость сотрудничества с образовательными учреждениями, родительскими организациями, правоохранительными органами и другими заинтересованными сторонами. **Постоянное обновление и совершенствование:** необходимость постоянного обновления системы в соответствии с развитием новых технологий и мошеннических схем. Преодоление всех этих проблем требует комплексного подхода и сотрудничества специалистов из разных областей. Успех проекта зависит от эффективного решения технических, психолого-педагогических, юридических и финансовых вопросов.
27	**Каким способом будет решена проблема*** *Необходимо описать детально, как именно ваши товары и услуги помогут потребителям справляться с проблемой*	**1. Технические решения:** **Разработка и внедрение усовершенствованных алгоритмов машинного обучения:** обучение моделей на больших данных о различных видах мошенничества, включая фишинг, социальную инженерию, кражу личных данных. Алгоритмы должны динамически адаптироваться к новым угрозам и мошенническим схемам. **Многофакторная аутентификация:** внедрение более надежных методов аутентификации (например, двухфакторной аутентификации) для защищенного доступа к платформам и аккаунтам. **Блокировка вредоносных ресурсов и контента:** разработка эффективных систем для автоматического распознавания и блокировки вредоносных веб-сайтов, ссылок, файлов и сообщений. **Система раннего оповещения:** разработка и внедрение систем, способных идентифицировать и сигнализировать об аномальной активности или подозрительных попытках мошенничества в режиме реального времени. **Интеграция с антивирусными программами и системами безопасности:** интеграция с существующими системами безопасности для расширения охвата и усиления защиты. **Прозрачные и понятные интерфейсы:** предоставление пользователям простой и интуитивно понятной информации о рисках и безопасном поведении в интернете. **2. Образовательные и просветительские подходы:** **Разработка и внедрение образовательных программ для детей и подростков:** обучение критическому мышлению, распознаванию мошеннических схем, безопасному поведению в онлайн-среде. Акцент на практических навыках.

		Использование интерактивных материалов (игр, тренингов, квестов): превращение обучения в увлекательный процесс, делающий безопасность в интернете актуальной и понятной для молодежи. **Партнерство с образовательными учреждениями и родительскими организациями:** вовлечение педагогов, родителей и других значимых лиц в процесс обучения безопасности. **Создание онлайн-платформ для обмена опытом и консультаций:** предоставление детям и подросткам возможности делиться опытом и получать поддержку от экспертов. **Информационная поддержка для родителей:** предоставление родителям инструментов и информации о том, как обеспечить безопасность своих детей в интернете. **3. Юридические и нормативные решения:** **Усиление ответственности за киберпреступность:** установление строгих наказаний за мошенничество в интернете, предоставление правоохранительным органам необходимых инструментов для расследования и пресечения противоправных действий. **Разработка и внедрение специальных законов:** законы, регулирующие онлайн-поведение детей и подростков и обеспечивающие их безопасность. **Совместные работы по развитию онлайн-безопасности:** международное сотрудничество для обмена опытом и передовыми практиками. **4. Социально-психологические решения:** **Поощрение позитивного онлайн-поведения:** стимулирование и поощрение безопасных и позитивных онлайн-взаимодействий. **Развитие навыков саморегуляции и стрессоустойчивости:** помощь подросткам в преодолении кибербуллинга и негативного контента. **Программы поддержки и защиты жертв мошенничества:** обеспечение доступности психологической помощи для тех, кто пострадал от онлайн-мошенничества. **5. Комплексный подход:** **Использование многоуровневой защиты:** сочетание технических, образовательных, юридических и социальных методов для достижения максимального результата. **Постоянное обновление и развитие проекта:** проекты должны быть динамичными, реагировать на новые угрозы и адаптироваться к меняющимся потребностям. **Сбор обратной связи:** регулярный сбор мнений пользователей, использование данных для совершенствования системы. Ключевой момент — не изолировать подростков от интернета, а помочь им пользоваться им безопасно и осознанно. Внедрение этих методов позволит постепенно снижать риски мошенничества и повышать уровень безопасности в цифровом пространстве.

28	**Оценка потенциала «рынка» и рентабельности бизнеса** *(для проектов, прошедших во второй этап акселерационной программы)* *Необходимо привести кратко обоснование сегмента и доли рынка, потенциальные возможности для масштабирования бизнеса, а также детально раскрыть информацию,* *указанную в пункте 16.*	**Потенциал рынка:** **Огромный и растущий:** количество детей и подростков, использующих интернет, постоянно увеличивается. Риски мошенничества и психологических проблем в онлайн-среде также растут. Это создает большой рынок для продуктов и сервисов, направленных на повышение безопасности. **Разнообразные ниши:** существует множество возможных направлений: приложения для родителей, инструменты для школ, сервисы для социальных сетей, продукты, ориентированные на конкретные возрастные группы. **Возможность монетизации:** платные подписки, партнерские программы, продажа данных о потреблении услуг, монетизация через рекламу, если это не повлияет на эффективность. Важно найти баланс между социальной миссией и коммерческими интересами. **Факторы, влияющие на рентабельность:** **Стоимость разработки и внедрения:** разработка эффективных алгоритмов, программного обеспечения и сервисов может быть очень дорогостоящей. **Расходы на маркетинг и продвижение:** привлечение целевой аудитории (детей, подростков и родителей) и убеждение их в необходимости пользоваться предлагаемыми сервисами требует значительных усилий и бюджета. **Поддержка и обслуживание:** необходимость технической поддержки, обновления ПО и постоянного улучшения продукта. **Конкурентная среда:** на рынке уже существуют аналогичные продукты, и конкуренция может быть высокой. **Доверие и репутация:** очень важно, чтобы предлагаемый продукт пользовался доверием детей, родителей и других заинтересованных сторон. **Социальная ответственность:** проект не должен восприниматься просто как коммерческая деятельность, важна этичная разработка и внедрение. **Рентабельность (оценка):** **Низкая или отсутствующая в традиционном смысле (краткосрочная):** основной акцент на социальном, а не на финансовом доходе. Первоначальные расходы на разработку и маркетинг будут велики. **Долгосрочная рентабельность (потенциально высокая):** постоянное развитие и расширение рынка, привлечение новых клиентов и партнеров, формирование положительного имиджа компании, возможные инвестиции в дальнейшее развитие. **Социальная рентабельность:** проект сможет снизить риски, улучшить жизнь многих людей и, возможно, предотвратить серьезные проблемы в будущем. **Вложения в будущее:** инвестиции в этот проект могут рассматриваться как долгосрочные вложения в будущее, улучшение жизни общества. **Заключение:** Рентабельность проекта, вероятно, будет низкой в краткосрочной перспективе, но его потенциал для получения долгосрочной прибыли и положительного социального влияния весьма высок. Главное — разработать продукт, который окажется

		полезным, безопасным и эффективным, и сосредоточиться на создании репутации надежного партнера в области онлайн-безопасности. Взгляд на проект с точки зрения социальной ответственности и долгосрочного развития, скорее всего, принесет наилучшие результаты. Необходимо найти баланс между коммерческими целями и миссией проекта, который призван защищать детей и подростков.
29	**План дальнейшего развития стартап-проекта** *(для проектов, прошедших во второй этап акселерационной программы)* *Укажите, какие шаги будут предприняты в течение 6-12 месяцев после завершения прохождения акселерационной программы, какие меры поддержки планируется привлечь*	**Постоянный мониторинг угроз:** постоянное отслеживание новых методов мошенничества и адаптация системы. **Обратная связь от пользователей:** регулярный сбор отзывов и их использование для улучшения продукта. **Командная работа и сотрудничество:** создание сильной команды специалистов с разными компетенциями (разработчики, дизайнеры, психологи, юристы). **Эффективная маркетинговая стратегия:** донесение информации о продукте до целевой аудитории. **Сотрудничество с партнерами:** создание партнерских отношений с организациями, занимающимися безопасностью детей в интернете.
