

УДК 338.46:004.9 DOI: 10.14451/1.249.81

Проектирование мобильного приложения для детей «Цифровой наставник»

© 2025 **Кобозева Елена Михайловна**

Кандидат экономических наук, доцент. Финансовый университет при Правительстве РФ, Краснодарский филиал, Россия, Краснодар.

E-mail: alena.cobozeva@yandex.ru

© 2025 **Молчан Алексей Сергеевич**

Доктор экономических наук, профессор. Финансовый университет при Правительстве РФ, Краснодарский филиал, Россия, Краснодар.

E-mail: alsmolchan@fa.ru

© 2025 **Иванова Алина Геннадьевна**

Студент. Финансовый университет при Правительстве РФ, Краснодарский филиал, Россия, Краснодар.

E-mail: ivanova.alin2017@yandex.ru

Ключевые слова: безопасность, кибербезопасность, цифровая безопасность, родительский контроль, кибербуллинг, мобильное приложение, риск, лендинг, онлайн.

В условиях стремительной цифровизации детской среды вопросы кибербезопасности приобретают критическую важность. Современные дети, активно использующие социальные сети и онлайн-платформы, ежедневно сталкиваются с угрозами: фейками (41%), мошенничеством (29%), кибербуллингом и зависимостью от интернета. Цель исследования заключается в разработке проекта мобильного приложения «Цифровой наставник», направленного на формирование безопасной цифровой среды для детей и подростков посредством интеграции технологических инструментов защиты и интерактивных образовательных методик. В статье отмечено, что приложение адресовано не только младшему поколению, но и их родителям и педагогам. Приложение создано с использованием инкрементной модели, что обеспечивает поэтапное внедрение функций с учетом обратной связи пользователей. Подчеркнуто, что инкрементная разработка позволит не только снизить риски за счет постепенного добавления и проверки функциональности, но создаст условия для органичного сочетания технических решений с образовательной составляющей. Охарактеризован целевой сегмент проектируемого приложения. Предложено концептуальное решение того, как проектируемое приложение будет отвечать на цифровые угрозы. Раскрыто понимание авторами статьи мобильного приложения как многофункционального инструмента. Перечислены и охарактеризованы структурные компоненты проектируемого приложения. Представлен спроектированный интерфейс лендинга мобильного приложения «Цифровой наставник». Сделан вывод о том, что успех внедрения проектируемого мобильного приложения будет зависеть от совместных усилий разработчиков, образовательных учреждений и родителей, для которых приложение станет связующим звеном в диалоге о кибербезопасности.

Современные дети погружены в цифровую среду с первых лет жизни. Социальные сети, мессенджеры и игровые платформы стали неотъемлемой частью их повседневности, а значит, вопросы цифровой безопасности перестают быть просто рекомендацией – они превращаются в необходимость. Однако осознанное взаимодействие с интернет-пространством требует не только технических ограничений, но и мягкого, адаптированного обучения.

Для комплексного решения этой задачи нами разработан проект мобильного приложения «Цифровой наставник». С одной стороны, оно даст родителям удобные инструменты для контроля онлайн-активности детей, включая фильтрацию контента. С другой – через интерактивные аудиосказки и игровые сценарии объяснит основы кибербезопасности на понятном детям языке. Такой подход не просто запрещает, а учит распознавать риски, формируя здоровые цифровые привычки с раннего возраста.

В результате «Цифровой наставник» станет не просто «родительским контролем», а связующим звеном между детьми и взрослыми в вопросах безопасного использования технологий – там, где ограничения дополняются доверием и пониманием.

Цель исследования заключается в разработке проекта мобильного приложения «Цифровой наставник», направленного на формирование безопасной цифровой среды для детей и подростков посредством интеграции технологических инструментов защиты и интерактивных образовательных методик. Разработка образовательного проекта мобильного приложения «Цифровой наставник» осуществлена с использованием инкрементной модели, что позволяет гармонично интегрировать технологические и педагогические аспекты проекта. Такой подход обеспечивает поэтапное внедрение функций: сначала создание базовых инструментов родительского контроля, затем добавление интерактивных обучающих модулей. Каждый этап разработки включает тестирование с участием ключевых пользовательских групп: родители оценивают

удобство настроек безопасности, а дети тестируют игровые сценарии и анимированные аудиосказки, что позволяет оперативно корректировать контент с учетом возрастных особенностей восприятия. Инкрементная разработка не только снижает риски за счет постепенного добавления и проверки функциональности, но и создает условия для органичного сочетания технических решений (фильтрация контента, настройки доступа) с образовательной составляющей, где запреты дополняются доступными объяснениями правил цифровой безопасности. Это позволяет сформировать у детей осознанное отношение к онлайн-пространству при постоянном участии родителей в этом процессе. В работе применялись данные исследований Альянса по защите детей в цифровой среде (распространение фейков, мошенничество, кибербуллинг), статистика МВД РФ о росте IT-преступлений среди несовершеннолетних, аналитика Лаборатории Касперского о снижении родительского контроля с возрастом детей, а также результаты локального опроса 50 родителей в Краснодаре, выявившего проблемы с несанкционированными покупками и осознанием детьми цифровых рисков.

Масштабный опрос Альянса по защите детей в цифровой среде охватил 2439 участников: подростков, родителей и педагогов из 15 регионов России. Результаты показали, что 9 из 10 детей ежедневно сталкиваются с онлайн-угрозами. Например, 41% опрошенных подростков признались, что неоднократно становились жертвами фейковых новостей, а 29% – попадали в ловушки интернет-мошенников. Родители и учителя выделили зависимость от игр и соцсетей как главную проблему: 60% семей и 42% педагогов отметили её негативное влияние на учебный процесс.

Треть подростков (30%) открыто заявили, что не знают, как противостоять фишинговым атакам или кибербуллингу. Только 24% из них используют блокировку подозрительных аккаунтов, в то время как родители видят выход в регулярных беседах: 35% матерей и 28% отцов проводят такие разговоры еженедельно. Интересно, что почти половина родителей (47%) и учителей

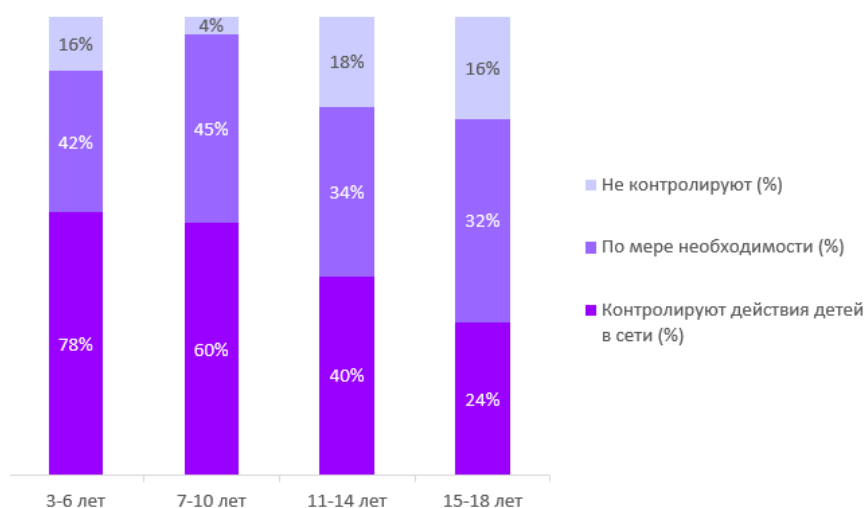


Рис. 1. Контроль за действиями детей в сети.

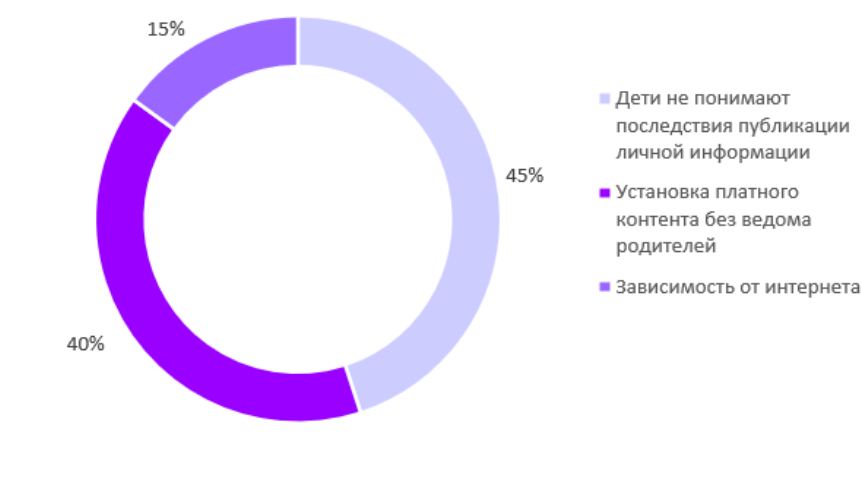


Рис. 2. Распределение ключевых проблем цифровой безопасности детей по данным опроса родителей.

(53%) сами недостаточно осведомлены о видах противоправного контента. При этом 48% педагогов и 47% родителей убеждены, что цифровые риски имеют как технологическую, так и психологическую природу, в то время как треть подростков склонны видеть в них в первую очередь психологическую угрозу. Отдельно отмечается запрос на усиление роли государства: более 40% взрослых участников опроса считают необходимым более активное вмешательство властей в обеспечение детской цифровой безопасности.

Аналитики Лаборатории Касперского выявили

парадокс: чем старше ребенок, тем меньше родители вовлечены в его цифровую жизнь. Если в младшей возрастной группе (3–6 лет) 78% мам и пап строго следят за онлайн-активностью, то к 15–18 годам этот показатель падает до 24% (рис. 1).

Эти данные подтверждают необходимость автоматизированных решений, которые помогают родителям сохранять баланс между свободой и безопасностью ребенка.

Согласно данным МВД РФ, за период с 2020 по 2023 год число компьютерных преступлений, совершенных несовершеннолетними, возросло

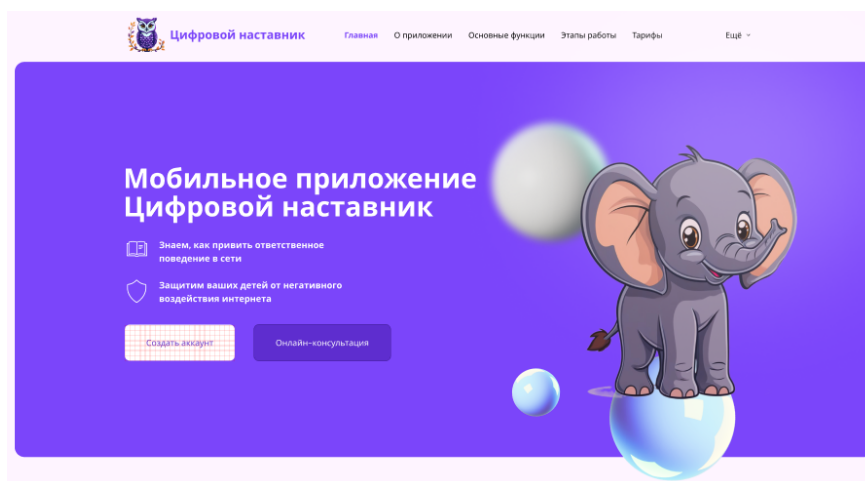


Рис. 3. Главная страница лендинг-сайта «Цифровой наставник».

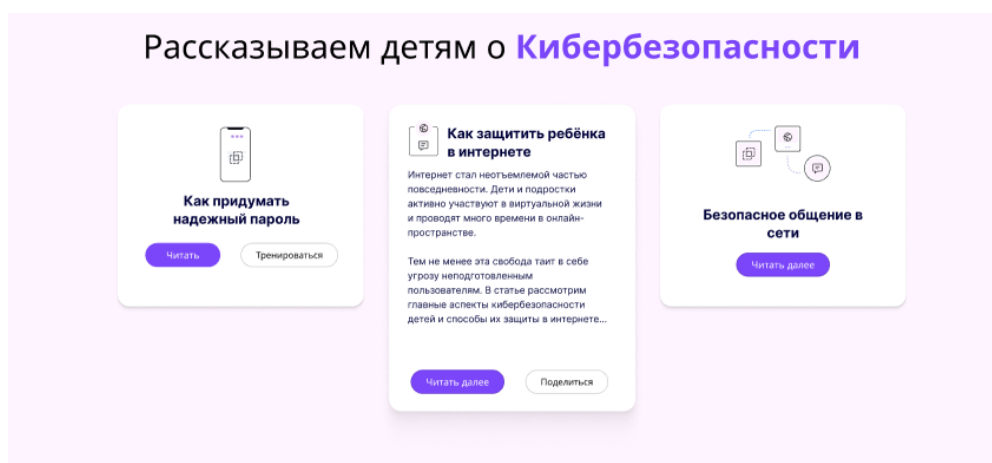


Рис. 4. Раздел статей на лендинг-сайте «Цифровой наставник».

в 74 раза. Если в 2020 году фиксировались единичные случаи (54 инцидента), то в 2023 году их количество достигло четырех тысяч. Специалисты объясняют эту тревожную динамику двумя ключевыми факторами: повсеместной цифровизацией подростковой среды и отсутствием эффективных механизмов мониторинга онлайн-активности молодежи. Как отмечают эксперты по кибербезопасности, современные подростки зачастую не осознают юридических последствий своих действий в сети. При этом существующие системы родительского контроля и образовательные программы пока не успевают адаптироваться к быстро меняющемуся ландшафту интернет-угроз.

Чтобы понять, с какими трудностями сталкиваются семьи в цифровой среде, мы пообщались

с 50 краснодарскими родителями школьников (рис. 2).

Оказалось, главные боли современных мам и пап можно объединить в три группы.

Первая тревога – детская беспечность. Больше половины участников опроса (45%) признались: их дети не до конца осознают, чем может обернуться выкладка фото, геолокации или других персональных данных в соцсетях. Как шутит одна мама: «Сын считает, что если поставить на аватарку кота вместо своего лица, то хакерам он уже неинтересен».

Ещё острее стоит вопрос незапланированных трат. 40 % респондентов сталкивались с ситуациями, когда ребёнок без спроса подключал платные услуги в играх или приложениях.

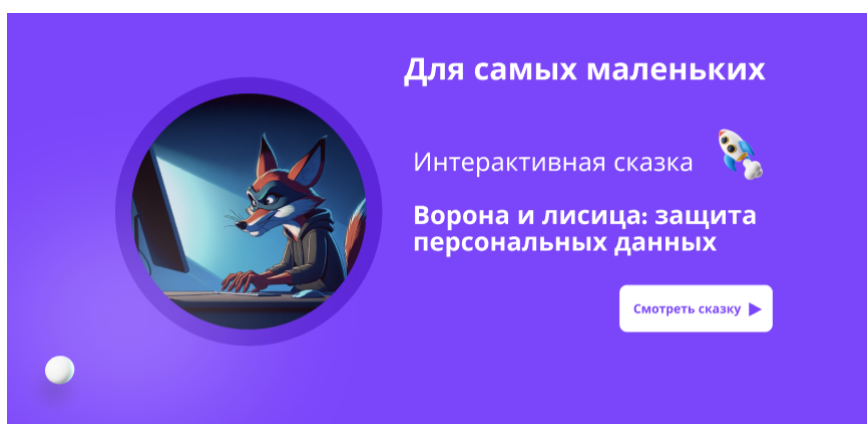


Рис. 5. Раздел лендинга с аудиосказкой по кибербезопасности.

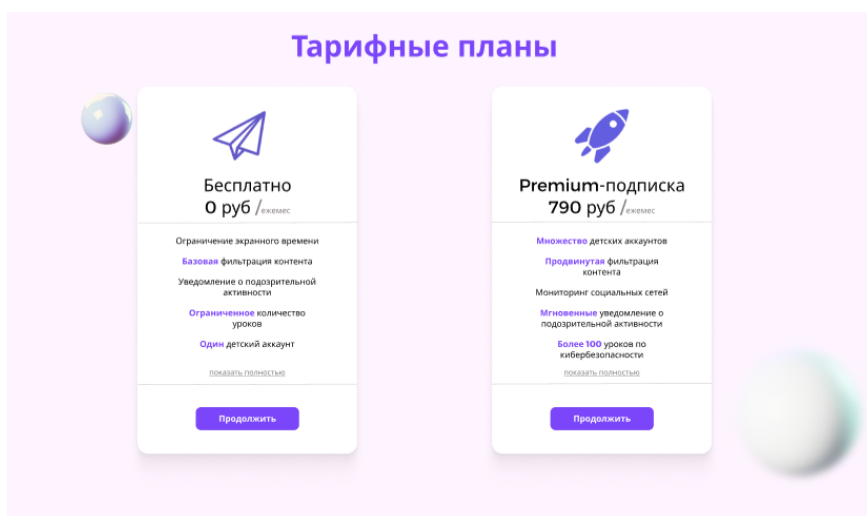


Рис. 6. Раздел лендинга с тарифными планами.

Третья проблема – растущая привязанность к гаджетам. Каждый третий родитель (15 %) отмечает, что дети буквально «прилипают» к экранам, заменяя реальное общение виртуальным. Учителя подтверждают: на переменах школьники чаще листают ленту TikTok, чем играют в догонялки.

Эти данные перекликаются с федеральной статистикой, убеждающей в том, что обычных запретов уже недостаточно. Нужны «умные» решения, которые не просто заблокируют опасный сайт, но и объяснят ребёнку, почему не стоит переходить по подозрительным ссылкам.

В результате опроса был составлен портрет пользователей мобильного приложения «Цифровой наставник» (табл. 1).

Из таблицы 1 можно четко выделить основные

группы пользователей, для которых разрабатывается приложение.

Во-первых, это родители 25–45 лет, находящиеся в состоянии между заботой и доверием. Представьте маму, которая замечает, что её десятилетний сын всё свободное время проводит в TikTok. Она волнуется: «А вдруг он увидит что-то травмирующее или начнёт общаться с незнакомцами?» Но как проверить, не превращаясь в «шпиона»? Или папу, который обнаружил, что дочка случайно оформила платную подписку в игре и теперь ему приходится разбираться с банком. Эти родители не хотят просто запрещать. Они мечтают о помощнике, который:

- покажет, куда и с кем заходит ребёнок в сети – без чтения личных переписок;

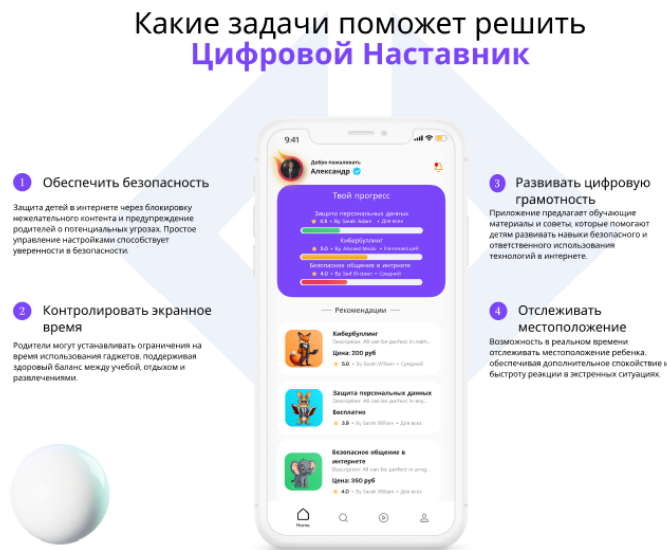


Рис. 7. Описание продукта «Цифровой наставник».

Таблица 1. Описание целевого сегмента мобильного приложения «Цифровой наставник».

Критерий	Родители и опекуны (25–45 лет)	Дети и подростки (8–16 лет)	Учителя и педагоги
Интересы	Безопасность детей, цифровая грамотность	Соцсети, игры, развлекательный контент	Образование, методики обучения
Потребности	Контроль онлайн-активности, фильтрация	Защита от кибербуллинга, мошенничества	Методические материалы
География	Россия	Россия	Россия
Образование	Среднее/высшее	Школьное	Высшее педагогическое
Основные задачи	Мониторинг, настройка ограничений	Обучение через игры и аудиосказки	Анализ уровня грамотности

- автоматически блокирует сайты с опасным контентом, как «невидимый щит»;
- подскажет, как объяснить подростку, почему не стоит выкладывать геолокацию в Instagram.

Вторая группа – дети 8–16 лет, поколение, растущее в лайках и стримах. Для них интернет – это мир друзей, мемов и бесконечных возможностей. Но в этом мире есть ловушки:

- одноклассник высмеял фото в чате класса;
- в игре предложили «бесплатные» кристаллы за номер карты родителей;
- в рекомендациях YouTube внезапно всплывают странные видео.

Скучные лекции о безопасности? Это как заставлять есть брокколи вместо бургера. Поэтому приложение превращает правила в приключения:

- квест, где нужно спасти персонажа от «троллей» в соцсетях;
- аудиосказка о том, как хакеры крадут пароли;
- мини-игра, где за правильные ответы открываются уровни.

Здесь нет нравоучений – только «прокачка» навыков выживания в цифровом мире.

Учителя и педагоги — третья группа. Эти люди с высшим образованием ищут способы объяснять школьникам, как вести себя в сети. Им нужны готовые уроки о кибербезопасности и инструменты, чтобы проверить, насколько ученики разбираются в цифровых угрозах. Скажем, тесты или задания, которые покажут, кто из детей легко ведется на фейки, а кто умеет защитить свои данные.

Современные вызовы цифрового мира потребуют комплексного подхода к безопасности детей в интернете. Проектируемое мобильное приложение видится нам как многофункциональный инструмент, который не только ограничит потенциально опасный контент, но и обучит детей правилам безопасного поведения в сети.

Особенности структуры приложения:

1. наличие серий интерактивных заданий, разработанных с учетом возрастных особенностей детей. Цель заданий — в игровой форме научить пользователей распознавать мошеннические схемы, защищать персональные данные и правильно реагировать на кибербуллинг;
2. использование анимированных аудиосказок и басен, которые в доступной форме объяснят основы цифровой гигиены;
3. для защиты от нежелательного контента реализация многоуровневой системы фильтрации, автоматически блокирующей доступ к опасным сайтам и приложениям. Родители смогут вручную настраивать ограничения, создавая безопасную цифровую среду для ребенка;
4. применение функции контроля экранного времени, позволяющей устанавливать разумные лимиты использования гаджетов;
5. отслеживание местоположения ребенка, с предоставлением родителям информации о его перемещениях в режиме реального времени;
6. внедрение инструментов для мониторинга онлайн-общения, которые смогут выявить потенциально опасные контакты;

7. наличие специальных разделов с рекомендациями по цифровому воспитанию и методическими материалами для родителей и педагогов. Это позволит взрослым лучше понимать цифровые угрозы и эффективнее помогать детям с ними справляться.

Нами был спроектирован интерфейс лендинга мобильного приложения «Цифровой наставник» (рис. 3).

Лендинг-сайт приложения «Цифровой наставник» представляет собой многофункциональную платформу, ориентированную на обеспечение безопасности детей в цифровом пространстве. Главная страница начинается с приветственного блока, где подчеркиваются ключевые преимущества приложения: обучение ответственному поведению в сети и защита от онлайн-угроз. Кнопки «Создать аккаунт» и «Онлайн-консультация» сразу привлекают внимание, предлагая пользователям начать взаимодействие с сервисом.

В разделе «Рассказываем детям о кибербезопасности» размещены образовательные материалы, такие как статьи о создании надежных паролей и безопасном общении в соцсетях (рис. 4).

Особый акцент сделан на аудиторию младшего возраста: для них предусмотрена интерактивная сказка «Ворона и лисица», которая в игровой форме объясняет важность защиты персональных данных (рис. 5).

Тарифная страница четко разделяет возможности бесплатной и премиум-версий: первая включает базовые функции контроля, а вторая расширяет их мониторингом соцсетей, продвинутой фильтрацией и доступом к обширной библиотеке уроков (рис. 6).

Дизайн лендинга выдержан в минималистичном стиле с акцентом на удобство навигации. Раздел «Основные функции» детально описывает, как приложение помогает родителям ограничивать экранное время, блокировать опасный контент и отслеживать местоположение ребенка (рис. 7).

Отдельный блок посвящен развитию цифровой грамотности через игровые сценарии и обучающие модули. Лендинг не только рекламирует

продукт, но и становится ресурсом для повышения осведомленности семей о киберрисках, объединяя технологии с образованием.

Таким образом, приложение станет надежным помощником в создании безопасной цифровой среды для подрастающего поколения, сочетая в себе функции защиты, контроля и обучения.

Проектируемое приложение «Цифровой наставник» предлагает инновационный ответ на вызовы цифровой эпохи, где традиционные методы родительского контроля уже недостаточны. Как показали исследования, современные дети сталкиваются с множеством угроз — от мошенничества до психологического давления, при этом 30% подростков не знают, как правильно реагировать на такие риски. Родители и педагоги, в свою очередь, часто не обладают достаточными знаниями. «Цифровой наставник» позволит преодолеть этот разрыв за счет:

1. Синтеза технологий и педагогики — сочетания фильтрации контента с игровым обучением.

2. Учета потребностей всех участников процесса — простые инструменты для родителей, интерактивные форматы для детей, методические материалы для учителей.
3. Гибкой разработки, позволяющей адаптировать функционал к быстро меняющемуся ландшафту угроз.

В перспективе внедрение подобных решений сможет не только сократить число инцидентов, но и сформировать у подрастающего поколения осознанное отношение к цифровому пространству. Успех реализации будет зависеть от совместных усилий разработчиков, образовательных учреждений и родителей, для которых приложение станет связующим звеном в диалоге о безопасности.

Таким образом, «Цифровой наставник» — это не просто инструмент контроля, а шаг к созданию культуры ответственного использования технологий, где запреты дополняются доверием, а угрозы превращаются в возможности для обучения.

Библиографический список

1. В РФ число совершенных детьми IT-преступлений выросло в 74 раза за четыре года. — URL: <https://tass.ru/proisshestiya/20626725> (дата обр. 19.06.2025).
2. Взрослые и дети в интернете: аналитический отчет. — URL: https://kids.kaspersky.ru/files/KIDS_Report_RU_2022_final_UPD.pdf (дата обр. 01.06.2025).
3. Захарова Е. Н., Шалатов В. В., Ордынская М. Е. Использование потенциала цифровых технологий при совместном продвижении туристского продукта // Московский экономический журнал. — 2024. — Т. 9, № 10. — С. 369–384.
4. Исследование показало, что более 90% подростков в РФ сталкиваются с цифровыми угрозами. — URL: <https://tass.ru/obshchestvo/18647327> (дата обр. 17.06.2025).
5. Лендинг «Цифровой наставник». — URL: <https://www.figma.com/proto/XmQf3Mppx7m6ZTd90ms7qE/Cифровой-наставник?node-id=2754-306&t=tgVMAky5jMdM0zm0-0&scaling=scale-down-width&content-scaling=fixed&page-id=0%3A1>.
6. Модели и методологии разработки ПО. — URL: <https://gb.ru/blog/modeli-i-metodologii-razrabotki-po/> (дата обр. 16.06.2025).
7. Прохорова В. В., Кобозева Е. М., Коломыц О. Н. Инновационные методы и формы обучения как определяющие факторы повышения эффективности качества образования // Образование и право. — 2016. — № 6. — С. 193–197.
8. Тадтаева В. В., Абисалова Л. М. Развитие бизнеса в цифровой экономике // Вестник Академии знаний. — 2023. — 3 (56). — С. 213–216.
9. The 'digitalisation trap' of Russian regions / A. S. Molchan [et al.] // International Journal of Technology, Policy and Management. — 2023. — Vol. 23, no. 1. — P. 2–.