Муниципальное бюджетное общеобразовательное учреждение «Школа № 24 с углубленным изучением отдельных предметов имени Героя Советского Союза Буркина М. И.» городского округа Самара

«УТВЕРЖДАЮ»

Директор МБОУ «Школа №24»

г.о. Самара

_____М.В. Романова

ПРОЕКТ
«КиберДружина» на базе МБОУ «Школа № 24» г. о. Самара

Выполнил:
Приходько Анастасия Викторовна
советник директора по воспитанию
и взаимодействию с детскими
общественными объединениями
МБОУ «Школа № 24» г. о. Самара

Самара, 2026 год

ПАСПОРТ ПРОЕКТА «КИБЕРДРУЖИНА»

Параметр	Описание
1. Название проекта	«КиберДружина: формирование безопасного цифрового пространства»
2. География проекта	Российская Федерация (с приоритетным запуском в Самарской области)
3. Цели проекта	Создание системы обеспечения информационной безопасности школьников через формирование сети киберволонтерских отрядов и повышение уровня цифровой грамотности молодежи
4. Задачи проекта	- Создание методической базы для работы киберволонтеров - Формирование сети школьных кибердружин - Организация систематического мониторинга интернет-пространства - Повышение уровня цифровой грамотности учащихся - Развитие навыков выявления и противодействия киберпреступности - Создание системы взаимодействия с правоохранительными органами
5. Актуальность проекта в контексте Послания Президента РФ	Соответствует задачам по формированию гармонично развитой личности и обеспечению информационной безопасности подрастающего поколения
6. Актуальность в рамках Указа Президента РФ №204	Способствует достижению целей в сфере образования по воспитанию социально ответственной личности
7. Актуальность в контексте стратегических документов	Соответствует Стратегии развития воспитания до 2025 года в части формирования безопасного информационного пространства
8. Социальная значимость	- Защита детей от негативного контента - Формирование иммунитета к киберманипуляциям - Развитие навыков критического мышления - Создание позитивной цифровой среды
9. Новизна проекта	- Системный подход к обеспечению кибербезопасности - Вовлечение школьников в активную профилактическую деятельность - Сочетание обучающих и практических задач - Создание единой информационной платформы

10. Краткое содержание проекта	- Обучение волонтеров основам кибербезопасности - Мониторинг интернет-пространства - Проведение профилактических мероприятий - Взаимодействие с компетентными органами - Создание позитивного цифрового контента
11. Сроки реализации	Подготовительный этап: 3 месяца Основной этап: 6 месяцев Заключительный этап: 2 месяца
12. Команда проекта	Руководитель проекта: - Куратор от образовательного учреждения - Педагоги-организаторы - Педагоги дополнительного образования - Советник директора по воспитанию и взаимодействию с детскими общественными объединениями - Эксперты в сфере IT-безопасности
13. Поддержка проекта	Министерство образования УМВД Роскомнадзор IT-компании Кибер школы Общественные организации
14. Ожидаемые результаты	- Создание сети школьных кибердружин - Повышение уровня цифровой грамотности участников - Снижение количества случаев кибербуллинга - Выявление и блокировка противоправного контента - Формирование активной гражданской позиции
15. Система контроля качества	Регулярный мониторинг деятельности Оценка уровня знаний участников Анализ результативности мероприятий Сбор обратной связи
16. Информационное сопровождение	Создание официального паблика в социальных сетях, мессенджере MAX Публикация материалов в СМИ Организация пресс-мероприятий
17. Бюджет проекта	Материально-техническое обеспечение Методическое сопровождение Информационное обеспечение Организационные расходы Оплата стимулирующих выплат руководителю проекта

	Оплата стимулирующих выплат куратору реализующего проект
18. Перспективы развития	Расширение географии проекта Создание межрегиональной сети Разработка мобильного приложения Интеграция с государственными системами мониторинга

ДОПОЛНИТЕЛЬНЫЕ РАЗДЕЛЫ

План реализации проекта:

- Разработка методических материалов
- Формирование команд кибердружин
- Обучение участников
- Запуск мониторинга
- Проведение профилактических мероприятий
- Подведение итогов

Система оценки эффективности:

- Количество выявленных нарушений
- Число обученных участников
- Охват профилактическими мероприятиями
- Количество заблокированного противоправного контента

Риски проекта:

- Технические сбои
- Недостаточное финансирование
- Низкая вовлеченность участников
- Изменение законодательства

Меры по минимизации рисков:

- Создание резервных копий данных
- Поиск дополнительных источников финансирования
- Мотивационные механизмы для участников
- Регулярный мониторинг законодательства

1. ВВЕДЕНИЕ

1.1. Актуальность выбранной темы

В эпоху цифровизации интернет стал неотъемлемой частью жизни школьников. Однако вместе с возможностями он несёт серьёзные угрозы: кибербуллинг, фишинг, мошенничество, доступ к противоправному контенту. По данным исследований, более 60% подростков сталкиваются с киберугрозами, но лишь немногие умеют адекватно реагировать. Проект «КиберДружина» призван сформировать у школьников навыки безопасного поведения в интернете и вовлечь их в активную профилактику киберпреступности.

1.2. Обоснование возникшей проблемы

Проблема кибербезопасности школьников обусловлена:

- низким уровнем цифровой грамотности учащихся;
- отсутствием системных мер по защите детей в интернете на уровне образовательных учреждений;
- ростом числа киберпреступлений, направленных на несовершеннолетних;
- недостаточной координацией между школами, правоохранительными органами и IT-специалистами в сфере профилактики.

1.3. Определение конкретной задачи и её формулировка

Задача проекта — создать сеть школьных «КиберДружин», которые будут:

- обучаться основам кибербезопасности;
- мониторить интернет-пространство на предмет противоправного контента;
- проводить просветительские мероприятия для сверстников и родителей;
- взаимодействовать с правоохранительными органами и IT-компаниями.

1.4. Цели и задачи

Цель: формирование безопасной цифровой среды для школьников через создание сети «КиберДружин» и повышение уровня киберграмотности.

Задачи:

1. Обучить 100+ школьников основам кибербезопасности.
2. Создать методический комплекс по кибербезопасности для школ.
3. Организовать регулярный мониторинг интернет-пространства (выявление 50+ случаев противоправного контента в семестр).
4. Провести 10+ просветительских мероприятий (лекции, квесты, вебинары).
5. Сформировать сеть из 10 школьных «КиберДружин» в регионе.
6. Разработать мобильное приложение для отчётности и обмена опытом.

1.5. Требования к проекту

- соответствие ФГОС и стратегическим документам в сфере образования;
- практическая значимость и возможность масштабирования;
- вовлечение всех участников образовательного процесса (учащиеся, педагоги, родители);
- интеграция с государственными системами мониторинга (Роскомнадзор, МВД);
- использование современных IT-технологий (аналитика данных, чат-боты).

2. ГЛАВЫ ОСНОВНОЙ ЧАСТИ

2.1. Немного истории: кибербезопасность в школе

Первые программы по кибербезопасности для школьников появились в 2010-х годах. Однако они были фрагментарными и не охватывали все аспекты проблемы. Сегодня требуется системный подход, объединяющий обучение, практику и профилактику. Проект «КиберДружина» продолжает эту традицию, адаптируя её к современным вызовам.

2.2. Выбор инструментов, приспособлений, оборудования

Для реализации проекта необходимы:

- **программные средства:** антивирусное ПО, системы анализа трафика, чат-боты для обучения;
- **образовательные ресурсы:** онлайн-курсы, тесты, интерактивные плакаты;
- **платформа для коммуникации:** Telegram-канал, сайт проекта, форум;
- **оборудование:** компьютеры с доступом в интернет, проекторы для презентаций;
- **методические материалы:** учебники, рабочие тетради, сценарии мероприятий.

2.3. Технологическая часть проекта

Этап 1. Подготовка (1 месяц)

- формирование команды проекта (руководитель, кураторы, волонтёры);
- разработка программы обучения и методических материалов;
- заключение соглашений с партнёрами (МВД, Роскомнадзор, IT-компании).

Этап 2. Обучение (2 месяца)

- курс «Основы кибербезопасности» (10 занятий);
- тренинги по выявлению фишинговых сайтов и мошеннических схем;
- мастер-классы по работе с аналитическими инструментами.

Этап 3. Практическая деятельность (5 месяцев)

- мониторинг соцсетей и форумов на предмет противоправного контента;
- анализ и передача данных в компетентные органы;
- проведение квестов и викторин по кибербезопасности;
- создание видеороликов и инфографики о безопасных практиках.

Этап 4. Разработка мобильного приложения (3 месяца)

- проектирование интерфейса и логики работы;
- программирование (использование Python, Flutter);
- тестирование и внедрение.

2.4. Изготовление «продукта» проекта

Итоговыми продуктами проекта станут:

- мобильное приложение «КиберДружина» (отчётность, чат, тесты);
- методический комплекс «Кибербезопасность для школьников»;
- серия образовательных видеороликов;
- карта киберугроз региона (визуализация данных мониторинга).

3. Оценка работы

Критерии оценки эффективности:

- количество обученных школьников (целевой показатель — 100 человек);
- число выявленных случаев противоправного контента (не менее 50 за семестр);
- охват просветительскими мероприятиями (не менее 500 человек);
- активность в социальных сетях (рост подписчиков на 30% за полгода);
- отзывы партнёров и участников (анкеты, интервью).

Методы оценки:

- анкетирование участников до и после проекта;
- анализ статистических данных (отчёты, метрики приложения);
- экспертная оценка специалистов в сфере IT-безопасности;
- мониторинг СМИ и социальных сетей (упоминание проекта).

4. Самооценка

Сильные стороны проекта:

- инновационный подход (сочетание обучения и практики);
- междисциплинарность (объединение IT, педагогики, юриспруденции);
- практическая значимость (реальные кейсы, взаимодействие с органами);
- потенциал масштабирования (возможность внедрения в других регионах).

Слабые стороны:

- необходимость обучения педагогов работе с IT-инструментами;
- зависимость от технической инфраструктуры школ.

Сроки реализации: 12 месяцев (с возможностью продления)

Целевая аудитория:

- Учащиеся 7-11 классов (12-17 лет)
- Педагоги образовательных учреждений
- Родители школьников
- **Специалисты в сфере IT-безопасности**

География реализации: Самарская область (с перспективой масштабирования)

5. Планируемые улучшения:

- разработка онлайн-курса для педагогов;
- привлечение спонсоров для обеспечения оборудованием;
- создание системы мотивации для участников (сертификаты, грамоты).

6. Перспективы развития:

- расширение сети «КиберДружин» до 20 школ;
- интеграция с региональными программами по кибербезопасности;
- разработка модуля по киберэтике и цифровому этикету;
- участие в федеральных конкурсах и грантовых программах.

7. Ожидаемые результаты:

- повышение уровня киберграмотности школьников на 30%;
- снижение случаев кибербуллинга в школах-участниках на 20%;
- формирование сообщества экспертов-школьников в сфере кибербезопасности;
- создание устойчивой системы профилактики киберпреступлений среди несовершеннолетних.

8. Механизм оценки эффективности

Критерии оценки:

- Количество выявленных нарушений
- Уровень знаний участников (тестирование)
- Активность в социальных сетях
- Отзывы участников и партнеров

9. Бюджет проекта

Распределение средств:

- Материально-техническое обеспечение: 200 000 руб.
- Методическое сопровождение: 300 000 руб.
- Информационное обеспечение: 100 000 руб.
- Организационные расходы: 100 000 руб.
- Оплата стимулирующих выплат: 600 000 руб.
- Итого: 1 300 000 рублей

10. Команда проекта

Ключевые специалисты:

- Руководитель проекта (опыт в IT и педагогике)
- Методист по кибербезопасности
- IT-специалист
- Психолог
- Координатор по работе с партнерами

11. Риски и их минимизация

Основные риски:

- Технические сбои
- Низкая вовлеченность участников
- Изменение законодательства

Меры минимизации:

- Создание резервных копий
- Система мотивации участников
- Регулярный мониторинг изменений

12. Перспективы развития

Планы развития:

- Расширение географии проекта
- Создание межрегиональной сети
- Разработка дополнительных модулей
- Интеграция с государственными системами

13. Партнеры проекта

Потенциальные партнеры:

- Министерство образования
- УМВД
- Роскомнадзор
- IT-компании
- Общественные организации

14. План мониторинга

Система контроля

- Регулярная отчетность
- Промежуточная оценка
- Финальный аудит

Инструменты оценки

- Анкетирование
- Тестирование
- Анализ статистики
- Экспертная оценка

15. Вспомогательные материалы

- Программа обучения
- План мероприятий
- Формы отчетности
- Методические рекомендации
- Примеры успешных кейсов

16. Планы масштабирования

- Расширение географии
- Создание межрегиональной сети
- Разработка дополнительных модулей
- Интеграция с государственными системами

Вывод: проект «КиберДружина» — это системный подход к решению проблемы кибербезопасности школьников, сочетающий обучение, практику и профилактику. Его реализация позволит создать безопасную цифровую среду, воспитать поколение IT-грамотных граждан и предотвратить множество киберпреступлений.