Муниципальное бюджетное общеобразовательное учреждение г. Астрахани
"Средняя общеобразовательная школа № 6"

| РАССМОТРЕНО | ПРИНЯТО | УТВЕРЖДЕНО |
|---|---|---|
| Методическим советом | Педагогическим советом | Директором |
| Протокол №4 | Протокол №15 | Кагиян А.Э. |
| от 29.05.2026 | от 25.06.2026 | Приказ №01 |
| | | от 01.09.2026 |

Рабочая программа внеурочной деятельности

Цифровая безопасность. Что можно, а что нет.

10-11 классы

на 2026 – 2027 учебный год

Учитель: Григорьева И.В.

город Астрахань

2026

## 1. Пояснительная записка

**Цель курса** — сформировать у обучающихся ответственное поведение в цифровой среде: умение различать разрешённое и запрещённое, осознавать последствия своих действий в сети и нести за них ответственность.

**Задачи:**

- познакомить с правами и обязанностями пользователя в цифровой среде;
- сформировать навыки безопасного общения, поиска и проверки информации;
- показать границы дозволенного: персональные данные, авторское право, кибербуллинг, мошенничество;
- познакомить с видами юридической ответственности за проступки в сети;
- отработать практические навыки на кейсах и проектах.

**Аудитория:** обучающиеся 10-11 классов. Занятия — 1 час в неделю, всего 34 часа.

**Формы работы:** беседы и дискуссии, разбор кейсов, практикумы за компьютером, ролевые и деловые игры, групповой проект, квизы и тесты.

## 2. Планируемые результаты

Обучающиеся будут **знать**:

- понятия «цифровой след», «персональные данные», «цифровая репутация»;
- основные права и обязанности пользователя сети;
- какие действия в сети запрещены законом и какая ответственность за них предусмотрена;
- правила безопасного использования сервисов, платежей и ИИ-помощников.

Обучающиеся будут **уметь**:

- проверять достоверность информации и распознавать фейки;
- настраивать приватность аккаунтов и защищать персональные данные;
- отличать законное использование чужого контента от нарушения авторских прав;
- действовать при столкновении с кибербуллингом, мошенничеством, опасным контентом;
- оценивать свои поступки в сети с точки зрения «можно / нельзя / последствия».

## 3. Содержание курса и тематический план

### Раздел 1. Цифровое общество и ответственность (3 ч)

| № | Тема | Содержание |
|---|---|---|
| 1 | Вводное занятие. Цифровой мир: возможности и риски | Правила работы с техникой. Обзор курса. Дискуссия «Мой цифровой день» |
| 2 | Цифровой след и репутация | Что остаётся в сети навсегда, кто это видит, как это влияет на учёбу и работу |
| 3 | Права и обязанности пользователя | Свобода слова и её границы. Права автора, право на изображение, право на неприкосновенность частной жизни |

**Раздел 2. Что можно: ответственные практики (10 ч)**

| № | Тема | Содержание |
|---|---|---|
| 4 | Эффективный поиск информации | Поисковые операторы, выбор источников, оценка надёжности сайта |
| 5 | Фактчекинг | Признаки фейка, перекрёстная проверка, сервисы проверки фактов |
| 6 | Сетевой этикет | Общение в мессенджерах и соцсетях: тон, конфликт, выход из спора |
| 7 | Деловая переписка | Электронное письмо, резюме, обращение в организацию |
| 8 | Госуслуги и цифровые сервисы | Регистрация, безопасность аккаунта, что удобно делать онлайн |
| 9 | Авторское право: когда чужое можно | Легальное использование: цитирование, лицензии Creative Commons, бесплатные библиотеки |
| 10 | ИИ-помощники в учёбе | Что можно: справка, идеи, проверка. Что нельзя: выдавать чужое за своё, доверять без проверки |
| 11 | Безопасные покупки и платежи | Признаки надёжного магазина, защищённые платежи, что нельзя сообщать никому |
| 12 | Фото, видео и согласие | Право на изображение гражданина: когда публиковать чужое фото можно, а когда нельзя |
| 13 | Практикум по разделу 2 | Тест + разбор кейсов «легально/нелегально» |

**Раздел 3. Что нельзя: запреты и ответственность (12 ч)**

| № | Тема | Содержание |
|---|---|---|
| 14 | Персональные данные: что нельзя публиковать | ФЗ-152: паспорт, адрес, геометки, документы. Практика: проверяем свои публикации |
| 15 | Пароли и доступы | Почему пароли нельзя передавать, двухфакторная аутентификация, менеджеры паролей |
| 16 | Кибербуллинг | Как выглядит травля в сети, роли участников, алгоритм действий |
| 17 | Ответственность за травлю | Гражданско-правовая, административная, уголовная ответственность; куда обращаться |
| 18 | Фейки, дипфейки и репосты | Почему репост недостоверного или противоправного материала — не «просто лайк» |
| 19 | Мошенничество и социальная инженерия | Фишинг, скам, «бесплатные подарки», звонки «из банка». Практикум: распознай обман |
| 20 | Вредоносное ПО | Вирусы и трояны: что нельзя устанавливать и распространять, последствия |
| 21 | Пиратство | Скачивание и раздача контента: авторские права, ответственность за нарушение |
| 22 | Несанкционированный доступ | «Взлом ради интереса» — это преступление. Границы хакерства и легальные профессии |
| 23 | Деструктивный и запрещённый контент | Что запрещено публиковать и распространять; как реагировать и куда сообщать |

| № | Тема | Содержание |
|---|---|---|
| 24 | Возраст ответственности | С 14, 16, 18 лет: что грозит. Кейс-разбор реальных (обезличенных) ситуаций |
| 25 | Практикум по разделу 3 | Кейсовый тест «Можно или нельзя?» + мини-суд над ситуацией |

**Раздел 4. Практикум и проект (6 ч)**

| № | Тема | Содержание |
|---|---|---|
| 26 | Аудит цифрового следа | Проверяем себя: поиск своего имени, чистка публикаций |
| 27 | Настройки приватности | Настраиваем аккаунты соцсетей и мессенджеров |
| 28 | Кейс-игра «Что можно, а что нельзя?» | Групповая игра с разбором спорных ситуаций |
| 29–31 | Групповой проект | Разработка памятки, буклета или короткого видео «Правила цифровой ответственности» для класса |

**Раздел 5. Итоги (3 ч)**

| № | Тема | Содержание |
|---|---|---|
| 32 | Защита проектов | Презентация памяток и роликов |
| 33 | Итоговый квиз | Командная игра «Цифровой ответственный гражданин» |
| 34 | Итоговое занятие | Рефлексия, чек-лист цифрового ответственного поведения |

**4. Формы контроля**

Текущий — наблюдение, устные опросы, мини-тесты после разделов 2 и 3. Итоговый — защита группового проекта и итоговый квиз. Оценку удобно вести в баллах: участие в кейсах, практических работах и проекте.

**5. Материально-техническое обеспечение**

Кабинет с компьютерами или ноутбуками с выходом в интернет, проектор, доступ к сервисам проверки фактов и материалам по цифровой грамотности (например, задания «Урока цифры», материалы порталов по информационной безопасности детей).

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 187598946305064097190711460653033521119524543986

Владелец Кагиян Армен Эдуардович

Действителен С 09.09.2026 по 09.09.2027