

Рассмотрена на заседании ШМО  
Протокол № 1  
от «26» август 2024 г.

Согласовано  
зам. директора по УР

Утверждена  
приказом №172 от 26.08.2024  
Директор МБОУ «Староромашкинская СОШ»  
Сабитов Р.Ш.



## **РАБОЧАЯ ПРОГРАММА**

**элективного курса по информатике «Информационная безопасность»**

**Муниципального бюджетного общеобразовательного учреждения «Староромашкинская СОШ» Чистопольского  
муниципального района Республики Татарстан  
на уровень среднего общего образования**

Принята на заседании  
педагогического совета  
протокол № 1  
от 26 августа 2024 г.

## **ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**Рабочая программа по информатике составлена на основе следующих нормативных документов:**

1. ФЗ «Об образовании в Российской Федерации» № 273-ФЗ от 29.12.2012г.;
2. Федеральная образовательная программа среднего общего образования. (приказ Министерства просвещения Российской Федерации от 18.05.2023 № 371 "Об утверждении федеральной образовательной программы среднего общего образования" (Зарегистрирован 12.07.2023 № 74228);
3. Учебного плана МБОУ «Староромашкинская средняя общеобразовательная школа» 2024/2025 учебного года, утверждённого приказом №172 от 26.08.2024 года;
4. Положение о рабочих программах МБОУ «Староромашкинская СОШ», утвержденного приказом № 161 от 26.08.2023 г.;
5. Рабочей программы воспитания в МБОУ «Староромашкинская СОШ» на 2023-2028 годы приказ № 160 от 26.08.2023 года.

## 1. Планируемые результаты освоения элективного курса

Планируется достижение некоторых предметных результатов, актуальных для данного курса в интеграции с предметами: «Обществознание» и «Информатика» (раздел «Социальная информатика») для 11 класса например:

- формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации;
- освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам;
- формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

В результате освоения курса учащиеся будут

*знать и понимать:*

- источники угроз, поступающих на мобильный телефон, планшет, компьютер
- виды угроз
- проблемные ситуации в сетевом взаимодействии
- правила поведения для защиты от угроз
- правила поведения в проблемных ситуациях
- этикет сетевого взаимодействия
- роль близких людей, семьи для устранения проблем и угроз в сети Интернет и мобильной телефонной связи
- телефоны экстренных служб
- личные данные
- позитивный Интернет;

*уметь:*

- правильно использовать аватар с учетом защиты личных данных
- формировать и использовать пароль
- использовать код защиты телефона
- регистрироваться на сайтах без распространения личных данных
- вести общение в социальной сети или в мессенджере сообщений

- правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.)
- отключиться от нежелательных контактов использовать позитивный Интернет.

## 2. Содержание элективного курса

Главная цель курса — обеспечить социальные аспекты информационной безопасности в воспитании школьников в условиях цифрового мира, включение цифровой гигиены в контекст воспитания детей на регулярной основе, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов обучения и воспитания детей.

Задачи курса по информационной безопасности детей:

- формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт гуманных, уважительных отношений с окружающими;
- создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствий деструктивных действий, формирования мотивации
- к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;
- формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности экстремизма во всех его формах в сети Интернет;
- мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;
- научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, осознавать ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Курс для учащихся 10–11 классов включает изучение правовой грамоты в сфере информационной безопасности, включая основные виды юридической ответственности (уголовной, административной и гражданско-правовой) за преступления и проступки в области информационной безопасности.

Полученные знания помогут избежать ошибок и опасностей, которые подстерегают нас в информационном мире, а также ответственно работать в информационном пространстве с соблюдением норм права. Важную часть курса составляет изучение правовой информации об основных законодательных актах в сфере информационной безопасности, а также материалов, размещенных на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, на основании которых рекомендуется проектная работа, например составление информационной листовки, буклета по темам:

- персональные данные <http://rkn.gov.ru/personal-data/protection-of-the-innocent/>
- контроль и надзор в сфере информационных технологий <http://rkn.gov.ru/it/control/>
- контроль и надзор в сфере связи <http://rkn.gov.ru/communication/control/>
- контроль и надзор в сфере массовых коммуникаций <http://rkn.gov.ru/mass-communications/>

### 3. Тематическое планирование

#### 11 класс

№ п/п	Разделы	Кол-во часов	Количество часов НРЭО/РРЯ
1	Правовые основы информационной безопасности	5	-
2	Законодательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности	7	-
3	Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности	12	-
4	Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности	29	-
5	Практика применения правил и норм информационной безопасности	14	-
	Итого	67	-