МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ -

СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 25 ИМЕНИ В.Г. ФЕОФАНОВА

ПРИНЯТО
на педагогическом совете
Протокол № 25 от 24.06.2026

УТВЕРЖДАЮ
Директор МАОУ-СОШ №25
_____ О.А. Добычина
Приказ № 576-о от 01.07.2026

РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

для основного общего образования (5 классы)

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Актуальность курса

Современный этап развития общества характеризуется стремительным ростом объёмов информации и расширением цифровой среды, в которую с раннего возраста погружается каждый школьник. Согласно Стратегии государственной культурной политики на период до 2030 года (утверждена распоряжением Правительства РФ от 11 сентября 2024 г. № 2501-р), одной из приоритетных задач является формирование информационной грамотности граждан, обеспечивающей гармоничное развитие личности.

Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» закрепляют особые требования к обеспечению безопасности несовершеннолетних в информационном пространстве. В условиях роста угроз кибербуллинга, фишинга, вовлечения несовершеннолетних в деструктивные сетевые сообщества и распространения недостоверной информации задача целенаправленного формирования у обучающихся навыков безопасного поведения в цифровой среде приобретает особую значимость.

Программа курса «Информационная безопасность» для 5 класса является логическим продолжением и конкретизацией программы «Основы информационной культуры школьников» и ориентирована на формирование у обучающихся базовых представлений о безопасности личности в информационном обществе, практических навыков защиты персональных данных и критического отношения к информации.

1.2. Цель курса

Формирование у обучающихся 5 класса основ информационной безопасности, культуры безопасного и ответственного поведения в цифровой среде, навыков защиты персональной информации и критического восприятия информации.

1.3. Задачи курса

- сформировать представление о понятиях «информация», «информационная безопасность», «персональные данные», «цифровой след»;
- ознакомить обучающихся с основными видами угроз информационной безопасности в сети Интернет (кибербуллинг, фишинг, вредоносные программы, недостоверная информация);

- сформировать навыки безопасного поведения при работе с приложениями на различных устройствах и в сети Интернет;
- обучить базовым нормам информационной этики и права, сетевому этикету;
- сформировать практические умения защиты персональной информации (создание надёжных паролей, распознавание мошеннических сообщений);
- развивать критическое мышление и навыки оценки достоверности информации;
- воспитывать ответственное отношение к собственному цифровому следу и уважение к правам других пользователей.

1.4. Место курса в образовательном процессе

Программа рассчитана на 34 академических часа в течение одного учебного года (1 час в неделю) и реализуется в рамках внеурочной деятельности для обучающихся 5 классов. Программа может реализовываться как в параллели 5 классов, так и в разновозрастной группе. Формы проведения занятий: беседы, практикумы, практические занятия, проектная деятельность, экскурсия (виртуальная) в цифровую среду.

2. ОБЩАЯ ХАРАКТЕРИСТИКА КУРСА

Курс имеет практико-ориентированный характер и построен на принципах системно-деятельностного подхода. Содержание курса структурировано по пяти разделам:

1. **«Человек в мире информации»** — введение в понятие информации, коммуникации, информационной безопасности как части общей культуры личности.
2. **«Угрозы информационной безопасности»** — изучение основных видов угроз в цифровой среде.
3. **«Персональные данные и цифровой след»** — формирование навыков защиты личной информации.
4. **«Информационная этика и право»** — освоение норм сетевого этикета и правовых основ работы с информацией.
5. **«Проектная деятельность»** — обобщение и практическое применение полученных знаний.

Значительное внимание уделяется практическим формам работы: разбору кейсов, моделированию ситуаций, созданию памяток и проектов, что обеспечивает формирование у обучающихся устойчивых навыков безопасного поведения.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

3.1. Личностные результаты

Гражданское воспитание:

- готовность к выполнению обязанностей гражданина и реализации его прав, уважение прав, свобод и законных интересов других людей;
- неприятие любых форм экстремизма, дискриминации, в том числе в сети Интернет;
- представление об основных правах, свободах и обязанностях гражданина в цифровом пространстве.

Патриотическое воспитание:

- осознание российской гражданской идентичности, проявление интереса к культуре и истории Российской Федерации;
- ценностное отношение к достижениям своей Родины, в том числе в сфере информационных технологий.

Духовно-нравственное воспитание:

- ориентация на моральные ценности и нормы в ситуациях нравственного выбора в цифровой среде;
- готовность оценивать своё поведение и поступки, а также поведение других людей с позиции нравственных и правовых норм;
- активное неприятие асоциальных поступков, в том числе кибербуллинга.

Физическое воспитание, формирование культуры здоровья и эмоционального благополучия:

- осознание ценности жизни, ответственное отношение к своему здоровью;
- соблюдение правил безопасности, в том числе навыков безопасного поведения в интернет-среде;
- способность адаптироваться к стрессовым ситуациям и меняющимся информационным условиям;
- умение осознавать эмоциональное состояние себя и других, управлять собственным эмоциональным состоянием.

Трудовое воспитание:

- установка на активное участие в решении практических задач;
- интерес к практическому изучению профессий, связанных с информационными технологиями и информационной безопасностью.

Экологическое воспитание:

- осознание своей роли как гражданина и потребителя в условиях взаимосвязи природной, технологической и социальной сред.

Ценности научного познания:

- овладение языковой и читательской культурой как средством познания мира;
- овладение основными навыками исследовательской деятельности.

Адаптация обучающегося к изменяющимся условиям социальной и природной среды:

- освоение социального опыта, основных социальных ролей, норм и правил общественного поведения;
- способность действовать в условиях неопределённости, повышать уровень своей компетентности через практическую деятельность.

3.2. Метапредметные результаты

Познавательные универсальные учебные действия:

- выявлять и характеризовать существенные признаки объектов (явлений);
- выявлять дефициты информации, данных, необходимых для решения поставленной задачи;
- выявлять причинно-следственные связи при изучении явлений и процессов;
- делать выводы с использованием дедуктивных и индуктивных умозаключений;
- применять различные методы, инструменты и запросы при поиске и отборе информации;
- выбирать, анализировать, систематизировать и интерпретировать информацию различных видов и форм представления;
- находить сходные аргументы (подтверждающие или опровергающие одну и ту же идею) в различных информационных источниках;
- самостоятельно выбирать оптимальную форму представления информации;
- оценивать надёжность информации по критериям, предложенным педагогическим работником или сформулированным самостоятельно;
- эффективно запоминать и систематизировать информацию.

Коммуникативные универсальные учебные действия:

- формулировать суждения, выражать эмоции в соответствии с целями и условиями общения;
- выражать себя (свою точку зрения) в устных и письменных текстах;
- распознавать невербальные средства общения, понимать значение социальных знаков, знать и распознавать предпосылки конфликтных ситуаций и смягчать конфликты, вести переговоры;

- понимать намерения других, проявлять уважительное отношение к собеседнику и в корректной форме формулировать свои возражения;
- в ходе диалога и (или) дискуссии задавать вопросы по существу обсуждаемой темы;
- сопоставлять свои суждения с суждениями других участников диалога, обнаруживать различие и сходство позиций;
- публично представлять результаты выполненного опыта (исследования, проекта);
- самостоятельно выбирать формат выступления с учётом задач презентации и особенностей аудитории.

Регулятивные универсальные учебные действия:

- выявлять проблемы для решения в жизненных и учебных ситуациях;
- ориентироваться в различных подходах принятия решений;
- составлять план действий (план реализации намеченного алгоритма решения), корректировать предложенный алгоритм;
- делать выбор и брать ответственность за решение;
- владеть способами самоконтроля, самомотивации и рефлексии;
- давать адекватную оценку ситуации и предлагать план её изменения;
- учитывать контекст и предвидеть трудности, которые могут возникнуть при решении учебной задачи;
- объяснять причины достижения (недостижения) результатов деятельности;
- вносить коррективы в деятельность на основе новых обстоятельств;
- оценивать соответствие результата цели и условиям;
- ставить себя на место другого человека, понимать мотивы и намерения другого;
- регулировать способ выражения эмоций;
- осознанно относиться к другому человеку, его мнению;
- признавать своё право на ошибку и такое же право другого.

Совместная деятельность:

- понимать и использовать преимущества командной и индивидуальной работы;
- принимать цель совместной деятельности, коллективно строить действия по её достижению;
- уметь обобщать мнения нескольких людей;
- планировать организацию совместной работы, определять свою роль;
- выполнять свою часть работы, достигать качественного результата;
- оценивать качество своего вклада в общий продукт;
- сравнивать результаты с исходной задачей и вклад каждого члена команды.

3.3. Предметные результаты

- владение основными понятиями: информация, информационная безопасность, персональные данные, цифровой след, кибербуллинг, фишинг, вредоносное программное обеспечение;
- умение характеризовать основные виды угроз информационной безопасности в сети Интернет;
- умение соблюдать сетевой этикет, базовые нормы информационной этики и права при работе с приложениями на любых устройствах и в сети Интернет;
- умение выбирать безопасные стратегии поведения в сети Интернет;
- умение обеспечивать личную безопасность при использовании ресурсов сети Интернет, в том числе умение защищать персональную информацию от несанкционированного доступа и его последствий (разглашения, подмены, утраты данных);
- умение распознавать попытки и предупреждать вовлечение себя и окружающих в деструктивные и криминальные формы сетевой активности (в том числе кибербуллинг, фишинг);
- владение приёмами создания надёжных паролей и оценки их стойкости;
- умение оценивать достоверность информации, представленной в сети Интернет;
- умение создавать личное информационное пространство с соблюдением норм безопасности;
- владение умениями пользования цифровыми сервисами государственных услуг и цифровыми образовательными сервисами с соблюдением правил безопасности.

4. СОДЕРЖАНИЕ ПРОГРАММЫ

Раздел 1. Человек в мире информации (4 ч)

Информация и её роль в жизни человека. Виды информации. Информационная безопасность как часть общей культуры личности. Базовые элементы коммуникации. Цифровая среда: возможности и риски. Понятие «информационная безопасность». Основные направления информационной безопасности личности. Правила безопасного поведения при работе с приложениями на любых устройствах.

Раздел 2. Угрозы информационной безопасности (10 ч)

Понятие угрозы информационной безопасности. Основные виды угроз в сети Интернет. Кибербуллинг: понятие, признаки, способы противодействия. Фишинг и мошеннические сообщения: распознавание и защита. Вредоносное

программное обеспечение и его виды. Недостоверная информация и фейки: способы распознавания. Опасность вовлечения в деструктивные сетевые сообщества. Основные технологические и социально-психологические аспекты использования сети Интернет (сетевая анонимность, цифровой след, аутентичность субъектов и ресурсов).

Раздел 3. Персональные данные и цифровой след (8 ч)

Понятие персональных данных. Цифровой след: понятие, виды, последствия. Способы защиты персональной информации от несанкционированного доступа и его последствий (разглашения, подмены, утраты данных). Надёжный пароль: принципы создания и оценки стойкости. Правила размещения личной информации в сети Интернет. Настройки конфиденциальности в приложениях и социальных сетях. Безопасные стратегии поведения в сети.

Раздел 4. Информационная этика и право (6 ч)

Сетевой этикет. Базовые нормы информационной этики и права при работе с приложениями на любых устройствах и в сети Интернет. Уважение к правам других пользователей. Ответственность за размещение информации. Защита детей от информации, причиняющей вред их здоровью и развитию (Федеральный закон № 436-ФЗ). Реестр иностранных агентов и федеральный список экстремистских материалов: основы правовой грамотности.

Раздел 5. Проектная деятельность (6 ч)

Работа с информацией. Выполнение проектов по теме «Информационная безопасность». Разработка памяток, буклетов, инфографики. Подготовка и презентация проектов. Рефлексия и оценка результатов.

5. ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Наименование раздела и темы	Количество часов
Раздел 1. Человек в мире информации		**4**

№ п/п	Наименование раздела и темы	Количество часов
1.1	Информация и её роль в жизни человека. Виды информации	1
1.2	Информационная безопасность как часть культуры личности	1
1.3	Цифровая среда: возможности и риски	1
1.4	Правила безопасного поведения при работе с приложениями	1
Раздел 2. Угрозы информационной безопасности		**10**
2.1	Понятие угрозы информационной безопасности. Основные виды угроз	1
2.2	Кибербуллинг: понятие, признаки, способы противодействия	1
2.3	Практикум: распознавание ситуаций кибербуллинга	1
2.4	Фишинг и мошеннические сообщения: распознавание	1
2.5	Практикум: анализ мошеннических сообщений	1

№ п/п	Наименование раздела и темы	Количество часов
2.6	Вредоносное программное обеспечение и его виды	1
2.7	Недостоверная информация и фейки: способы распознавания	1
2.8	Практикум: проверка достоверности информации	1
2.9	Опасность вовлечения в деструктивные сетевые сообщества	1
2.10	Сетевая анонимность и аутентичность субъектов и ресурсов	1
Раздел 3. Персональные данные и цифровой след		**8**
3.1	Понятие персональных данных	1
3.2	Цифровой след: понятие, виды, последствия	1
3.3	Способы защиты персональной информации	1
3.4	Надёжный пароль: принципы создания	1
3.5	Практикум: генерация и оценка надёжности паролей	1

№ п/п	Наименование раздела и темы	Количество часов
3.6	Правила размещения личной информации в сети Интернет	1
3.7	Настройки конфиденциальности в приложениях	1
3.8	Безопасные стратегии поведения в сети	1
Раздел 4. Информационная этика и право		**6**
4.1	Сетевой этикет: основные правила	1
4.2	Базовые нормы информационной этики и права	1
4.3	Уважение к правам других пользователей. Ответственность за размещение информации	1
4.4	Защита детей от информации, причиняющей вред здоровью (ФЗ № 436-ФЗ)	1
4.5	Правовая грамотность: реестр иностранных агентов и экстремистские материалы	1

№ п/п	Наименование раздела и темы	Количество часов
4.6	Практикум: разбор правовых ситуаций в цифровой среде	1
Раздел 5. Проектная деятельность		**6**
5.1	Работа с информацией. Выбор темы проекта	1
5.2	Разработка памятки «Мои правила информационной безопасности»	1
5.3	Создание инфографики по теме безопасности в сети	1
5.4	Подготовка проекта «Информационная безопасность»	1
5.5	Презентация проектов	1
5.6	Рефлексия. Итоговое занятие	1
ОБЩЕЕ КОЛИЧЕСТВО ЧАСОВ		**34**

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Нормативные документы:

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;
- Стратегия государственной культурной политики на период до 2030 года (распоряжение Правительства РФ от 11.09.2024 № 2501-р).

Информационные ресурсы:

- Реестр иностранных агентов: https://minjust.gov.ru/ru/pages/reestr-inostrannykh-agentov/;
- Федеральный список экстремистских материалов: https://minjust.gov.ru/ru/extremist-materials/;
- Портал «Грамота.ру»;
- Цифровые образовательные сервисы.

Материально-техническое обеспечение: компьютер с выходом в Интернет, проектор, интерактивная доска, раздаточные материалы (памятки, кейсы).

7. ФОРМЫ АТТЕСТАЦИИ И КОНТРОЛЯ

Оценка результатов освоения курса осуществляется в форме педагогического наблюдения, выполнения практических работ, защиты проектов. Итоговая аттестация не предусмотрена. Результаты фиксируются в портфолио обучающегося.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 145792345010397423411790935696345598984963060873

Владелец Добычина Ольга Александровна

Действителен С 08.04.2026 по 08.04.2027