

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ СМОЛЕНСКОЙ ОБЛАСТИ
Управление образования и молодёжной политики Администрации города Смоленска
МБОУ «СШ № 33»

РАССМОТРЕНО

Руководитель кафедры



Гайжутене Е.И.

Протокол № 1 от «29»
августа 2025 г.

ПРИНЯТО

Решением

педагогического совета
МБОУ «СШ № 33»

Протокол № 1 от «29»
августа 2025 г.

УТВЕРЖДЕНО

Директор МБОУ «СШ № 33»



Жойкин С.А.

Приказ № 82/од от «29» августа
2025 г.



СОГЛАСОВАНО

Заместитель директора



Куляпкина И.В.

РАБОЧАЯ ПРОГРАММА
по курсу внеурочной деятельности
«Информационная безопасность»
для обучающихся 10 классов

2025 -2026 учебный год

1. Пояснительная записка

Программа разработана в соответствии с:

- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- ФГОС среднего общего образования;
- Концепцией информационной безопасности детей (распоряжение Правительства РФ от 02.12.2015 № 2471-р);
- Доктриной информационной безопасности РФ (Указ Президента РФ от 05.12.2016 № 646);
- Стратегией развития информационного общества в РФ на 2017–2030 годы (Указ Президента РФ от 09.05.2017 № 203).

Цель курса — формирование у обучающихся культуры информационной безопасности, навыков безопасного поведения в цифровом пространстве и понимания правовых аспектов работы с информацией.

Задачи:

- изучить основные угрозы информационной безопасности и способы защиты от них;
- освоить правила работы с персональными данными и парольной защитой;
- понять правовые основы ответственности за правонарушения в информационной сфере;
- развить навыки критического анализа информации в сети;
- сформировать осознанное отношение к цифровой репутации и сетевому этикету.

Место курса в учебном плане: 34 часа (1 час в неделю).

2. Планируемые результаты

Личностные:

- осознание ценности личной информации и необходимости её защиты;
- понимание ответственности за распространение информации в сети;
- готовность соблюдать нормы информационной этики.

Метапредметные:

- умение анализировать риски при работе с цифровыми ресурсами;
- способность критически оценивать информацию из разных источников;
- навыки безопасного использования сетевых сервисов.

Предметные:

- знание основных видов информационных угроз и способов защиты;
- владение методами безопасной аутентификации и хранения паролей;
- понимание правовых норм в сфере информационной безопасности;
- умение настраивать конфиденциальность в соцсетях и мессенджерах;
- навыки распознавания фишинга и вредоносного контента.

3. Содержание курса

Модуль 1. Правовые основы информационной безопасности (6 ч)

- Понятие информационной безопасности. Основные угрозы.
- Законодательство РФ в сфере информационной безопасности.
- Виды юридической ответственности (уголовная, административная, гражданско-правовая).
- Защита персональных данных: права и обязанности.
- Авторское право в цифровой среде.
- Правовые аспекты использования соцсетей и мессенджеров.

Модуль 2. Безопасность персональных данных (8 ч)

- Что такое персональные данные. Риски их утечки.
- Правила создания и хранения надёжных паролей.
- Многофакторная аутентификация.
- Настройки конфиденциальности в соцсетях.
- Безопасная работа с электронной почтой.
- Защита мобильных устройств.
- Резервное копирование данных.
- Безопасное использование облачных сервисов.

Модуль 3. Кибер угрозы и защита от них (10 ч)

- Вредоносные программы: виды и способы распространения.
- Фишинг и социальная инженерия.
- Мошенничество в интернете: схемы и защита.
- Кибербуллинг: профилактика и реагирование.
- Фальшивые новости и дезинформация.
- Безопасность онлайн-платежей.
- Уязвимости Wi-Fi и публичных сетей.
- Защита от слежки и несанкционированного доступа.
- Антивирусные программы: выбор и использование.
- Безопасный сёрфинг: фильтры и расширения.

Модуль 4. Цифровая культура и этика (10 ч)

- Цифровой след и репутация.
- Сетевой этикет: правила общения.
- Ответственность за контент: публикации, комментарии, репосты.
- Безопасное общение с незнакомцами.
- Профилактика интернет-зависимости.
- Критическое мышление в цифровой среде.
- Позитивные ресурсы интернета: образование и карьера.
- Профессии в сфере информационной безопасности.
- Государственная политика в области информационной безопасности.
- Практикум: разбор кейсов по информационной безопасности.

4. Тематическое планирование (КТП) 10Б класс 2025-2026 учебный год

Учитель Гращенкова Т.П.

№	Тема занятия	Кол-во часов	Дата (план)	Дата (факт)
1	Введение. Что такое информационная безопасность	1		
2	Основные угрозы в цифровом пространстве	1		
3	Законодательство РФ в сфере ИБ	1		
4	Юридическая ответственность за правонарушения в сети	1		
5	Защита персональных данных: права и обязанности	1		
6	Авторское право в цифровой среде	1		
7	Что такое персональные данные и почему их нужно защищать	1		
8	Надёжные пароли: создание и хранение	1		
9	Многофакторная аутентификация	1		
10	Настройки конфиденциальности в соцсетях	1		
11	Безопасная работа с электронной почтой	1		
12	Защита мобильных устройств	1		
13	Резервное копирование данных	1		
14	Безопасное использование облачных сервисов	1		
15	Вредоносные программы: виды и защита	1		
16	Фишинг и социальная инженерия	1		
17	Мошенничество в интернете	1		
18	Кибербуллинг: как защититься	1		
19	Фальшивые новости и дезинформация	1		
20	Безопасность онлайн-платежей	1		
21	Уязвимости Wi-Fi и публичных сетей	1		
22	Защита от слежки и несанкционированного доступа	1		
23	Антивирусные программы: выбор и настройка	1		
24	Безопасный сёрфинг: инструменты и приёмы	1		
25	Цифровой след и репутация	1		
26	Сетевой этикет: правила общения	1		

№	Тема занятия	Кол-во часов	Дата (план)	Дата (факт)
27	Ответственность за публикуемый контент	1		
28	Безопасное общение с незнакомцами	1		
29	Профилактика интернет-зависимости	1		
30	Критическое мышление в цифровой среде	1		
31	Позитивные ресурсы интернета	1		
32	Профессии в сфере ИБ	1		
33	Государственная политика в области ИБ	1		
34	Практикум: разбор кейсов по ИБ	1		

5. Формы контроля и оценивания

- **Текущий контроль:** тесты, практические задания, анализ кейсов.
- **Промежуточный контроль:** проектная работа (например, «Создание безопасного цифрового профиля»).
- **Итоговый контроль:** защита проекта или итоговый тест.

6. Учебно-методическое обеспечение

Основные ресурсы:

- Федеральный портал «Информационно-просветительская поддержка» (<https://национальныепроекты.рф/>);
- Материалы Роскомнадзора и МВД РФ по кибербезопасности;
- Образовательные платформы (Stepik, Яндекс Учебник) по ИБ.

Дополнительные материалы:

- видеолекции экспертов по кибербезопасности;
- интерактивные тренажёры по распознаванию фишинга;
- кейсы реальных инцидентов ИБ (с обезличиванием данных).